

AO 120 (Rev. 08/10)

TO: <b>Mail Stop 8</b> <b>Director of the U.S. Patent and Trademark Office</b> <b>P.O. Box 1450</b> <b>Alexandria, VA 22313-1450</b>	<b>REPORT ON THE</b> <b>FILING OR DETERMINATION OF AN</b> <b>ACTION REGARDING A PATENT OR</b> <b>TRADEMARK</b>
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court \_\_\_\_\_ for the District of Delaware \_\_\_\_\_ on the following

Trademarks or  Patents. (  the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED 9/11/2015	U.S. DISTRICT COURT for the District of Delaware
PLAINTIFF ICONTROL NETWORKS, INC.		DEFENDANT SECURENET TECHNOLOGIES LLC
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,855,635	12/21/2010	Icontrol Networks, Inc.
2 8,473,619	6/25/2013	Icontrol Networks, Inc.
3 8,478,844	7/2/2013	Icontrol Networks, Inc.
4 8,073,931	12/6/2011	Icontrol Networks, Inc.
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
--------------------

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director    Copy 3—Upon termination of action, mail this copy to Director  
 Copy 2—Upon filing document adding patent(s), mail this copy to Director    Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: <b>Mail Stop 8</b> <b>Director of the U.S. Patent and Trademark Office</b> <b>P.O. Box 1450</b> <b>Alexandria, VA 22313-1450</b>	<b>REPORT ON THE</b> <b>FILING OR DETERMINATION OF AN</b> <b>ACTION REGARDING A PATENT OR</b> <b>TRADEMARK</b>
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Southern District of Indiana on the following  
 Trademarks or  Patents. (  the patent action involves 35 U.S.C. § 292.):

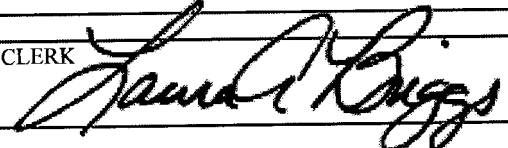

DOCKET NO. 1:15-cv-1222-P/K	DATE FILED 8/5/2015	U.S. DISTRICT COURT Southern District of Indiana	
PLAINTIFF ELI LILLY AND COMPANY		DEFENDANT UROPEP BIOTECH GbR.	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1 8,791,124	7/29/2014		
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT  Order of dismissal dated 9/11/2015 attached
--

CLERK 	(BY) DEPUTY CLERK 	DATE 9/14/2015
--	---	-------------------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director  
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: <b>Mail Stop 8</b> <b>Director of the U.S. Patent and Trademark Office</b> <b>P.O. Box 1450</b> <b>Alexandria, VA 22313-1450</b>	<b>REPORT ON THE</b> <b>FILING OR DETERMINATION OF AN</b> <b>ACTION REGARDING A PATENT OR</b> <b>TRADEMARK</b>
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Missouri on the following

Trademarks or  Patents . (  the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 4:15CV1408 RWS	DATE FILED 9/11/2015	U.S. DISTRICT COURT Eastern District of Missouri
PLAINTIFF Prosper Funding, LLC		DEFENDANT Prosper Capital, LLC Prosper Women Entrepreneurs
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 3,374,113	1/22/2008	Prosper Marketplace, Inc.
2 3,274,817	8/7/2007	Prosper Markeetplace, Inc.
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
--------------------

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director  
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

<b>Mail Stop 8</b> <b>Director of the U.S. Patent and Trademark Office</b> <b>P.O. Box 1450</b> <b>Alexandria, VA 22313-1450</b>	<b>REPORT ON THE</b> <b>FILING OR DETERMINATION OF AN</b> <b>ACTION REGARDING A PATENT OR</b> <b>TRADEMARK</b>
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court \_\_\_\_\_ for the District of Delaware on the following

Trademarks or  Patents. (  the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED 9/16/2014	U.S. DISTRICT COURT for the District of Delaware
PLAINTIFF Icontrol Networks, Inc.		DEFENDANT SecureNet Technologies LLC
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,624,750	9/23/2003	Icontrol Networks, Inc.
2 7,262,690	8/28/2007	Icontrol Networks, Inc.
3 7,855,635	12/21/2010	Icontrol Networks, Inc.
4 8,335,842	12/18/2012	Icontrol Networks, Inc.
5 8,473,619	6/25/2013	Icontrol Networks, Inc.
6 8,478,844	7/2/2013	Icontrol Networks, Inc.
7 8,612,591	12/17/2013	Icontrol Networks, Inc.

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

AO 120 (Rev. 08/10)

TO: <b>Mail Stop 8</b> <b>Director of the U.S. Patent and Trademark Office</b> <b>P.O. Box 1450</b> <b>Alexandria, VA 22313-1450</b>	<b>REPORT ON THE</b> <b>FILING OR DETERMINATION OF AN</b> <b>ACTION REGARDING A PATENT OR</b> <b>TRADEMARK</b>
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court \_\_\_\_\_ for the District Court of Delaware \_\_\_\_\_ on the following

Trademarks or  Patents. (  the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED 9/10/2014	U.S. DISTRICT COURT for the District Court of Delaware
PLAINTIFF CLOUDING CORP.		DEFENDANT EMC CORPORATION, et al.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5,495,607	2/27/1996	CLOUDING CORP.
2 5,825,891	10/20/1998	CLOUDING CORP.
3 5,944,839	8/31/1999	CLOUDING CORP.
4 6,631,449	10/7/2003	CLOUDING CORP.
5 6,738,799	5/18/2004	CLOUDING CORP.

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED 9/10/2014	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input checked="" type="checkbox"/> Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,925,481	8/2/2005	CLOUDING CORP.
2 7,254,621	8/7/2007	CLOUDING CORP.
3 7,065,637	6/20/2006	CLOUDING CORP.
4 7,272,708	9/18/2007	CLOUDING CORP.
5 7,032,089	4/18/2006	CLOUDING CORP.

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
--------------------

CLERK	(BY) DEPUTY CLERK	DATE

AO 120 (Rev. 08/10)

<b>TO:</b> <b>Mail Stop 8</b> <b>Director of the U.S. Patent and Trademark Office</b> <b>P.O. Box 1450</b> <b>Alexandria, VA 22313-1450</b>	<b>REPORT ON THE</b> <b>FILING OR DETERMINATION OF AN</b> <b>ACTION REGARDING A PATENT OR</b> <b>TRADEMARK</b>
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court District of Delaware on the following

Trademarks or  Patents. (  the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED 4/17/2014	U.S. DISTRICT COURT District of Delaware
PLAINTIFF Antennatech, LLC		DEFENDANT Chevron Corporation
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 US 8,112,131 B2	2/7/2012	Antennatech, LLC
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK HOLDER OF PATENT OR TRADEMARK
1	
2	
3	
4	
5	

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT  <i>Dismissed Voluntarily - See Attached</i>
---

CLERK <b>John A Cerino, Clerk</b> <b>United States District Court</b> <b>844 N. King Street, Unit 18</b> <b>Wilmington, DE 19801</b>	(BY) DEPUTY CLERK 	DATE 9/17/14
---	-----------------------	-----------------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director  
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

<b>TO:</b> <b>Mail Stop 8</b> <b>Director of the U.S. Patent and Trademark Office</b> <b>P.O. Box 1450</b> <b>Alexandria, VA 22313-1450</b>	<b>REPORT ON THE</b> <b>FILING OR DETERMINATION OF AN</b> <b>ACTION REGARDING A PATENT OR</b> <b>TRADEMARK</b>
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Virginia on the following

Trademarks or  Patents. (  the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 1:13-CV-00834	DATE FILED 07/10/2013	U.S. DISTRICT COURT Eastern District of Virginia
PLAINTIFF iControl Networks, Inc.		DEFENDANT Alarm.com Incorporated, et al.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,262,690	8/28/2007	Mygard PLC, Buckinghamshire
2 7,911,341	3/22/2011	iControl Networks Inc.
3 8,073,931	12/6/2011	iControl Networks Inc.,
4 8,335,842	12/18/2012	iControl Networks Inc.,
5 8,473,619	6/25/2013	iControl Networks Inc.,

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1 8,478,844	7/2/2013	iControl Networks Inc.,	
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
--------------------

CLERK Fernando Galindo	(BY) DEPUTY CLERK Judith Lanham	DATE 7/11/2013
---------------------------	------------------------------------	-------------------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director  
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy



APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/189,788	07/02/2013	8478844	ICON.P001D3	7650

98195 7590 06/12/2013  
 Gregory & Sawrie LLP  
 2022 Bissonnet Street  
 Houston, TX 77005

### ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

**Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)**  
 (application filed on or after May 29, 2000)

The Patent Term Adjustment is 53 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

- Marc Baum, San Jose, CA;
- Paul J. Dawes, Woodside, CA;
- Mike Kinney, Foster city, CA;
- Reza Raji, Menlo Park, CA;
- David Swenson, Glyndon, MN;
- Aaron Wood, Boulder Creek, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit [SelectUSA.gov](http://SelectUSA.gov).



**PART B - FEE(S) TRANSMITTAL**

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**  
**or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the **ISSUE FEE** and **PUBLICATION FEE** (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

98195                      7590                      05/08/2013  
**Gregory & Sawrie LLP**  
**2018 Bissonnet Street**  
**Houston, TX 77005**

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

_____ (Depositor's name)
_____ (Signature)
_____ (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/189,788	08/12/2008	Marc Baum	ICON.P001D3	7650

**TITLE OF INVENTION:** FORMING A SECURITY NETWORK INCLUDING INTEGRATED SECURITY SYSTEM COMPONENTS AND NETWORK DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$890	\$300	\$0	\$1190	08/08/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
MEJIA, ANTHONY	2451	709-220000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Gregory & Sawrie LLP

2 \_\_\_\_\_

3 \_\_\_\_\_

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

**iControl Networks, Inc.**

**Redwood City, CA**

Please check the appropriate assignee category or categories (will not be printed on the patent):  Individual  Corporation or other private group entity  Government

4a. The following fee(s) are submitted:

- Issue Fee
- Publication Fee (No small entity discount permitted)
- Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- A check is enclosed.
- Payment by credit card. Form PTO-2038 is attached.
- The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number \_\_\_\_\_ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

- Applicant certifying micro entity status. See 37 CFR 1.29
- Applicant asserting small entity status. See 37 CFR 1.27
- Applicant changing to regular undiscounted fee status.

**NOTE:** Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

**NOTE:** If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

**NOTE:** Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

**NOTE:** The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature \_\_\_\_\_

Date May 22, 2013

Typed or printed name Richard L. Gregory, Jr.

Registration No. 42,607

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12189788
<b>Filing Date:</b>	12-Aug-2008
<b>Title of Invention:</b>	FORMING A SECURITY NETWORK INCLUDING INTEGRATED SECURITY SYSTEM COMPONENTS AND NETWORK DEVICES
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Filer:</b>	Richard L. Gregory/Kim Moore
<b>Attorney Docket Number:</b>	ICON.P001D3

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
Utility Appl Issue Fee	2501	1	890	890
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>1190</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	15848703
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	FORMING A SECURITY NETWORK INCLUDING INTEGRATED SECURITY SYSTEM COMPONENTS AND NETWORK DEVICES
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	98195
<b>Filer:</b>	Richard L. Gregory/Kim Moore
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	22-MAY-2013
<b>Filing Date:</b>	12-AUG-2008
<b>Time Stamp:</b>	19:11:03
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1190
RAM confirmation Number	5905
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / zip	Pages (if appl.)
		SecureNet Technologies, LLC Exhibit 1003			Page 13

1	Issue Fee Payment (PTO-85B)	ICON_P001D3_Issue_Fee_Payment_22MAY2013.pdf	251554	no	2
			03ef39947cc4dc31781c227f094b7fb977a88e4f		

**Warnings:**

**Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	32045	no	2
			1c57f2e88f2511e29f3ea203c931ad0764969bb6		

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>			283599		
-------------------------------------	--	--	--------	--	--

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



NOTICE OF ALLOWANCE AND FEE(S) DUE

98195 7590 05/08/2013
Gregory & Sawrie LLP
2018 Bissonnet Street
Houston, TX 77005

Table with 2 columns: EXAMINER (MEJIA, ANTHONY), ART UNIT (2451), PAPER NUMBER (7650)

DATE MAILED: 05/08/2013

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

12/189,788 08/12/2008 Marc Baum ICON.P001D3 7650

TITLE OF INVENTION: FORMING A SECURITY NETWORK INCLUDING INTEGRATED SECURITY SYSTEM COMPONENTS AND NETWORK DEVICES

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

nonprovisional SMALL \$890 \$300 \$0 \$1190 08/08/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

98195                      7590                      05/08/2013  
**Gregory & Sawrie LLP**  
 2018 Bissonnet Street  
 Houston, TX 77005

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/189,788	08/12/2008	Marc Baum	ICON.P001D3	7650

TITLE OF INVENTION: FORMING A SECURITY NETWORK INCLUDING INTEGRATED SECURITY SYSTEM COMPONENTS AND NETWORK DEVICES

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$890	\$300	\$0	\$1190	08/08/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
MEJIA, ANTHONY	2451	709-220000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
---	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--



5. **Change in Entity Status** (from status indicated above)

- Applicant certifying micro entity status. See 37 CFR 1.29
- Applicant asserting small entity status. See 37 CFR 1.27
- Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

---

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

---

Authorized Signature \_\_\_\_\_

Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_

Registration No. \_\_\_\_\_

---

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

---



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
12/189,788 08/12/2008 Marc Baum ICON.P001D3 7650

98195 7590 05/08/2013
Gregory & Sawrie LLP
2018 Bissonnet Street
Houston, TX 77005

Table with 1 column: EXAMINER
MEJIA, ANTHONY

Table with 2 columns: ART UNIT, PAPER NUMBER
2451

DATE MAILED: 05/08/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

## Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<b>Notice of Allowability</b>	<b>Application No.</b> 12/189,788	<b>Applicant(s)</b> BAUM ET AL.	
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451	<b>AIA (First Inventor to File) Status</b> No

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to amendment submitted/entered with filing of RCE filed on 04/10/2013.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 1-3, 5-51. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

- a)  All    b)  Some    \*c)  None of the:
1.  Certified copies of the priority documents have been received.
  2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

**Interim copies:**

- a)  All    b)  Some    c)  None of the: Interim copies of the priority documents have been received.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.  
**Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |  |   |
|--|---|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 5. <input checked="" type="checkbox"/> Examiner's Amendment/Comment       |
| 2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date _____    | 6. <input type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material | 7. <input type="checkbox"/> Other _____.                                  |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____.                     |   |

/ANTHONY MEJIA/  
Examiner, Art Unit 2451

## **DETAILED ACTION**

### ***Information Disclosure Statement***

1. The information disclosure statement filed **15 October 2009** and **07 June 2012** fail to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed.

Furthermore, the citations listed on page 8 of the IDS submitted on **07 June 2012** and page 4 of the IDS submitted on **15 October 2009** is missing dates. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

### ***Conclusion***

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY MEJIA whose telephone number is (571)270-3630. The examiner can normally be reached on Mon-Thur 9:30AM-8:00PM EST.

Art Unit: 2451

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANTHONY MEJIA/

Examiner, Art Unit 2451

<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 1 of 2

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,192,418 B1	Hale et al.	719/312
*	B	US-2001/0030597 A1	Inoue et al.	340/3.7
*	C	US-2002/0180579 A1	Nagaoka et al.	340/3.1
*	D	US-2003/0023839 A1	Burkhardt et al.	713/1
*	E	US-2003/0062997 A1	Naidoo et al.	340/531
*	F	US-6,686,838 B1	Rezvani et al.	340/506
*	G	US-6,756,998 B1	Bilger, Brent	715/764
*	H	US-2005/0120082 A1	Hesselink et al.	709/203
*	I	US-6,963,981 B1	Bailey et al.	726/22
*	J	US-2005/0267605 A1	Lee et al.	700/019
*	K	US-7,015,806 B2	Naidoo et al.	340/531
*	L	US-7,043,537 B1	Pratt, Richard W.	709/220
*	M	US-2006/0142968 A1	Han et al.	702/120

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
N					
O					
P					
Q					
R					
S					
T					

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
U					
V					
W					
X					

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 2 of 2

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification	
*	A	US-7,107,322 B1	09-2006	Freeny, Jr., Charles C.	709/217
*	B	US-2006/0242395 A1	10-2006	Fausak, Andrew T.	713/001
*	C	US-2006/0271695 A1	11-2006	Lavian, Yoel	709/229
*	D	US-2006/0282886 A1	12-2006	Gaug, Mark	726/005
*	E	US-7,149,814 B2	12-2006	Neufeld et al.	709/248
*	F	US-7,164,907 B2	01-2007	Cochran et al.	455/419
*	G	US-2007/0079385 A1	04-2007	Williams et al.	726/027
*	H	US-2007/0143440 A1	06-2007	Reckamp et al.	709/217
*	I	US-2007/0256105 A1	11-2007	Tabe, Joseph Akwo	725/078
*	J	US-7,412,447 B2	08-2008	Hilbert et al.	1/1
*	K	US-7,681,201 B2	03-2010	Dale et al.	719/313
*	L	US-7,970,863 B1	06-2011	Fontaine, Jean-Emmanuel	709/218
*	M	US-2011/0283006 A1	11-2011	Ramamurthy, Venkatesh	709/228

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	660	(gateway) near5 (connect\$3 communicat\$3) near5 (devices sensors) near5 (home location)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 19:07
L2	9	(gateway) near5 (connect\$3 communicat\$3) near5 (directly) near5 (devices sensors) near5 (home location)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 19:23
S1	2	"20060271695"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:01
S2	18	12/189757	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:01
S3	45868	709/201.ccls. 709/202.ccls. 709/203.ccls. 709/224.ccls. 709/225.ccls. 709/227.ccls. 717/101.ccls. 717/102.ccls. 707/203.ccls. 718/101.ccls. 726/1.ccls. 706/46.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:05
S4	34837379	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:05
S5	39563	S3 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:06
S6	3955	(automatically) near5 (locat\$3	US-PGPUB;	OR	ON	2011/03/27

		discover\$3 find\$3) near5 (components devices sensors)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:06
S7	201056	(generat\$3 creat\$3) near5 (network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S8	797	S6 AND S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S9	659	S8 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S10	797	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)) AND ((generat\$3 creat\$3) near5 (network))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S11	659	S10 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S12	476	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)) AND ((generat\$3 creat\$3) near5 (network)) AND (security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S13	416	S12 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:12
S14	25	(automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors) near5 (security surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2011/03/27 15:19

			IBM_TDB			
S15	23	S14 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:20
S16	3	"7015806".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:24
S17	2	"6756998".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:32
S18	2	"20020103898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 16:49
S19	2	"6686838".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/26 19:18
S20	9	"20030062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:29
S21	15	"2003/0062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:30
S22	2	09/969521	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:41
S23	2	"20090077622"	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2011/12/14 17:37

				EPO; JPO; DERWENT; IBM_TDB			
S24	2	"20040037295"		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 11:36
S25	2	"20020103898"		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 12:11
S26	3	"20040267939"		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/03 10:02
S27	383	"20010034754" "20020026476" "20020038380" "20020083342" "20020103898" "20020107910" "20020112051" "20020143923" "20020180579" "20030009552" "20030041167" "20030062997" "20030115345" "20030174648" "20030210126" "20040003241" "20040037295" "20040086088" "20040139227" "20040177163" "20040267937" "20050066045" "20050079855" "20050108091" "20050125083" "20050149639" "20050197847" "20050216580" "20050231349" "20060088092" "20060181406" "20060187900" "20060282886" "20070061266" "20070286210" "20070298772" "20080065681" "20080147834" "20080183842"	"20020004828" "20020029276" "20020052913" "20020095490" "20020103927" "20020111698" "20020112182" "20020156564" "20020184301" "20030009553" "20030052923" "20030090473" "20030132018" "20030187920" "20030236841" "20040015572" "20040054789" "20040123149" "20040162902" "20040243835" "20050038326" "20050069098" "20050086126" "20050108369" "20050128083" "20050169288" "20050216302" "20050222820" "20060009863" "20060105713" "20060182100" "20060200845" "20070052675" "20070106124" "20070286369" "20080042826" "20080084296" "20080180240" "20080235326"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/08/27 09:42

		"20090070436"   "20090165114"   "20090204693"   "20090240787"   "20090240814"   "20100082744"   "20100095111"   "20100095369"   "4779007"   "4860185"   "5086385"   "5519878"   "5579197"   "5963916"   "5991795"   "6037991"   "6052052"   "6140987"   "6198475"   "6219677"   "6286038"   "6288716"   "6331122"   "6353891"   "6363417"   "6370436"   "6377861"   "6452507"   "6462663"   "6467084"   "6480901"   "6493020"   "6496927"   "6529723"   "6542075"   "6563800"   "6574234"   "6580950"   "6587736"   "6591094"   "6601086"   "6609127"   "6615088"   "6643652"   "6643669"   "6648682"   "6658091"   "6721689"   "6721747"   "6756998"   "6789147"   "6795322"   "6826233"   "6865690"   "6912429"   "6928148"   "6930730"   "6931445"   "6959393"   "6990591"   "7016970"   "7024676"   "7034681"   "7047088"   "7047092"   "7072934"   "7099994"   "7130585"   "7148810"   "7174564"   "7183907"   "7203486"   "7222359"   "7237267"   "7305461"   "7337217"   "7337473"   "7343619"   "7349761"   "7349967"   "7367045"   "7370115"   "7383339"   "7403838"   "7409451"   "7428585"   "7430614"   "7440434"   "7457869"   "7469139"   "7469294"   "7480713"   "7480724"   "7506052"   "7509687"   "7526762"   "7551071"   "7558379"   "7577420"   "7587464"   "7627665"   "7634519"   "D416910"   "D451529"   "D464328"   "D464948").PN.				
S28	4802	(automaticlly) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/06 23:45
S29	0	(embedd\$3 stor\$3 sav\$3) near5 (operating ADJ system) near5 (gateway) near5 (client device terminal) near5 (control\$3 mana\$3) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 17:55
S30	107	(embedd\$3 stor\$3 sav\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2012/09/25 17:56

			DERWENT; IBM_TDB			
S31	6	(embedd\$3 stor\$3 sav\$3 add\$3) near5 (operating ADJ system) near5 (gateway) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:20
S32	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:22
S33	1	12/187788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:22
S34	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:22
S35	24546	(component widget) near5 (includ\$3 compris\$3) near5 ("OS" operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:26
S36	1079	(embedd\$3 stor\$3 sav\$3 add\$3) near5 (operating ADJ system) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:28
S37	568	(full) near5 (control\$4 management) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:29
S38	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:29
S39	447	S37 and S38	US-PGPUB; USPAT; USOCR;	OR	ON	2012/09/25 18:29

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S40	10	S36 AND S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:30
S41	631	((full) near5 (control\$4 management functions functionality) near5 (remote) near5 (server device system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:30
S42	11	S41 and S36	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:30
S43	1143	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote) near5 (server device system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:32
S44	216844	((control\$4 management functions functionality) near5 (remote) near5 (server device system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:32
S45	333	S43 and S44	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:42
S46	269	S45 and S38	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:42
S47	10	S46 and ((security sureveillance) ADJ (system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:43
S48	3045	((embedd\$3 stor\$3 sav\$3 add\$3	US-PGPUB;	OR	ON	2012/09/25

		copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external) near5 (server device system terminal)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			20:40
S49	3045	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:41
S50	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:41
S51	2363	S49 AND S50	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:41
S52	335741	(control\$4 manag\$3) near5 (remote external) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:43
S53	782	S49 AND S52	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:43
S54	1144	(gateway) near5 (control\$4 manag\$3) near5 (remote external) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:45
S55	810	S54 AND S50	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:46
S56	4	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2012/09/25 20:56



			IBM_TDB			
S57	2	"7970863".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:08
S58	5	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:32
S59	0	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 ("of") near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:33
S60	5	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:33
S61	5	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system (drivers)) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:33
S62	4768	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system (drivers)) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:33
S63	4768	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((operating ADJ system) (drivers)) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:34
S64	3741	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:35
S65	0	S64 and (icontrol)	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2012/09/25 21:36

			EPO; JPO; DERWENT; IBM_TDB			
S66	2739	("icontrol")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:37
S67	2	("icontrol") near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 22:06
S68	4768	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((drivers)operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 22:10
S69	7	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3 includ\$3) near5 ((drivers)(operating ADJ system)) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 22:14
S70	631	(full) near5 (control\$4 management functions functionality) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:32
S71	3741	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:32
S72	12	S71 and S70	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:32
S73	631	(full all) near5 (control\$4 management functions functionality) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:33
S74	671	(full all) near5 (control\$4 management functions functionality)	US-PGPUB; USPAT;	OR	ON	2012/09/25 23:34

		near5 (remote\$2) near5 (server device system)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S75	12	S74 AND S71	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:34
S76	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:34
S77	3741	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:35
S78	671	(full all) near5 (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:35
S79	12	S78 AND S77	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:35
S80	114	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)) SAME (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:47
S81	161	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((drivers) operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)) SAME (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:48
S82	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2012/09/25 23:49

			EPO; JPO; DERWENT; IBM_TDB			
S83	134	S81 AND S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:49
S84	261	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((drivers) operating ADJ system) near5 (remote external managed) near5 (server device system terminal component peripheral)) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:56
S85	266	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((drivers) operating ADJ system) near5 (remote external managed) near5 (device system terminal component peripheral)) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:56
S86	200	S85 AND S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:57
S87	0	(gateway gw) near5 ((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (device system terminal component peripheral)) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:59
S88	2	S86 AND ((Security surveillance camera) ADJ (system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:00
S89	555302	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (drivers) operating ADJ system (mini ADJ (operating ADJ system)) near5 (remote external managed) near5(server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:03
S90	167257	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ((drivers) operating ADJ system (mini ADJ (operating ADJ system)) near5 (remote external managed) near5(server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:03
S91	1644566	((drivers) operating ADJ system (mini ADJ (operating ADJ system))	US-PGPUB; USPAT;	OR	ON	2012/09/26 00:04

		near5 (remote external managed) near5(server))	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S92	1644566	((drivers) (operating ADJ system) (mini ADJ (operating ADJ system)) near5 (remote external managed) near5 (server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:05
S93	95	(mini ADJ (operating ADJ system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:06
S94	71	S93 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:06
S95	0	(mini ADJ (operating ADJ system)) near5 (remote\$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:08
S96	162	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:08
S97	107	S96 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:09
S98	4651	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:19
S99	256	S98 AND ((Security surveillance camera) ADJ (system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:19

S100	199	S99 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:20
S101	16	(full all) near5 (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system) SAME (Operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:21
S102	54	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ systems) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 01:03
S103	32	S102 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 01:03
S104	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:14
S105	199	(touchscreen interface gw gateway) same (reduced footprint mini) same ((operating ADJ system) Linux windows) same (remote)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:17
S106	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:18
S107	148	S105 AND S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:18
S108	147	(touchscreen interface gw gateway) same (reduced footprint mini) same ((operating ADJ system) Linux) same (remote)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2012/09/26 02:19

			DERWENT; IBM_TDB			
S109	113	S108 and S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:19
S110	360	(touchscreen interface gw gateway) same (reduced footprint mini) same ((operating ADJ system) Linux) same (host remote)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:20
S111	6	(touchscreen interface gw gateway) same (reduced footprint mini) same ((operating ADJ system) Linux) same (remote ADJ (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:23
S112	2	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (reduced footprint mini) same ((operating ADJ system) Linux) same (remote ADJ (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:24
S113	2	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (minature reduced footprint mini) same ((operating ADJ system) Linux) same (remote ADJ (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:24
S114	838	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (minature reduced footprint mini) same ((operating ADJ system) Linux)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:25
S115	667	S114 and S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:25
S116	445	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (compact minature reduced footprint mini) near5 ((operating ADJ system) Linux)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:31
S117	671	(full all) near5 (control\$4 management functions functionality) near5 (remote\$2) near5 (server	US-PGPUB; USPAT; USOCR;	OR	ON	2012/09/26 02:32

		device system)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S118	0	S116 and S117	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:32
S119	334	S116 and S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:32
S120	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:35
S121	157	ihub "ihub" "ihub client"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:36
S122	254370	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (compact minature reduced footprint mini minios)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:48
S123	8	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ( minios)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:48
S124	9	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ((minature reduced footprint mini) ADJ ((operating ADJ system) Linux)).CLM.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:02
S125	0	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ((minature reduced footprint mini) ADJ ((operating ADJ system) "OS") near5 (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:04
S126	12971	(embedd\$3 stor\$3 sav\$3 copy\$3	US-PGPUB;	OR	ON	2012/09/26



		sav\$3) near5 ((operating ADJ system) "OS") near5 (server host)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			03:04
S127	64	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (locally) near5 ((operating ADJ system) "OS") near5 (server host)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:05
S128	24	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (locally) near5 ((operating ADJ system) "OS") near5 (remote\$2 external\$2) near5 (server host)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:05
S129	64	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (locally) near5 ((operating ADJ system) "OS") near5 (server host)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:07
S130	37	S129 AND S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:08
S131	46	((minature reduced footprint mini) ADJ ((operating ADJ system) "OS") near5 (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:09
S132	26	S131 AND S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:10
S133	2	"6192418".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:16
S134	2	"6963981".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2012/09/26 03:19

			IBM_TDB			
S135	2	"20070256105"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:24
S136	2	"7681201".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:28
S137	2	"20070256105"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 16:40
S138	4	"2008045237"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/28 10:02
S139	3	"20080045237"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/28 10:03
S140	51	11/084232	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/04/22 13:13
S141	3	"20050216580"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/04/22 14:32
S142	51	11/084232	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/04/25 17:35
S143	1	12/878839	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2013/04/25 18:42

			EPO; JPO; DERWENT; IBM_TDB			
S144	2	"8335842".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/04/26 01:59
S145	250	( "20010016501"   "20010034754"   "20020004828"   "20020026476"   "20020029276"   "20020038380"   "20020052913"   "20020083342"   "20020095490"   "20020099809"   "20020103898"   "20020103927"   "20020107910"   "20020111698"   "20020112051"   "20020112182"   "20020128728"   "20020143923"   "20020156564"   "20020180579"   "20020184301"   "20030005030"   "20030009552"   "20030009553"   "20030041137"   "20030041167"   "20030051009"   "20030052923"   "20030062997"   "20030090473"   "20030115345"   "20030132018"   "20030174648"   "20030187920"   "20030210126"   "20030236841"   "20040003241"   "20040015572"   "20040037295"   "20040054789"   "20040086088"   "20040123149"   "20040139227"   "20040162902"   "20040177163"   "20040202351"   "20040243835"   "20040267937"   "20050010866"   "20050038326"   "20050066045"   "20050069098"   "20050079855"   "20050086126"   "20050102152"   "20050108091"   "20050108369"   "20050125083"   "20050128083"   "20050149639"   "20050169288"   "20050197847"   "20050216302"   "20050216580"   "20050222820"   "20050231349"   "20060009863"   "20060064305"   "20060088092"   "20060105713"   "20060111095"   "20060181406"   "20060182100"   "20060187900"   "20060200845"   "20060206220"   "20060271695"   "20060282886"   "20070052675"   "20070061266"   "20070106124"   "20070142022"   "20070256105"   "20070286210"   "20070286369"   "20070298772"   "20080042826"   "20080065681"   "20080084296"   "20080147834"   "20080180240"   "20080183842"   "20080235326").PN. OR ("20090070436"   "20090165114"   "20090204693"   "20090240787"   "20090240814"   "20100082744"   "20100095111"   "20100095369"   "4754261"   "4779007"   "4833449"   "4860185"   "4993059"   "5086385"   "5519878"   "5579197"	US-PGPUB; USPAT; USOCR	OR	OFF	2013/04/26 02:03

		"5715394"   "5907279"   "5963916"   "5991795"   "6037991" "6052052"   "6060994"   "6134591"   "6140987"   "6198479" "6219677"   "6281790"   "6286038"   "6288716"   "6331122" "6351829"   "6353891"   "6363417"   "6363422"   "6370436" "6377861"   "6385772"   "6400265"   "6462507"   "6462663" "6467084"   "6480901"   "6493020"   "6496927"   "6529723" "6542075"   "6563800"   "6574234"   "6580950"   "6587736" "6591094"   "6601086"   "6609127"   "6615088"   "6621827" "6636893"   "6643652"   "6643669"   "6648682"   "6658091" "6661340"   "6686838"   "6690411"   "6693545"   "6721689" "6721747"   "6738824"   "6756998"   "6778085"   "6781509" "6789147"   "6795322"   "6798344"   "6826233"   "6865690" "6891838"   "6912429"   "6928148"   "6930599"   "6930730" "6931445"   "6943681"   "6959393"   "6965313"   "6970183" "6972676"   "6975220"   "6990591"   "7016970"   "7020697" "7020701"   "7024676"   "7030752"   "7032002"   "7034681" "7039391"   "7047088"   "7047092"   "7072934"   "7079020" "7080046"   "7085937"   "7099944"   "7103152"   "7106176" "7113090"   "7113099"   "7120232"   "7120233"   "7130383" "7130585"   "7148810"   "7149798"   "7174564"   "7183907" "7203486"   "7209945"   "7218217"   "7222359"   "7237267" "7250854").PN. OR ("7254779"   "7262690"   "7305461"   "7337217" "7337473"   "7343619"   "7349761"   "7349967"   "7367045" "7370115"   "7383339"   "7403838"   "7409451"   "7428585" "7430614"   "7440434"   "7457869"   "7469139"   "7469294" "7480713"   "7480724"   "7506052"   "7509687"   "7526762" "7551071"   "7558379"   "7577420"   "7587464"   "7627665" "7634519"   "8140658"   "D416910"   "D451529"   "D464328" "D464948").PN. OR ("8335842").URPN.				
S146	483	(gateway "gw" system) near5 (data content) near5 (components devices) SAME (Security ADJ system)	US-PGPUB; OR USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2013/04/26 18:50

			IBM_TDB			
S147	45	S146 AND (discover\$3) near5 (devices components sensors)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/04/26 18:53
S148	35152288	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/04/26 18:59
S149	11	"20030062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/05/01 15:44
S150	770	(server system gateway) near5 (states status) near5 (devices sensors) near5 (home location)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 17:27
S151	323701	(interface "GUI") near5 (sensors devices cameras)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 17:30
S152	262	S150 and S151	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 17:31
S153	35153785	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 17:31
S154	210	S152 AND S153	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 17:31
S155	23	(server system gateway) near5 (chang\$3) near5 (states status) near5 (devices sensors) near5 (home location)	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2013/05/02 17:43

			EPO; JPO; DERWENT; IBM_TDB			
S156	52	(server system gateway) near5 (chang\$3 updat\$3) near5 (states status) near5 (devices sensors) near5 (home location)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 17:57
S157	3	(server system gateway) near5 (display\$3) near5 (chang\$3 updat\$3) near5 (states status) near5 (devices sensors) near5 (home location)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/05/02 17:58

**EAST Search History (Interference)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L8	7	((server system gateway) near5 (chang\$3 updat\$3) near5 (states status) near5 (devices sensors) near5 (home location)).CLM.	US- PGPUB; USPAT; UPAD	OR	ON	2013/05/02 19:25
L9	0	((server system gateway) near (chang\$3 updat\$3) near (states status) near (devices sensors) near (home location)).CLM.	US- PGPUB; USPAT; UPAD	OR	ON	2013/05/02 19:27
L10	4	((server system gateway) near (chang\$3 updat\$3) near (states status) near (devices sensors)).CLM.	US- PGPUB; USPAT; UPAD	OR	ON	2013/05/02 19:28

5/ 2/ 2013 8:38:31 PM

C:\Users\amejia\Documents\EAST\Workspaces\12189757A.wsp

Searching for: (gateway and server and state and security and changes and sensor) and (location or home) ([start a new search](#))

Found **229** within *The ACM Guide to Computing Literature* (Bibliographic citations from major publishers in computing)

**Limit your search** to [Publications from ACM and Affiliated Organizations](#) (Full-Text collection: **376,898** items)

## REFINE YOUR SEARCH

▼ Refine by Keywords

▼ Refine by People

Names  
Institutions  
Authors  
Editors  
Reviewers

▼ Refine by Publications

Publication Year  
Publication Names  
ACM Publications  
All Publications  
Content Formats  
Publishers

▼ Refine by Conferences

Sponsors  
Events  
Proceeding Series

Search Results

Related Journals

Related Magazines

Related SIGs

Related Conferences

Results 1 - 20 of 229

Sort by relevance

in expanded form

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)1 [Introduction---Network Convergence: Issues, Trends and Future](#)

Samir Chatterjee, Amitava Dutta, Vinay B. Chandhok

September 2004

**Information Systems Frontiers**, Volume 6 Issue 3**Publisher:** Kluwer Academic PublishersFull text available: [Publisher Site](#)**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count2 [Flexible Universal Networks---A New Approach to Telecommunication Services?](#)

Stephan Rupp, Franz Josef Sanel, Rodolfo Lopez Arias, Gerd Siegmund

April 2004

**Wireless Personal Communications: An International Journal**, Volume 29 Issue 1-2**Publisher:** Kluwer Academic PublishersFull text available: [Publisher Site](#)**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count

GPRS, WLAN integration, Mobile Number Portability and UMTS are some of the new technologies which are foreseen to carry many new service applications. In the near future, it is expected that mobile networks will go beyond connecting people and will connect ...

**Keywords:** 3G and 4G Internet protocols over heterogeneous networks, AAA, RADIUS, SIM access gateway, UMTS, WLAN, Web services, data model, home location register (HLR), mobility management, service control point (SCP), storage area networks (SAN), subscriber profile

3 [Building a software factory for pervasive systems development](#)

Javier Muñoz, Vicente Ferechano

June 2005

**CAISE'05:** Proceedings of the 17th international conference on Advanced Information Systems Engineering**Publisher:** Springer-VerlagFull text available: [Publisher Site](#)**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count

The rise of the number and complexity of pervasive systems is a fact. Pervasive systems developers need advanced development methods in order to build better systems in an easy way. Software Factories and the Model Driven Architecture (MDA) are two important ...

4 [Using standard Internet Protocols and applications in space](#)

Keith Hocie, Ed Criscuolo, Ron Parise

April 2005

**Computer Networks: The International Journal of Computer and Telecommunications Networking**, Volume 47 Issue 5**Publisher:** Elsevier North-Holland, Inc.**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count

This paper discusses approaches for using standard Internet technologies to meet the communication needs of future space missions. It summarizes work done by the Operating Missions as Nodes on the Internet (OMNI) project at NASA/GSFC since 1997. That ...

**Keywords:** Internet in space, Internet space missions, Space communication protocols, Space shuttle STS-107, Spacecraft networking

5 [CGI-based applications for distributed embedded systems for monitoring temperature and humidity](#)

Grisha Spasov, Nikolay Kakanakov

June 2004


**CompSysTech '04:** Proceedings of the 5th international conference on Computer systems and technologies**Publisher:** ACM

## ADVANCED SEARCH

[Advanced Search](#)

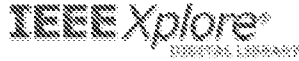
## FEEDBACK

[Please provide us with feedback](#)Found **229** of **2,121,947**

 There is a more recent version of your browser available. For an optimal experience, please consider upgrading to the most recent version of your browser. Your browser still supports access to key content and functionality but may experience occasional display issues



[IEEE.org](#) | [IEEE Xplore Digital Library](#) | [IEEE Standards](#) | [IEEE Spectrum](#) | [More Sites](#)



Access provided by:  
United States Patent and  
Trademark Office  
Sign Out



#### SEARCH RESULTS

You searched for: {{{{{{gateway} AND server} AND device sensors cameras} AND states OR statuses} AND network} AND changes OR updates} AND remote}

584 Results returned

< First | 1 | 2 | 3 | 4 | 5 | >> Last >

#### Experience with prefix discovery servers and IPSec VPN gateways

Sax, W. ; Jillson, C. ; Wollman, W. ; Jegers, H.  
Military Communications Conference, 2005. MILCOM 2005. IEEE  
Digital Object Identifier: 10.1109/MILCOM.2005.1605768  
Publication Year: 2005, Page(s): 725 - 735 Vol. 2  
IEEE CONFERENCE PUBLICATIONS

#### A framework to access networked appliances in wide area networks

Rahman, M. ; Braun, D. ; Bushmitch, D.  
Consumer Communications and Networking Conference, 2005. CCNC 2005 Second IEEE  
Digital Object Identifier: 10.1109/CCNC.2005.1405180  
Publication Year: 2005, Page(s): 261 - 266  
Cited by 1  
IEEE CONFERENCE PUBLICATIONS

#### A scalable web-based real-time information distribution service for industrial applications

Sebastine, S. ; Kyeung-Don Kang ; Abdelzaher, T.F. ; Son, S.H.  
Industrial Electronics Society, 2001. IECON '01. The 27th Annual Conference of the IEEE  
Volume: 3  
Digital Object Identifier: 10.1109/IECON.2001.975565  
Publication Year: 2001, Page(s): 1810 - 1815 vol.3  
IEEE CONFERENCE PUBLICATIONS

#### Monitoring of states and preventive maintenance [of distribution networks]

Hameury, H.  
Electricity Distribution, Part 1: Contributions. CHRED, 14th International Conference and Exhibition on (IEE Conf. Publ. No. 438)  
Volume: 1  
Digital Object Identifier: 10.1049/cp-19970460  
Publication Year: 1997, Page(s): 20/1 - 20/4 vol.1  
IET CONFERENCE PUBLICATIONS

#### Remote visualization and management tools for underwater operations

den Bosch, A.O. ; Santamaria, J.C.  
OCEANS, 2001. MTS/IEEE Conference and Exhibition  
Volume: 3  
Digital Object Identifier: 10.1109/OCEANS.2001.988145  
Publication Year: 2001, Page(s): 1953 - 1959 vol.3  
IEEE CONFERENCE PUBLICATIONS

#### A proposed protocol for remote control of automated assessment devices

Kissock, P.S. ; Fritchard, D.A.



Security Technology, 1996. 30th Annual 1996 International  
Carnahan Conference  
Digital Object Identifier: 10.1109/CCST.1996.551851  
Publication Year: 1996, Page(s): 115 - 119  
IEEE CONFERENCE PUBLICATIONS

**Metricom's Bicochet Network: alternative new  
technology for traffic signals**

Davis, R.E., III ; Aguigui, K.G.  
Intelligent Transportation Systems, 2001. Proceedings. 2001  
IEEE  
Digital Object Identifier: 10.1109/ITSC.2001.946819  
Publication Year: 2001, Page(s): 1120 - 1125  
IEEE CONFERENCE PUBLICATIONS

**Remote operation of the TETR BBS experiment from  
an off-site location**

Fonck, R.J. ; Cosby, G. ; Durst, R. ; Gibney, T. ; Thompson, M.  
; Paul, S.F.  
Review of Scientific Instruments  
Volume: 63, Issue: 10  
Digital Object Identifier: 10.1063/1.1143568  
Publication Year: 1992, Page(s): 4803 - 4805  
Cited by 3  
AIP JOURNALS & MAGAZINES

**Video surveillance for hazardous conditions using  
sensor networks**

Chung-Kuo Chang ; Huang, J.  
Networking, Sensing and Control, 2004 IEEE International  
Conference on  
Volume: 2  
Digital Object Identifier: 10.1109/ICNSC.2004.1297066  
Publication Year: 2004, Page(s): 1008 - 1013 Vol.2  
Cited by 5  
IEEE CONFERENCE PUBLICATIONS

**Minimal cost replication of dynamic Web contents  
under flat update delivery**

Xueyan Tang ; Chanson, S.T.  
Parallel and Distributed Systems, IEEE Transactions on  
Volume: 15, Issue: 5  
Digital Object Identifier: 10.1109/TPDS.2004.1278100  
Publication Year: 2004, Page(s): 431 - 439  
Cited by 7  
IEEE JOURNALS & MAGAZINES

**A generic embedded device for retrieving and  
transmitting information of various customized  
applications**

Fan-Tien Cheng ; Guo-Wei Huang ; Chun-Hung Chen ;  
Min-Hsiung Hung  
Robotics and Automation, 2004. Proceedings. ICRA '04. 2004  
IEEE International Conference on  
Volume: 1  
Digital Object Identifier: 10.1109/ROBOT.2004.1307277  
Publication Year: 2004, Page(s): 978 - 983 Vol.1  
Cited by 2  
IEEE CONFERENCE PUBLICATIONS

**Simple mobility support for IPsec tunnel mode**

Byoung-Jo, K. ; Srinivasan, S.  
Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003  
IEEE 58th  
Volume: 3  
Digital Object Identifier: 10.1109/VETECF.2003.1285375  
Publication Year: 2003, Page(s): 1999 - 2003 Vol.3  
Cited by 1  
IEEE CONFERENCE PUBLICATIONS

**Improving collision detection in distributed virtual  
environments by adaptive collision prediction  
tracking**

Ohlenburg, J.

Virtual Reality, 2004. Proceedings. IEEE  
 Digital Object Identifier: 10.1109/VR.2004.1310059  
 Publication Year: 2004, Page(s): 83 - 90  
 Cited by 6  
 IEEE CONFERENCE PUBLICATIONS

**Bi-directional communication into the deep ocean based on OrbComm satellite transmission and acoustic underwater communication**

Meinecke, G. ; Ratmeyer, V. ; Wefer, G.  
 OCEANS '99 MTS/IEEE. Riding the Crest into the 21st Century  
 Volume: 3  
 Digital Object Identifier: 10.1109/OCEANS.1999.800199  
 Publication Year: 1999, Page(s): 1405 - 1409 vol 3  
 IEEE CONFERENCE PUBLICATIONS

**A compact monitoring system for process valves**

Ahsan, G. ; Amer, W. ; Grosvenor, R.L. ; Prickett, P.W.  
 Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on  
 Volume: 1  
 Digital Object Identifier: 10.1109/ETFA.2005.1612639  
 Publication Year: 2005, Page(s): 4 pp. - 1046  
 IEEE CONFERENCE PUBLICATIONS

**An architecture for component evolution**

Ryan, A. ; Newmarch, J.  
 Consumer Communications and Networking Conference, 2005. CCNC. 2005 Second IEEE  
 Digital Object Identifier: 10.1109/CCNC.2005.1405220  
 Publication Year: 2005, Page(s): 498 - 503  
 IEEE CONFERENCE PUBLICATIONS

**The forcegrid: a buffer structure for haptic interaction with virtual elastic objects**

Mazzella, F. ; Montgomery, K. ; Lalonde, J.-C.  
 Robotics and Automation, 2002. Proceedings. ICRA '02. IEEE International Conference on  
 Volume: 1  
 Digital Object Identifier: 10.1109/ROBOT.2002.1013477  
 Publication Year: 2002, Page(s): 939 - 946 vol.1  
 Cited by 3  
 IEEE CONFERENCE PUBLICATIONS

**An analysis of the Slapper worm**

Arce, I. ; Levy, E.  
 Security & Privacy, IEEE  
 Volume: 1, Issue: 1  
 Digital Object Identifier: 10.1109/MSECP.2003.1177002  
 Publication Year: 2003, Page(s): 82 - 87  
 Cited by 19  
 IEEE JOURNALS & MAGAZINES

**Haptic media synchronization using time adjustment algorithm for noncollaborative telehaptics**

Wongwitt, O. ; Chira, S.  
 Mechatronics, 2005. ICM '05. IEEE International Conference on  
 Digital Object Identifier: 10.1109/ICMECH.2005.1529318  
 Publication Year: 2005, Page(s): 555 - 561  
 Cited by 2  
 IEEE CONFERENCE PUBLICATIONS

**A haptic virtual environment for industrial training**

Hosseini, M. ; Malric, F. ; Georganas, Nicolas D.  
 Haptic Virtual Environments and Their Applications, IEEE International Workshop 2002 HAVE  
 Digital Object Identifier: 10.1109/HAVE.2002.1106909  
 Publication Year: 2002, Page(s): 25 - 30  
 IEEE CONFERENCE PUBLICATIONS

**ANT-on-YARDS: FPGA/ MPU hybrid architecture for telecommunication data processing**

Tsutsui, A. ; Miyazaki, T.

Very Large Scale Integration (VLSI) Systems, IEEE Transactions on  
 Volume: 5 , Issue: 2  
 Digital Object Identifier: 10.1109/92.678868  
 Publication Year: 1998 , Page(s): 199 - 211  
 Cited by 2  
 IEEE JOURNALS & MAGAZINES

**Architecture and implementation of a remote management framework for dynamically reconfigurable devices**

Chakraborty, R ; Ottavanger, H.  
 Networks, 2002. ICON 2002. 10th IEEE International Conference on  
 Digital Object Identifier: 10.1109/ICON.2002.1039340  
 Publication Year: 2002 , Page(s): 375 - 380  
 Cited by 2  
 IEEE CONFERENCE PUBLICATIONS

**Update and implementation of H.262 remote device control protocol for multimedia conference**

Dong Su Seong  
 Industrial Electronics, 2001. Proceedings. ISIE 2001. IEEE International Symposium on  
 Volume: 1  
 Digital Object Identifier: 10.1109/ISIE.2001.931922  
 Publication Year: 2001 , Page(s): 394 - 398 vol.1  
 IEEE CONFERENCE PUBLICATIONS

**Study on web-based network electrical machine control**

Wu Zhuanfeng ; Liu Weiguo ; Zhou Kiwei ; Ma Xin  
 Electrical Machines and Systems, 2005. ICEMS 2005. Proceedings of the Eighth International Conference on  
 Volume: 2  
 Digital Object Identifier: 10.1109/ICEMS.2005.202831  
 Publication Year: 2005 , Page(s): 1640 - 1643  
 IEEE CONFERENCE PUBLICATIONS

**A flexible architecture for remote server-based emulation**

Yan Gu ; Fujimoto, R.  
 Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, 2004. (MASCOTS 2004). Proceedings. The IEEE Computer Society's 12th Annual International Symposium on  
 Digital Object Identifier: 10.1109/MASCOT.2004.1348300  
 Publication Year: 2004 , Page(s): 447 - 454  
 Cited by 1  
 IEEE CONFERENCE PUBLICATIONS

< First | 1 | 2 | 3 | 4 | 5 | >> Last >

[Sign In](#) | [Create Account](#)

**IEEE Account**

[Change Username/Password](#)  
[Update Address](#)

**Purchase Details**

[Payment Options](#)  
[Order History](#)  
[Access Purchased Documents](#)

**Profile Information**


[Communications Preferences](#)  
[Profession and Education](#)  
[Technical Interests](#)

**Need Help?**

[US & Canada: +1 800 678 4330](#)  
[Worldwide: +1 732 981 0000](#)  
[Contact & Support](#)

[About IEEE Xplore](#) | [Contact](#) | [Help](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Site Map](#) | [Privacy & Opting Out of Cookies](#)

A non-profit organization, IEEE is the world's largest professional association for the advancement of technology.  
 © Copyright 2013 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions


<b><i>Issue Classification</i></b> 	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

CPC			Type	Version
Symbol				

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version


US ORIGINAL CLASSIFICATION			INTERNATIONAL CLASSIFICATION									
CLASS		SUBCLASS	CLAIMED					NON-CLAIMED				
709		220	G	0	6	F	15 / 177 (2006.01.01)					
<b>CROSS REFERENCE(S)</b>												
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											
709	201	202	203	224	225							
709	227											

/ANTHONY MEJIA/ Examiner, Art Unit 2451	04/22/2013	<b>Total Claims Allowed:</b>	
(Assistant Examiner)	(Date)	50	
(Primary Examiner)	(Date)	O.G. Print Claim(s)	O.G. Print Figure
		1	1

<b>Issue Classification</b> 	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

717	101	102																	
707	203																		
718	101																		
726	1																		
706	46																		

/ANTHONY MEJIA/ Examiner.Art Unit 2451  (Assistant Examiner)	04/22/2013  (Date)	<b>Total Claims Allowed:</b>  50	
(Primary Examiner)	(Date)	O.G. Print Claim(s)  1	O.G. Print Figure  1

<b>Issue Classification</b> 	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant		<input type="checkbox"/> CPA		<input checked="" type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47									
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	16	17	32	33	48	49								
2	2	17	18	33	34	49	50								
3	3	18	19	34	35	50	51								
	4	19	20	35	36		52								
4	5	20	21	36	37										
5	6	21	22	37	38										
6	7	22	23	38	39										
7	8	23	24	39	40										
8	9	24	25	40	41										
9	10	25	26	41	42										
10	11	26	27	42	43										
11	12	27	28	43	44										
12	13	28	29	44	45										
13	14	29	30	45	46										
14	15	30	31	46	47										
15	16	31	32	47	48										

/ANTHONY MEJIA/ Examiner, Art Unit 2451  (Assistant Examiner)	04/22/2013  (Date)	<b>Total Claims Allowed:</b>  50	
(Primary Examiner)	(Date)	O.G. Print Claim(s)  1	O.G. Print Figure  1



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7650

<b>SERIAL NUMBER</b> 12/189,788	<b>FILING or 371(c) DATE</b> 08/12/2008 <b>RULE</b>	<b>CLASS</b> 709	<b>GROUP ART UNIT</b> 2451	<b>ATTORNEY DOCKET NO.</b> ICON.P001D3
------------------------------------	---	---------------------	-------------------------------	---

**APPLICANTS**

Marc Baum, San Jose, CA;  
 Paul J. Dawes, Woodside, CA;  
 Mike Kinney, Foster city, CA;  
 Reza Raji, Menlo Park, CA;  
 David Swenson, Glyndon, MN;  
 Aaron Wood, Boulder Creek, CA;

**\*\* CONTINUING DATA \*\*\*\*\***

This application is a DIV of 12/189,757 08/11/2008 which claims benefit of 60/968,005 08/24/2007 and claims benefit of 60/987,359 11/12/2007 and claims benefit of 60/987,366 11/12/2007 and claims benefit of 61/019,162 01/04/2008 and claims benefit of 61/019,167 01/04/2008 and claims benefit of 61/023,489 01/25/2008 and claims benefit of 61/023,493 01/25/2008 and claims benefit of 61/023,496 01/25/2008 and claims benefit of 61/087,967 08/11/2008 and is a CIP of 11/084,232 03/16/2005 PAT 8335842 and is a CIP of 11/761,718 06/12/2007 PAT 7711796 and is a CIP of 11/761,745 06/12/2007 and is a CIP of 12/019,554 01/24/2008 PAT 7911341 and is a CIP of 12/019,568 01/24/2008

**\*\* FOREIGN APPLICATIONS \*\*\*\*\***

**\*\* IF REQUIRED, FOREIGN FILING LICENSE GRANTED \*\* \*\* SMALL ENTITY \*\***

Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Met after Allowance	<b>STATE OR COUNTRY</b>	<b>SHEETS DRAWINGS</b>	<b>TOTAL CLAIMS</b>	<b>INDEPENDENT CLAIMS</b>
35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Initials	CA	14	5+ 50	4
Verified and Acknowledged <u>/ANTHONY MEJIA/</u> Examiner's Signature					


**ADDRESS**

Gregory & Sawrie LLP  
 2018 Bissonnet Street  
 Houston, TX 77005  
 UNITED STATES

**TITLE**

Forming A Security Network Including Integrated Security System Components and Network Devices

<b>FILING FEE</b>	FEES: Authority has been given in Paper	<input type="checkbox"/> All Fees
		<input type="checkbox"/> 1.16 Fees (Filing)
		<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)

<b>Index of Claims</b> 	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>


<b>N</b>	<b>Non-Elected</b>
<b>I</b>	<b>Interference</b>

<b>A</b>	<b>Appeal</b>
<b>O</b>	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010	04/26/2011	04/29/2011	12/19/2011	09/25/2012	04/22/2013		
1	1	✓	✓	✓	✓	✓	=		
2	2	✓	✓	✓	✓	✓	=		
3	3	✓	✓	✓	✓	✓	=		
	4	✓	✓	-	-	-	-		
4	5	✓	✓	✓	✓	✓	=		
5	6	✓	✓	✓	✓	✓	=		
6	7	✓	✓	✓	✓	✓	=		
7	8	✓	✓	✓	✓	✓	=		
8	9	✓	✓	✓	✓	✓	=		
9	10	✓	✓	✓	✓	✓	=		
10	11	✓	✓	✓	✓	✓	=		
11	12	✓	✓	✓	✓	✓	=		
12	13	✓	✓	✓	✓	✓	=		
13	14	✓	✓	✓	✓	✓	=		
14	15	✓	✓	✓	✓	✓	=		
15	16	✓	✓	✓	✓	✓	=		
16	17	✓	✓	✓	✓	✓	=		
17	18	✓	✓	✓	✓	✓	=		
18	19	✓	✓	✓	✓	✓	=		
19	20	✓	✓	✓	✓	✓	=		
20	21	✓	✓	✓	✓	✓	=		
21	22	✓	✓	✓	✓	✓	=		
22	23	✓	✓	✓	✓	✓	=		
23	24	✓	✓	✓	✓	✓	=		
24	25	✓	✓	✓	✓	✓	=		
25	26	✓	✓	✓	✓	✓	=		
26	27	✓	✓	✓	✓	✓	=		
27	28	✓	✓	✓	✓	✓	=		
28	29	✓	✓	✓	✓	✓	=		
29	30	✓	✓	✓	✓	✓	=		
30	31	✓	✓	✓	✓	✓	=		
31	32	✓	✓	✓	✓	✓	=		
32	33	✓	✓	✓	✓	✓	=		
33	34	✓	✓	✓	✓	✓	=		
34	35	✓	✓	✓	✓	✓	=		
35	36	✓	✓	✓	✓	✓	=		



<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

<b>N</b>	<b>Non-Elected</b>
<b>I</b>	<b>Interference</b>

<b>A</b>	<b>Appeal</b>
<b>O</b>	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010	04/26/2011	04/29/2011	12/19/2011	09/25/2012	04/22/2013		
36	37	✓	✓	✓	✓	✓	=		
37	38	✓	✓	✓	✓	✓	=		
38	39	✓	✓	✓	✓	✓	=		
39	40	✓	✓	✓	✓	✓	=		
40	41	✓	✓	✓	✓	✓	=		
41	42	✓	✓	✓	✓	✓	=		
42	43	✓	✓	✓	✓	✓	=		
43	44	✓	✓	✓	✓	✓	=		
44	45	✓	✓	✓	✓	✓	=		
45	46	✓	✓	✓	✓	✓	=		
46	47	✓	✓	✓	✓	✓	=		
47	48	✓	✓	✓	✓	✓	=		
48	49	✓	✓	✓	✓	✓	=		
49	50	✓	✓	✓	✓	✓	=		
50	51	✓	✓	✓	✓	✓	=		
	52					✓	-		

<b>Search Notes</b>  	<b>Application/Control No.</b>  12189788	<b>Applicant(s)/Patent Under Reexamination</b>  BAUM ET AL.
	<b>Examiner</b>  ANTHONY MEJIA	<b>Art Unit</b>  2451

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
709	201, 202, 203, 224, 225, 227	5/2/2013	A.M.
717	101, 102	5/2/2013	A.M.
707	203	5/2/2013	A.M.
718	101	5/2/2013	A.M.
726	1	5/2/2013	A.M.
706	46	5/2/2013	A.M.

SEARCH NOTES		
Search Notes	Date	Examiner
EAST Class Limited w/Text Search (See Search History)	5/2/2013	A.M.
EAST Text Search (See Search History)	5/2/2013	A.M.
EAST Assignee Search (See Search History)	08/23/2010	A.M.
EAST Inventor Search (See Search History)	08/23/2010	A.M.
ALL EAST Searches Using: US-PGPUB, USPAT, USOCR, FPRS, JPO, EPO, DERWENT, IBM_TDB	5/2/2013	A.M.
NPL Search (See ACM and IEEE Search History)	5/2/2013	A.M.
Consulted allowable subject matter in Claims 1 and 49-51 and subject matter disclosed in related application: 12/189, 780 w/ PE A.SALAD AU 2456	5/2/2013	A.M.

/ANTHONY MEJIA/ Examiner.Art Unit 2451	
---	--

**INTERFERENCE SEARCH**

<b>US Class/ CPC Symbol</b>	<b>US Subclass / CPC Group</b>	<b>Date</b>	<b>Examiner</b>
709	200	5/2/2013	

/ANTHONY MEJIA/  
Examiner.Art Unit 2451

### REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL (Submitted Only via EFS-Web)

Application Number	12/189,788	Filing Date	2008-08-12	Docket Number (if applicable)	ICON.P001D3	Art Unit	2451
First Named Inventor	Marc Baum			Examiner Name	Anthony Mejia		

**This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.**  
 Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

#### SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_

Other \_\_\_\_\_

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other \_\_\_\_\_

#### MISCELLANEOUS

Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months \_\_\_\_\_  
 (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

Other \_\_\_\_\_

#### FEES

**The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**

The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No \_\_\_\_\_

#### SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Patent Practitioner Signature

Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Richard L. Gregory, Jr./	Date (YYYY-MM-DD)	2013-04-10
Name	Richard L. Gregory, Jr.	Registration Number	42607

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12189788
<b>Filing Date:</b>	12-Aug-2008
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Filer:</b>	Richard L. Gregory/David Sawrie
<b>Attorney Docket Number:</b>	ICON.P001D3

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				
Extension - 3 months with \$0 paid	2253	1	700	700

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
RCE - 2nd and Subsequent Request	2820	1	850	850
<b>Total in USD (\$)</b>				<b>1550</b>



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	15486668
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	98195
<b>Filer:</b>	Richard L. Gregory/David Sawrie
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	10-APR-2013
<b>Filing Date:</b>	12-AUG-2008
<b>Time Stamp:</b>	18:43:20
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1550
RAM confirmation Number	5578
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / zip (if appl.)	Pages (if appl.)
		SecureNet Technologies, LLC Exhibit 1003			Page 65

1		P001D3_filed_response_10APR2013.pdf	3562905 e9bdb33ff5164d87be8dc38abf1dad1044555990	yes	25
<b>Multipart Description/PDF files in .zip description</b>					
		<b>Document Description</b>	<b>Start</b>	<b>End</b>	
		Amendment Submitted/Entered with Filing of CPA/RCE	1	1	
		Claims	2	11	
		Applicant Arguments/Remarks Made in an Amendment	12	23	
		Extension of Time	24	25	
<b>Warnings:</b>					
<b>Information:</b>					
2	Request for Continued Examination (RCE)	ICON_P001D3_RCE_10APR2013.pdf	697839 5342ac463f3943a57c7dfa6e1738ad11a100cc9c	no	3
<b>Warnings:</b>					
<b>Information:</b>					
3	Fee Worksheet (SB06)	fee-info.pdf	32104 0b89123689f45cd83c429b7cf39fa700b22bdc3	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			4292848		
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					

IN THE UNITED STATES PATENT OFFICE

In Re Application of: )  
 )  
 Marc Baum, et al. ) Examiner: Anthony Mejia  
 ) Art Unit: 2451  
 )  
 Application No.: 12/189,788 )  
 )  
 Filed: August 12, 2008 )  
 )  
 For: FORMING A SECURITY NETWORK )  
 INCLUDING INTEGRATED SECURITY )  
 SYSTEM COMPONENTS AND NETWORK )  
 DEVICES )

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE

Sir:

Applicant respectfully requests consideration of the following amendments and remarks contained herein in response to the Office Action mailed October 10, 2012.

AMENDMENTS

IN THE CLAIMS

1. (Currently amended) A method comprising:
  - coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components;
  - automatically discovering the plurality of security system components at the gateway and establishing ~~communications~~ a first communication channel between the gateway and the plurality of security system components;
  - automatically discovering a ~~plurality of premise network~~ plurality of premise network devices at the gateway and establishing ~~communications~~ a second communication channel between the gateway and the ~~plurality of premise network~~ plurality of premise network devices, wherein the second communication channel is independent of the first communication channel; and
  - forming a security network by electronically integrating into the gateway communications and functions of the ~~plurality of premise network~~ plurality of premise network devices and the plurality of security system components, ~~wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server~~;
  - receiving at the gateway security data from the plurality of security system components, device data of the network devices, and remote data from the security server;
  - generating processed data by processing at the gateway the security data, the device data, and the remote data;
  - determining a state change of the security system using the processed data; and
  - maintaining at the security server with use of the processed data objects corresponding to the plurality of security system components and the network devices.

2. (Original) The method of claim 1, comprising controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device.

3. (Original) The method of claim 2, wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

Claim 4 (Canceled).

5. (Previously presented) The method of claim 1, comprising using protocols of the security system to discover the security system components, wherein the gateway includes the protocols of the security system.

6. (Previously presented) The method of claim 1, comprising the gateway receiving protocols of the security system from the security server in response to a request, wherein the gateway uses the protocols received to discover the security system components.

7. (Original) The method of claim 1, wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components.

8. (Currently amended) The method of claim 7, wherein the connection management component automatically discovers the ~~plurality of premise network~~ devices.

9. (Currently amended) The method of claim 7, wherein the connection management component automatically installs the ~~plurality of premise~~ network devices in the security network.

10. (Currently amended) The method of claim 7, wherein the connection management component automatically configures the ~~plurality of premise~~ network devices for operation in the security network.

11. (Currently amended) The method of claim 1, wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the ~~plurality of premise~~ network devices.

12. (Currently amended) The method of claim 1, wherein the gateway includes a device connect component that includes definitions of the security system components and the ~~plurality of premise~~ network devices.

13. (Original) The method of claim 1, wherein the premise local area network is coupled to a wide area network via a premise router.

14. (Original) The method of claim 1, wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network.

15. (Currently amended) The method of claim 1, wherein the gateway is coupled to the ~~plurality of premise~~ network devices using a wireless coupling.

16. (Original) The method of claim 1, wherein the gateway is coupled to the security server via the internet.

17. (Original) The method of claim 1, wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring

station is located at a third location different from the first location and the second location.

18. (Currently amended) The method of claim 1, wherein the security system is coupled to a central monitoring station via a ~~primary communication link~~ third communication channel, wherein the gateway is coupled to the central monitoring station via a ~~secondary communication link~~ fourth communication channel that is different than the ~~primary communication link~~ third communication channel.

19. (Currently amended) The method of claim 18, comprising transmitting event data of the security system components and the ~~plurality of premise~~ network devices to the central monitoring station via the gateway and the ~~secondary communication link~~ fourth communication channel.

20. (Currently amended) The method of claim 19, wherein the event data comprises changes in device states of at least one of security system components and ~~plurality of~~ premise network devices, data of at least one of security system components and ~~plurality of~~ premise network devices, and data received by at least one of security system components and ~~plurality of~~ premise network devices.

21. (Currently amended) The method of claim 18, comprising transmitting event data of the security system to the central monitoring station via the gateway and the ~~secondary communication link~~ fourth communication channel when the ~~primary communication link~~ third communication channel is unavailable.

22. (Currently amended) The method of claim 18, wherein the ~~secondary communication link~~ fourth communication channel includes a broadband coupling.

23. (Currently amended) The method of claim 18, wherein the ~~secondary communication link~~ fourth communication channel includes a General Packet Radio Service (GPRS) coupling.
24. (Currently amended) The method of claim 18, comprising transmitting messages comprising event data of the security system components and the ~~plurality of premise network~~ network devices to remote client devices via the gateway and the ~~secondary communication link~~ fourth communication channel.
25. (Currently amended) The method of claim 24, wherein the event data comprises changes in device states of at least one of security system components and ~~plurality of premise network~~ premise network devices, data of at least one of security system components and ~~plurality of premise network~~ premise network devices, and data received by at least one of security system components and ~~plurality of premise network~~ premise network devices.
26. (Original) The method of claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.
27. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.
28. (Currently amended) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the ~~plurality of premise network~~ network devices.
29. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.



30. (Currently amended) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the ~~plurality of premise~~ network devices.

31. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the security system components.

32. (Currently amended) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the ~~plurality of premise~~ network devices.

33. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the security system components.

34. (Currently amended) The method of claim 1, wherein the security server manages access to current and logged state data for the ~~plurality of premise~~ network devices.

35. (Currently amended) The method of claim 1, wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the ~~IP~~ network devices.

36. (Original) The method of claim 1, wherein the security server manages communications with the security system components.

37. (Currently amended) The method of claim 1, wherein the security server manages communications with the ~~plurality of premise~~ network devices.

38. (Original) The method of claim 1, wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data.
39. (Original) The method of claim 38, wherein the notifications include one or more of short message service messages and electronic mail messages.
40. (Original) The method of claim 38, wherein the event data is event data of the security system components.
41. (Currently amended) The method of claim 38, wherein the event data is event data of the ~~plurality of premise~~ network devices.
42. (Currently amended) The method of claim 1, wherein the security server transmits event data of the security system components and the ~~plurality of premise~~ network devices to a central monitoring station of the security system over the ~~secondary communication link~~ fourth communication channel.
43. (Original) The method of claim 1, wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.
44. (Currently amended) The method of claim 1, wherein the ~~plurality of premise~~ network device is an Internet Protocol device.
45. (Currently amended) The method of claim 1, wherein the ~~plurality of premise~~ network device is a camera.
46. (Currently amended) The method of claim 1, wherein the ~~plurality of premise~~ network device is a touchscreen.

47. (Currently amended) The method of claim 1, wherein the ~~plurality of premise~~ network device is a device controller that controls an attached device.

48. (Currently amended) The method of claim 1, wherein the ~~plurality of premise~~ network device is a sensor.

49. (Currently amended) A method comprising:

forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, ~~the security system including that includes~~ security system components located at the first location, wherein the security server is located at a second location different from the first location; and

~~automatically discovering a plurality of premise network devices at the gateway and establishing a coupling between the gateway and the plurality of premise network devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise network devices and the security system components into the gateway and the security network, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server;~~

receiving at the gateway security data from the security system components, device data of the network devices, and remote data from the security server;

generating processed data by processing at the gateway the security data, the device data, and the remote data;

determining a state change of the security system using the processed data; and maintaining at the security server with use of the processed data objects corresponding to the plurality of security system components and the network devices.

50. (Currently amended) A method comprising:

automatically discovering a security system at a gateway and establishing communications between the gateway and the security system in a facility, wherein the

security system includes a plurality of security system components that are proprietary to the security system; and

automatically discovering a plurality of network devices at the gateway and establishing communications between the gateway and the plurality of network devices, wherein the gateway forms a ~~premise~~ security network at the facility and couples the ~~premise~~ security network to a local area network of the facility, wherein the gateway forms the ~~premise~~ security network by electronically integrating into the gateway communications and functions of the plurality of network devices and the plurality of security system components, ~~wherein objects corresponding to at least one of the plurality of security system components and the plurality of network devices are maintained on a remote server;~~

receiving at the gateway security data from the plurality of security system components, device data of the plurality of network devices, and remote data from the remote server;

generating processed data by processing at the gateway the security data, the device data, and the remote data;

determining a state change of the security system using the processed data; and maintaining at the remote server with use of the processed data objects corresponding to the plurality of security system components and the plurality of network devices.

51. (Currently amended) A method comprising:

forming a security network by automatically discovering a security system at a gateway and establishing communications between the gateway and the security system, the security system including security system components installed at a facility, wherein the gateway is located at a first location, wherein the gateway is coupled to a security server at a second location different than the first location;

automatically discovering a plurality of network devices at the gateway and establishing communications between the security network and the plurality of network devices located at the facility, the gateway electronically integrating communications and

functions of the plurality of network devices and the security system components into the gateway and the security network; and

receiving at the gateway security data from the security system components, device data of the plurality of network devices, and remote data from the security server;

generating processed data by processing at the gateway the security data, the device data, and the remote data;

determining a state change of the security system using the processed data;

maintaining at the security server with use of the processed data objects corresponding to the plurality of security system components and the network devices;

and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the plurality of network devices, ~~wherein objects corresponding to at least one of the security system components and the plurality of network devices are maintained on the security server.~~

Claim 52 (Canceled).

REMARKS

Claims 1-3 and 5-52 are pending in the application. Claims 1-3 and 5-52 are rejected. Claims 1, 8-12, 15, 18-25, 28, 30, 32, 34, 35, 37, 41, 42, and 44-51 are amended herein. Claim 52 is canceled without prejudice herein. No new matter is added by the amendments and remarks presented herein.

Request for Continued Examination under 37 C.F.R. 1.114

This response is accompanied by a Request for Continued Examination under 37 C.F.R. 1.114 and the required fee.

Petition For Extension Of Time

A Petition For Extension Of Time Under 37 CFR 1.136(a) is submitted herewith along with the appropriate fee amount for a three (3) month extension of time.

Priority

Applicant respectfully submits that the disclosure of the prior-filed application, Application Number 11/084,232 filed on March 16, 2005, provides adequate support or enablement for claims 1, 60 and 61 as presented herein. In particular, and with reference to US Patent Application Publication Number US 2005/0216580 A1 (now US Patent Number 8,335,842), which corresponds to Application Number 11/084,232, support for the claims is found at least at paragraphs [0026], [0036], [0078-0091], [0114-0145], [0176-0179], [0226-0231], [0333-0358], [0370-0380], [0392-0396], [0447], [0451], [0453], [0455-0460], [0463], [0464], and figures 1 and 5-8.

Rejections under 35 U.S.C. §112

Claim 52 is rejected under 35 U.S.C. §112, first paragraph as failing to comply with the written description requirement. Claim 52 is canceled without prejudice herein. Therefore, Applicant respectfully requests withdrawal of this rejection.

Rejections under 35 U.S.C. §103

Claims 1-3, 5-9, 11, 12, 15-25, 28, 30-45 and 48 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo et al., United States (US) Patent Application Publication Number US 2003/0062997 A1 (“Naidoo”), in view of Bilger, US Patent Number 6,756,998 (“Bilger”), and further in view of Rezvani et al., US Patent Number 6,686,838 (“Rezvani”). Applicant respectfully submits that the claims as amended herein are patentably distinct from Naidoo, Bilger and/or Rezvani. Moreover, Naidoo, Bilger and/or Rezvani fail to teach each and every element of claims 1-3, 5-9, 11, 12, 15-25, 28, 30-45, and 48 as presented herein.

The Office Action states at page 6 that Naidoo does not explicitly teach the step of "automatically discovering security system components". Applicant agrees.

The Office Action states at page 7 that Naidoo and Bilger do not explicitly teach the step of "automatically discovering a plurality of premise devices at a gateway". Applicant agrees.

Regarding claim 1 as amended herein, Applicant respectfully submits that Naidoo describes a system and method for distributed monitoring and remote verification of conditions surrounding an alarm condition in a security system (abstract). Naidoo describes that the security system includes a security gateway, which is typically located at the desired premises to be monitored, and a monitoring client, typically located at a central station and operatively coupled to security gateway through a network. Naidoo describes that often, the security gateway is located at the target site, however, on some occasions, some or all components of security gateway may be located remotely, but remain operatively coupled to security sensors and video cameras which are at the premises (paragraph 0028).

Naidoo describes that the security gateway is a processor-based device that functions to detect alarm conditions at a target site and to capture information relating to such alarm conditions (paragraph 0032). Naidoo describes that, upon detection of an alarm condition, the security gateway captures video (usually through an attached video camera) of the target site, and sends the video to security system server in real time (paragraph 0028).

Naidoo describes that a monitoring client is generally a software program that may be used to display some or all of the information provided by security gateway. Monitoring client may be a stand-alone program or integrated into one or more existing software programs. Naidoo describes that one or more operators may then use this information to evaluate whether the alarm condition corresponds to an actual alarm condition and then take additional action, if desired, such as alerting the appropriate authorities (paragraph 0032).

Naidoo describes that the security system includes one or more sensors coupled to security gateway for the purpose of detecting alarm conditions. The security system is not limited to any specific type or model of sensor. Any sensor may be used, depending on the desired type and level of protection. Alarm sensors may be wired directly into an alarm control panel built into the security gateway or they may be wirelessly connected (paragraph 0033). Naidoo describes that the security system also includes one or more video cameras that are operable to capture video data of monitored premises. Naidoo describes that the security gateway may be configured to create an association between one or more sensors and an associated video camera (paragraph 0034).

Regarding claim 1, as amended, Applicant respectfully submits that Naidoo does not disclose coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components, forming a security network by electronically integrating into the gateway-communications and functions of the network devices and the plurality of security system components, receiving at the gateway security data from the plurality of security system components, device data of the network devices, and remote data from the security server, generating processed data by processing at the gateway the security data, the device data, and the remote data, determining a state change of the security system using the processed data, and maintaining at the security server with use of the processed data objects corresponding to the plurality of security system components and the network devices (emphasis added).

As set forth above, Naidoo describes that the security gateway is a processor-based device that functions to detect alarm conditions at a target site and to capture



information relating to such alarm conditions (paragraph 0032). Naidoo describes that, upon detection of an alarm condition, the security gateway captures video (usually through an attached video camera) of the target site, and sends the video to security system server in real time (paragraph 0028).

Naidoo describes that a monitoring client is generally a software program that may be used to display some or all of the information provided by security gateway. Monitoring client may be a stand-alone program or integrated into one or more existing software programs. Naidoo describes that one or more operators may then use this information to evaluate whether the alarm condition corresponds to an actual alarm condition and then take additional action, if desired, such as alerting the appropriate authorities (paragraph 0032). Therefore, Naidoo simply describes a security gateway that detects alarm conditions at a target site and forwards the detected conditions and related information to a security system server whereupon a monitoring client displays some or all of alarm condition information. Naidoo nowhere teaches coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components, forming a security network by electronically integrating into the gateway-communications and functions of the network devices and the plurality of security system components, receiving at the gateway security data from the plurality of security system components, device data of the network devices, and remote data from the security server, generating processed data by processing at the gateway the security data, the device data, and the remote data, determining a state change of the security system using the processed data, and maintaining at the security server with use of the processed data objects corresponding to the plurality of security system components and the network devices.

For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo. Applicant finds no teaching in Bilger and Rezvani to overcome the deficiencies of Naidoo set forth above.

Applicant respectfully submits that Bilger describes a home automation system interface and method for interfacing with a system that automatically controls controlled

devices throughout a home. A unique architecture of occupancy sensors includes entry/exit sensors for detecting movement through doorways that separate rooms in the home, room motion sensors for detecting room occupancy, spot sensors to detect occupancy of specific locations within the rooms, and house status sensors to detect the status of certain parameters of the home. A central controller communicates with the sensors and controlled objects over a communications network, where the sensors and controlled objects can be added to the system in a 'plug and play manner (abstract).

Figure 7 A of Bilger illustrates the preferred configuration for network 14, which includes a control/sensor network 52 wired to each "room" 4 in the house. Control/sensor network 52 is a single set of wires bused throughout the house, preferably while the house is under initial construction. Once the AC power lines are installed but before the walls are completed, the network wiring can be easily installed in just one day, often times using the same holes, conduit and/or junction boxes as the AC lines. The control/sensor network 52 is connected to all the sensors 10 and controlled objects 12, as well as to the central controller 16 (column 9, lines 56-66).

Figure 7A of Bilger illustrates a random configuration for control/sensor network 52. Figures 7B-7D of Bilger illustrate alternate configurations for routing control/sensor network 52 through the house. A single set of wires can be woven throughout the house in a straight bus or daisy chain configuration, as illustrated in Figure 7B of Bilger. The central controller could have one 15 or more central hubs 58 that have individual communications lines 60 each connected to a single sensor 10 or controlled object 12, as illustrated in Figure 7C of Bilger. The advantage of this embodiment is that the sensors 10 and controlled objects 12 can use standard Ethernet twisted pair connectors and hubs, but the drawback is that the system is less versatile, and more costly to wire. Alternately, the control/sensor network 52 could be wireless, where each sensor 10 and controlled object 12 including a transceiver 54 that communicates with one or more central transceivers 56 of the central controller 16 (as illustrated in Figure 7D of Bilger), or with other transceivers 54 in a token bus configuration (as illustrated in Figure 7E of Bilger). Lastly, control/sensor network 52 could be a powerline based system (e.g. X-10 system), where the sensors 10 controlled objects 12 and central controller 16 communicate with

each other over the existing AC power lines in the house (column 10, lines 9-31).

Therefore, in contrast to amended claim 1, Bilger does not teach coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components, forming a security network by electronically integrating into the gateway-communications and functions of the network devices and the plurality of security system components, receiving at the gateway security data from the plurality of security system components, device data of the network devices, and remote data from the security server, generating processed data by processing at the gateway the security data, the device data, and the remote data, determining a state change of the security system using the processed data, and maintaining at the security server with use of the processed data objects corresponding to the plurality of security system components and the network devices (emphasis added).

Applicant respectfully submits that Rezvani describes systems and methods for providing registration at a remote site that may include, for example, a monitoring module that may communicate with a remote site (abstract). Devices at one or more locations may interface with the monitoring modules. Rezvani describes that one or more monitoring modules and their associated interfaced devices may be referred to as "installations." Devices may include, for example, video cameras, still cameras, motion sensors, audible detectors, any suitable household appliances, or any other suitable device. Rezvani describes that monitoring modules may be stand-alone devices, software applications, any suitable combination of software and hardware, or any other suitable architecture (column 1, lines 41-50).

Rezvani describes that monitoring modules may communicate with one or more remote sites via a suitable communications network using any suitable communications protocol. The monitoring modules and remote sites may use a registration protocol to transmit registration information. The registration information may get stored in a database at the remote site (column 1, lines 51-56).

Rezvani describes that an installation, any of its components, or both may be associated with a particular user account (column 1, lines 59-60). Association of an

installation, installation elements, or both with corresponding user accounts may take place at the remote site. The remote site may make the association using any suitable database construct that may serve to cross reference the installation, installation elements, or both with user accounts (column 1, line 65 to column 2, line 3).

Rezvani describes that devices may be automatically detected by a monitoring module (column 2, lines 37-38). Rezvani describes that as new devices are added to a registered monitoring module, the monitoring module may automatically (i.e., without any user interaction) detect the presence of the new devices and automatically notify remote site of the presence of the new devices. Remote site may, in turn, add the new devices to the database (column 21, lines 5-11).

Although Rezvani discloses the automatic detection of devices, the detected device information is directed to and registered at a remote site. Rezvani teaches automatically detecting a device at an installation, extracting registration information from the device, communicating the registration information to a remote site that does not have requisite registration information associated with the device using a communications network, registering the device with the remote site based on the registration information, and associating the device at the remote site with a user account based on the registration information (claim 1, column 21, lines 41-53). Rezvani therefore teaches the automatic detection and extraction of registration information from devices at a first location (an installation), the communication of the registration information to a remote location, registration of devices at the remote location using the extracted information and the association of the devices at the remote site with a user account.

However, in contrast to amended claim 1, Rezvani does not teach coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components, forming a security network by electronically integrating into the gateway-communications and functions of the network devices and the plurality of security system components, receiving at the gateway security data from the plurality of security system components, device data of the network devices, and

remote data from the security server, generating processed data by processing at the gateway the security data, the device data, and the remote data, determining a state change of the security system using the processed data, and maintaining at the security server with use of the processed data objects corresponding to the plurality of security system components and the network devices (emphasis added).

Therefore, none of Naidoo, Bilger and Rezvani teaches coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components, forming a security network by electronically integrating into the gateway-communications and functions of the network devices and the plurality of security system components, receiving at the gateway security data from the plurality of security system components, device data of the network devices, and remote data from the security server, generating processed data by processing at the gateway the security data, the device data, and the remote data, determining a state change of the security system using the processed data, and maintaining at the security server with use of the processed data objects corresponding to the plurality of security system components and the network devices (emphasis added). For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo in view of Bilger and Rezvani.

As claims 2-3, 5-9, 11, 12, 15-25, 28, 30-45, and 48 depend from amended claim 1 and include further limitations thereon, and since amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani, Applicant submits that claims 2-3, 5-9, 11, 12, 15-25, 28, 30-45, and 48 are patentable over by Naidoo in view of Bilger and further in view of Rezvani.

Claims 10 and 29 are rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Tanaka et al., US Patent Application Publication number US 2004/0037295 A1 (“Tanaka”).

The Office Action states at pages 17-18 that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the connection management component automatically configures the premise devices for operation in the security network". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to

amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claims 10 and 29 which depend from amended claim 1, Applicant does not find any teaching in Tanaka that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 10 and 29 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Tanaka and respectfully requests that the rejection be withdrawn and allowance thereof.

Claim 26 is rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Patterson, US Patent Application Publication number US 2005/0086126 A1 (“Patterson”).

The Office Action states at page 19 that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the security server creates, modifies and terminates users corresponding to the security system". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claim 26 which depends from amended claim 1, Applicant does not find any teaching in Patterson that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claim 26 is patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Patterson and respectfully requests that the rejection be withdrawn and allowance thereof.

Claim 27 is rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moyer et al., US Patent Application Publication number US 2002/0103898 A1 (“Moyer”).

The Office Action states at page 20 that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the security server creates, modifies and terminates couplings

between the gateway and the security system components". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claim 27 which depends from amended claim 1, Applicant does not find any teaching in Moyer that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claim 27 is patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moyer and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 46-47 are rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Lingemann, US Patent Application Publication number US 2006/0009863 A1 ("Lingemann").

The Office Action states at page 21 that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the network device is a touchscreen". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claims 46-47 which depend from amended claim 1, Applicant does not find any teaching in Lingemann that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 46-47 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Lingemann and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 13-14 are rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moore et al., US Patent Application Publication number US 2007/0061266 A1 ("Moore").

The Office Action states at page 22 that Naidoo/Bilger/Rezvani does not

explicitly disclose "the premise local area network is coupled to a wide area network via a premise router". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claims 13-14 which depend from amended claim 1, Applicant does not find any teaching in Moore that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 13-14 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moore and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 49-51 are rejected as being unpatentable over Naidoo in view of Rezvani.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo in view of Rezvani does not teach or suggest each and every limitation of amended claim 49 and, as such, amended claim 49 is patentable over Naidoo in view of Rezvani. For at least these reasons, Applicant submits that amended claim 49 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and allowance therefore.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo in view of Rezvani does not teach or suggest each and every limitation of amended claim 50 and, as such, amended claim 50 is patentable over Naidoo in view of Rezvani. For at least these reasons, Applicant submits that amended claim 50 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and allowance therefore.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo in view of Rezvani does not teach or suggest each and every limitation of amended claim 51 and, as such, amended claim 51 is patentable over Naidoo in view of Rezvani. For at least these reasons, Applicant submits that amended claim 51 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection



be withdrawn and allowance therefore.

Further regarding claims 49-51, the Office Action states at pages 24, 26 and 27 that Naidoo does not explicitly teach the step of "automatically discovering the plurality of network devices at the gateway". Applicant agrees.

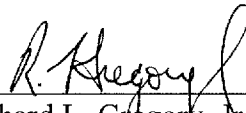
Claim 52 is rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Dale et al., US Patent Number 7,681,201 ("Dale"). Claim 52 is canceled without prejudice herein. Therefore, Applicant respectfully requests withdrawal of this rejection.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully submit that the rejections under 35 U.S.C. §103 and §112 have been overcome, and their withdrawal is respectfully requested. Applicants submit that claims 1-3 and 5-51 are in condition for allowance. The allowance of the claims is earnestly requested. If in the opinion of Examiner MEJIA a telephone conference would expedite the prosecution of the subject application, or if there are any issues that remain to be resolved prior to allowance of the claims, Examiner MEJIA is encouraged to call (408.821.8080) or email (rick@iprlaw.com) Rick Gregory.

Date: April 10, 2013

Respectfully submitted,  
GREGORY & SAWRIE LLP



Richard L. Gregory, Jr., Reg. No. 42,607  
Telephone: 408.821.8080  
Email: rick@iprlaw.com

GREGORY & SAWRIE LLP  
2018 Bissonnet Street  
Houston, Texas 77005  
Fax: 713-364-1397

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b>		Docket Number (Optional) <b>ICON.P001D3</b>
Application Number <b>12/189,788</b>	Filed <b>August 12, 2008</b>	
For <b>Forming A Security Network Including Integrated Security System Components and Network Devices</b>		
Art Unit <b>2451</b>	Examiner <b>MEJIA, Anthony</b>	
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.		
The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):		
	<u>Fee</u>	<u>Small Entity Fee</u>
<input type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$200	\$100
<input type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$600	\$300
<input checked="" type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$1,400	\$700
<input type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$2,200	\$1,100
<input type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$3,000	\$1,500
<input checked="" type="checkbox"/> Applicant asserts small entity status. See 37 CFR 1.27.		
<input type="checkbox"/> Applicant certifies micro entity status. See 37 CFR 1.29. <small>Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.</small>		
<input type="checkbox"/> A check in the amount of the fee is enclosed.		
<input checked="" type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.		
<input type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.		
<input type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number _____		
<input type="checkbox"/> Payment made via EFS-Web.		
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>		
I am the		
<input type="checkbox"/> applicant/inventor.		
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).		
<input checked="" type="checkbox"/> attorney or agent of record. Registration number <u>42,607</u>		
<input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number _____		
<u>/Richard L. Gregory, Jr./</u>	<b>+</b>	<u>April 10, 2013</u>
Signature		Date
<u>Richard L. Gregory, Jr.</u>		<u>408-821-8080</u>
Typed or printed name		Telephone Number
<b>NOTE:</b> This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.		
<input checked="" type="checkbox"/> * Total of <u>1</u> forms are submitted.		

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/189,788</b>	Filing Date <b>08/12/2008</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

ENTITY:  LARGE  SMALL  MICRO

**APPLICATION AS FILED – PART I**

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

**APPLICATION AS AMENDED – PART II**

AMENDMENT	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	<b>04/10/2013</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR			
	Total (37 CFR 1.16(i))	* 50	Minus	** 51	= 0	X \$40 = 0
	Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X \$210 = 0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
					TOTAL ADD'L FEE	<b>0</b>

AMENDMENT	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR			
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
					TOTAL ADD'L FEE	

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE  
 /PEARLIE A. FENNEL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**  
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**Office Action Summary**

Application No.	12/189,788	Applicant(s)	BAUM ET AL.
Examiner	ANTHONY MEJIA	Art Unit	2451

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 07 July 2012.
- 2a)  This action is **FINAL**.                    2b)  This action is non-final.
- 3)  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 4)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 5)  Claim(s) 1-3 and 5-52 is/are pending in the application.  
5a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 6)  Claim(s) \_\_\_\_ is/are allowed.
- 7)  Claim(s) 1-3 and 5-52 is/are rejected.
- 8)  Claim(s) \_\_\_\_ is/are objected to.
- 9)  Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 10)  The specification is objected to by the Examiner.
- 11)  The drawing(s) filed on 24 November 2008 is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 13)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All   b)  Some \*   c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
  
\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 06/07/2012 and 10/15/2009.
- 4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date 09/18/2012.
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes details for Gregory & Sawrie LLP and examination information for MEJIA, ANTHONY.

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

- rick@iprlaw.com
david@iprlaw.com
vlad@iprlaw.com

<b>Applicant-Initiated Interview Summary</b>	<b>Application No.</b> 12/189,788	<b>Applicant(s)</b> BAUM ET AL.	
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451	

All participants (applicant, applicant's representative, PTO personnel):

- (1) ANTHONY MEJIA. (3) \_\_\_\_\_.
- (2) Richard L. Gregory, Jr. (Reg. No. 42,607). (4) \_\_\_\_\_.

Date of Interview: 18 September 2012.

Type:  Telephonic  Video Conference  
 Personal [copy given to:  applicant  applicant's representative]

Exhibit shown or demonstration conducted:  Yes  No.  
If Yes, brief description: N/A.

Issues Discussed 101 112 102 103 Others  
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1-3 and 5-52.

Identification of prior art discussed: N/A.

**Substance of Interview**

(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner contacted Applicant's attorney to discuss potential proposed amendments to help place application in conditions of allowance. Applicants agreed to accept the attached proposed amendments, however upon further consideration, Examiner was unable to find sufficient support in the specification, specifically at paragraphs 0110-0111, 0119-0122, 0133-0143, and 147-162 and corresponding figures as directed by applicants, for the amended/added limitation: "...executing the security system operating system on a gateway operating system of the gateway, wherein the security system operating system is required for basic operation of the security system, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server" as currently recited in Claims 1,49-51. Furthermore, the incorporation of said amendment of said limitation does not patentably distinguish the claims over the prior art of record. Therefore no agreements were made and Claims 1-3 and 5-52 are not in conditions for allowance .

**Applicant recordation instructions:** The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

**Examiner recordation instructions:** Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Attachment

/A. M./  
Examiner, Art Unit 2451

## Summary of Record of Interview Requirements

### Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

### Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,  
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

### Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.



## **DETAILED ACTION**

### ***Information Disclosure Statement***

1. The information disclosure statement filed **15 October 2009** and **07 June 2012** fail to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. Furthermore, the citations listed on pages 1 and 8 of the IDS submitted on 07 June 2012 and page 4 of the IDS submitted on 15 October 2009 is missing dates. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

### ***Response to Amendment***

2. Acknowledgement is made that Claim 4 has been canceled. Claim 52 has been added, and pending with Claims 1-3 and 5-51.

### ***Priority***

3. The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of the first paragraph of 35 U.S.C. 112. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

The disclosure of the prior-filed application, Application No. 12/189,757 filed on **11 August 2008**, fails to provide adequate support or enablement in the manner provided by the first paragraph of 35 U.S.C. 112 for one or more claims of this application. In this case as per Claim 52, Examiner fails to see wherein the specification discloses: “...*the forming a security networking including embedding an operating system of the security system in a component of the gateway*” as currently recited in the claim.

### ***Response to Arguments***

4. Applicant’s alleged arguments, see pages 10-22 of Remarks, filed, **17 July 2012**, with respect to Claims 1-3, 5-9, 11-12, 15-25, 28, 30-45 and 48 rejection under 35 U.S.C. 103(a) have been fully considered but are not persuasive.

As per Claims 1 and 49-51, Applicants argue that Naidoo does not disclose coupling a gateway to a local network located in a first location and a

Art Unit: 2451

security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added). Applicants further submit that Naidoo in view of Bilger and further in view of Rezvani still do not teach the argued limitation above.

As per applicant's arguments above, Examiner respectfully disagrees. Naidoo clearly teaches the step of: "...coupling a gateway to a local network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components..." Naidoo discloses a security system for monitoring a premises by integrating broadband features, including audio and video capabilities, web access and wireless capabilities which is typically located at the desired premises 110 to be monitored, and a monitoring client 133, typically located at a central station and operatively coupled to security gateway 115 through a network 120. Often, security gateway 115 is located at the target site. However, on some occasions, some or all components of security gateway 115 may be located remotely, but remain operatively coupled to security sensors 105 and video cameras 112 which are at the premises. Therefore, Naidoo clearly teaches that although the security gateway is typically located at a target site, the security gateway can be located at the premises and remained connected

Art Unit: 2451

(coupled) to that all of the components (security sensors 105 and video cameras 112) of the security system (see pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6). Therefore, Naidoo clearly teaches the argued limitation of: "...coupling a gateway to a local network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components..."

Furthermore, as per applicants arguments that Naidoo fails to teach, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server.

Naidoo teaches security gateway including an alarm control panel, video module, user interface, communications interface, and audio interface. As shown in fig.6, components of the gateway are configured to communicate with one another through system bus, some or all of the components of security gateway may be directly connected. For instance, the alarm control panel may be configured to communicate with the other components of the security system to monitor their operational state. Also, the video module 620 may is capable of streaming live audio and video from the residence during alarming conditions, in which the video module 620 may include a PC motherboard, hard disk drive, and a digital signal processor. The operating system for video module 620 is embedded WindowsNT. So when, the security system is armed, audio and video data are constantly being stored in the video module's memory for potential use (see pars [0079], [0081], [0083-0084] and see fig.6). Therefore, Naidoo clearly

Art Unit: 2451

teaches the limitation wherein objects corresponding to the security system components are maintained on the security server.

Examiner encourages applicants to also further consider newly discovered reference Dale et al. (US 7,681,201 B2) as discussed below in the rejection under 35 U.S.C. 103(a) to Claim 52 and to further consider newly discovered pertinent reference Tabe (US 2007/0256105 A1) before submitting next response to Office Action.

5. As per Claims 2-3, 5-9, 11-12, 15-25, 28, 30-45, and 48, Applicant's arguments are not persuasive as for the same reasons as discussed above.

***Claim Rejections - 35 USC § 112***

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claim 52 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. In this case, Examiner fails to see wherein the specification discloses: "...the forming a security networking including embedding an operating system of the security system in a component of the gateway" as currently recited in Claim 52.

Appropriate correction and/or explanation is required.

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1-3, 5-9, 11-12, 15-25, 28, 30-45, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo et al. (US 2003/0062997) (hereinafter as Naidoo) in further view of Bilger (US 6,756,998) and in further view of Rezvani et al. (US 6,686,838) (hereinafter as Rezvani).

Regarding Claim 1, Naidoo teaches a method comprising:

coupling a gateway to a local area network located in a first location and a security server in a second location (see figs.1-2), wherein the first location includes a security system comprising:

a plurality of security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the gateway and the security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

Art Unit: 2451

automatically establishing communications between the gateway and premise devices pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

forming a security network by electronically integrating, via the gateway, communications and functions of the plurality of premise devices and the security system components, (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

The teachings of Naidoo do not explicitly teach the step of *automatically discovering security system components*.

However, Bilger in a similar field of endeavor discloses a home automation system interface for interfacing with a system that automatically controls controlled devices throughout the home including the step of *automatically discovering security system components at the gateway* (e.g., control objects are plug and play compatible and are automatically recognized by the central controller once connected to the network, col.8, lines 55-67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Bilger in order Naidoo's components to automatically install devices to the security system. One of ordinary skill in the art would have been motivated because it would ease installation of components by automatically installing the device to the security system.

Art Unit: 2451

In further the combined teachings of Naidoo and Bilger do not explicitly teach the step of *automatically discovering a plurality of premise devices at a gateway*.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Regarding Claim 2, Naidoo further teaches the step of controlling the functions of the security network via an interface coupled to the security network,



Art Unit: 2451

wherein the interface is accessed using a remote client device (pars [0040-0041]).

Regarding Claim 3, Naidoo further teaches the step wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices (par [0040] and see fig.2).

Regarding Claim 5, Naidoo-Rezvani-Bilger discloses the method of claim 4, comprising using protocols of the security system to discover the security system components, wherein the gateway includes the protocols (see Rezvani; col. 2/lines 27-36; the remote sites may validate received registration protocol messages used during the new object discovery process to discovery new devices).

Regarding Claim 6, Naidoo-Rezvani-Bilger discloses the method of claim 4, comprising requesting and receiving protocols of the security system from the security server, wherein the gateway receives and uses the protocols to discover the security system components (see Rezvani; col. 2, lines 27-36; the remote sites may validate received registration protocol messages used during the new object discovery process to discovery new devices).

Art Unit: 2451

Regarding Claim 7, Naidoo further teaches the step wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components (pars [0069], [0079], and [0087]).

Regarding Claim 8, Naidoo further teaches the step wherein the connection management component automatically discovers the premise devices (par [0040] and see fig.2).

Regarding Claim 9, Bilger teaches Cross will automatically install sensor in the selected room (col. 20, lines 1-13).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Bilger in order Naidoo's components to automatically install devices to the security system. One of ordinary skill in the art would have been motivated because it would ease installation of components by automatically installing the device to the security system.

Regarding Claim 11, Naidoo further teaches the step wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices (par [0099]).

Regarding Claim 12, Naidoo further teaches the step wherein the gateway includes a device connect component that includes definitions of the security system components and the premise devices (pars [0080-0081]).

Regarding Claim 15, Naidoo further teaches the step wherein the gateway is coupled to the premise devices using a wireless coupling (par [0033]).

Regarding Claim 16, Naidoo further teaches the step wherein the gateway is coupled to the security server via the internet (par [0030]).

Regarding Claim 17, Naidoo further teaches the step wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location (par [0043] and see fig.2).

Regarding Claim 18, Naidoo further teaches wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link (par [0043] and see fig.2).

Regarding Claim 19, Naidoo further teaches the step of transmitting event data of the security system components and the premise devices to the central

Art Unit: 2451

monitoring station via the gateway and the secondary communication link (par [0043] and see fig.2).

Regarding Claim 20, Naidoo further teaches the step wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of:

security system components and premise devices, and data received by at least one of security system components and premise devices (pars [0069], and [0080-0081]).

Regarding Claim 21, Naidoo further teaches the step of transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable (par [0043]).

Regarding Claim 22, Naidoo further teaches wherein the secondary communication link includes a broadband coupling (pars [0027] and [0122]).

Regarding Claim 23, Naidoo further teaches the step wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling (par [0043]).

Regarding Claim 24, Naidoo further teaches the step of transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link (pars [0027-0028], [0043], and [0046]).

Regarding Claim 25, Naidoo further teaches wherein the event data comprises changes in device states of at least one of:

security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices (pars [0069], and [0080-0081]).

Regarding Claim 28, Naidoo further teaches wherein the security server creates modifies and terminates couplings between the gateway and the premise devices (pars [0099-0101]).

Regarding Claim 30, Naidoo further teaches wherein wherein the security server performs creation, modification, deletion and configuration of the premise devices (pars [0099-0101]).

Regarding Claim 31, Naidoo further teaches wherein the security server creates automations, schedules and notification rules associated with the security system components (par [0045]).

Regarding Claim 32, Naidoo further teaches wherein the security server creates automations, schedules and notification rules associated with the premise devices (pars [0027-0028] and [0045]).

Regarding Claim 33, Naidoo further teaches the step wherein the security server manages access to current and logged state data for the security system components (pars [0049-0050]).

Regarding Claim 34, Naidoo further teaches the step wherein the security server manages access to current and logged state data for the premise devices (pars [0027-0028] and [0049-0050]).

Regarding Claim 35, Naidoo further teaches the step wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices (pars [0027-0028] and [0049-0050]).

Regarding Claim 36, Naidoo further teaches the step wherein the security server manages communications with the security system components (par [0049]).

Regarding 37, Naidoo further teaches the step wherein the security server manages communications with the premise devices (pars [0027-0028] and [0049]).

Regarding 38, Naidoo further teaches the step wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data (par [0053]).

Regarding 39, Naidoo further teaches the step wherein the notifications include one or more of short message service messages and electronic mail messages (par [0069]).

Regarding Claim 40, Naidoo further teaches the step wherein the event data is event data of the security system components (par [0053]).

Regarding Claim 41, Naidoo further teaches the step wherein the event data is event data of the premise devices (pars [0027-0028] and [0053]).

Regarding Claim 42, Naidoo further teaches the step wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link (pars [0027-0028], [0043], and [0046]).

Regarding Claim 43, Naidoo further teaches the step wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers (par [0059]).

Regarding Claim 44, the method of claim 1, wherein the premise device is an Internet Protocol device (par [0037]).

Regarding Claim 45, Naidoo further teaches the step wherein the premise device is a camera (pars [0040-0041]).

Regarding Claim 48, Naidoo further teaches the step wherein the premise device is a sensor (pars [0040-0041]).

10. Claims 10 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Tanaka et al. (US 2004/0037295).

Regarding Claim 10, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of Claim 7, *wherein the connection management component*



Art Unit: 2451

*automatically configures the premise devices for operation in the security network.*

Tanaka in the field of the same endeavor teaches creating a virtual local area network using a graphical user interface. In particular, Tanaka teaches the server automatically creates configuration information of the switch (see Tanaka: par [0083]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Tanaka in order for Naidoo server to perform configurations on the device. Tanaka teachings enabled Naidoo/Bilger/Rezvani to create, modify, and delete configuration settings of the switch. One of ordinary skill in the art would have been motivated because allowing for configurations to be created, modified and deleted increase the flexibility of a device by allowing configurations to be created, modified and deleted.

Regarding Claim 29, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani discloses the method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.

Tanaka in the field of the same endeavor teaches creating a virtual local area network using a graphical user interface. In particular, Tanaka teaches the server automatically creates configuration information of the switch and deletes the VLAN link. The server automatically issues command to delete the

Art Unit: 2451

connection to the switch (see Tanaka; [0083]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Tanaka in order for Naidoo/Bilger/Rezvani server to perform actions on the device configurations. Tanaka teachings enabled Naidoo/Bilger/Rezvani to create, modify, and delete configuration settings of the switch. One of ordinary skill in the art would have been motivated because allowing for configurations to be created, modified and deleted increase the flexibility of a device by allowing configurations to be created, modified and deleted.

11. Claims 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over in further view of Naidoo in further view of Bilger in further view of Rezvani and in further view of Patterson (US 2005/0086126).

Regarding Claim 26, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of Claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.

Patterson, in the field of the same endeavor teaches managing and linking network accounts to share access privileges among accounts. In particular, Patterson teaches that the server may create account, upgrade an account, or terminate the upgrading of an account (see Patterson; [0046]).

Therefore, it would have been obvious to a person of ordinary skill in the

Art Unit: 2451

art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Patterson in order for the server of Naidoo/Bilger/Rezvani to create, upgrade, and terminate accounts. One of ordinary skill would be motivated because Patterson suggest it would be desirable for an environment having different levels of access, a provider may charge higher fees for accounts with higher levels of access. Accordingly, from the provider's standpoint, it is desirable to encourage users to purchase more expensive subscriptions, and so the provider often attempts to make the accounts with higher levels of access more appealing to users (see Patterson; [0002]).

12. Claims 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over in further view of Naidoo in further view of Bilger in further view of Rezvani and in further view of Moyer et al. (US 2002/0103898).

Regarding Claim 27, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly discloses the method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.

Moyer in the field of the same endeavor teaches Session Initiated Protocol (SIP) to communicate with network capable appliances by leveraging SIP capabilities to directly communicating with the appliances. In particular, Moyer teaches that SIP is an application layer control and signaling protocol used for creating, modifying and terminating communication sessions between

Art Unit: 2451

participants (see Moyer; [0013]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Moyer in order for Naidoo/Bilger/Rezvani servers to create, modify, and terminate communication between the gateway and the security system utilizing SIP. One of ordinary skill in the art would be motivated because SIP is designed to be independent of the underlying transport layer and it can run on TCP, UDP, or SCTP.

13. Claim 46-47 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Lingemann (US 2006/0009863).

Regarding claim 46, Naidoo/Bilger/Rezvani the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of claim 1, wherein the network device is a touchscreen.

Lingemann in the field of the same endeavor teaches building an automation system including user interface units with touchscreen. In particular, Lingemann teaches (see Lingemann; fig. 10, [0076]; a touch screen interface unit as illustrated in fig. 10 used for controlling electrical devices).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Lingemann in order for Naidoo's device to incorporate a

Art Unit: 2451

touchscreen. One of ordinary skill in the art would have been motivated because a touchscreen would provide an ease of interaction by allowing the user to interact with what is displayed directly on the hand, where it is displayed, rather than indirect with a mouse or touchpad.

Regarding Claim 47, Naidoo/Bilger/Rezvani discloses the method of claim 24, wherein the network device is a device controller that controls an attached device (see Lingemann; fig. 10, [0076]; a touch screen interface unit as illustrated in fig. 10 used for controlling electrical devices).

14. Claim 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of oore et al. (US 2007/0061266).

Regarding Claim 13, Naidoo/Bilger/Rezvani substantially discloses the method of claim 1, wherein the premise local area network is coupled to a wide area network. (see Naidoo; fig. 2; [0047-0048, 0087]; the security gateway is located in the premise which is considered a LAN. The security gateway is also connected to the internet and the security system server located at the data center which is consider to be the WAN).

However, Naidoo/Bilger/Rezvani does not explicitly disclose the premise local area network is coupled to a wide area network via a premise router.

Moore in the field of the same endeavor teaches large-scale, reliable, and

Art Unit: 2451

secure foundations for distributed databases and content management systems combining unstructured and structured data, and allowing post-input reorganization to achieve a high degree of flexibility. In particular, Moore teaches a router that forward data packets across an internet work through a process known as routing that act as a junction between two networks (see Moore; [0217]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Moore in order for Naidoo/Bilger/Rezvani premise location to include a router that act as a junction between two networks. One of ordinary skill in the art would have been motivated because the router would have improved Naidoo/Bilger/Rezvani teachings by enabled data packets to be routed to networks.

Regarding Claim 14, the combined teachings of Naidoo/Bilger/Rezvani and Moore further teach wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network (see Naidoo; fig. 2; [0047-0048, 0087]; the security gateway is located in the premise which is considered a LAN. The security gateway is also connected to the internet and the security system server located at the data center which is considered to be the WAN and Moore use of routers (see Moore; [0217]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the

Art Unit: 2451

teachings of Moore in order for Naidoo/Bilger/Rezvani premise location to include a router that act as a junction between two networks. One of ordinary skill in the art would have been motivated because the router would have improved Naidoo/Bilger/Rezvani teachings by enabled data packets to be routed to networks.

15. Claims 49-51 rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo and in further view of Rezvani.

Regarding Claim 49, Naidoo teaches a method comprising:

forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

establishing a coupling between the gateway and a plurality of premise devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the gateway and security network (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

Art Unit: 2451

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Regarding Claim 50, Naidoo teaches a method comprising:

automatically discovering a security system at a gateway and establishing communications between a gateway and a security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and



automatically establishing communications between the gateway and a plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating communications and functions of the plurality of network devices and the security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see fig.1 and 6).

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an

Art Unit: 2451

improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Regarding Claim 51, Naidoo teaches a method comprising:

forming a security network by automatically discovering a security system at a gateway and establishing communications between the gateway and the security system, the security system including security system components installed at a facility (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the security network and a plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the security network (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the network devices (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating

Art Unit: 2451

the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

16. Claim 52 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Dale et al. (US 7,681,201 B2) (hereinafter as Dale).

Regarding Claim 52, the combined teachings of Naidoo/Bilger/Rezvani teach the method of Claim 1 as discussed above.

The combined teachings of Naidoo/Bilger/Rezvani do not explicitly teach wherein the forming a security network including embedding an operating system of the security system in a component of the gateway.

However, Dale in a similar field of endeavor discloses a method and system for integrating and controlling components and subsystems including wherein forming a security network including embedding an operating system of the security system in a component of a gateway (client) (e.g., user interface box represents graphics rendering and other OS specific I/O portions of the application, the user interface communicates with the servers through TCP/IP, the user interface 28 runs on multiple OSs with a component designed to handle operating system specific matters, the system includes an OSAPI adaptation layer that converts abstracted calls into operating system specific calls, in which the OSAPI adaptation layer cooperates with an operating specific API layer for various operating systems, while the applications maybe operating system specific, they may also include internal operating system abstractions of their own for portability use in various systems and configurations, col.3, lines 10-39, 60-67-col.4, lines 1-5, col.4, lines 14-38, 53-67 and col.5, lines 1-32).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the capability and interfaces used to control a corresponding server as disclosed in Dale in forming the security network as disclosed by the combined teachings of Naidoo/Bilger/Rezvani to achieve the claimed invention. As disclosed by Dale, the motivation for the combination would be to provide a method and system for integrating and controlling multiple

Art Unit: 2451

components and subsystems for use as embedded systems that allows for reuse across many diverse products and platforms by multiple vendors (see col.1, lines 18-36 of Dale).

### ***Conclusion***

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Reply to a final rejection or action must include cancellation of, or appeal from the rejection of, each rejected claim. If any claim stands allowed, the reply to a final rejection or action must comply with any requirements or objections as to form (see 1.113). If prosecution in an application is closed, an applicant may request continued examination of the application by filing a submission and the fee set forth in § 1.17(e) prior to the earliest of: (c) A submission as used in this section includes, but is not limited to, an information disclosure statement, an

Art Unit: 2451

amendment to the written description, claims, or drawings, *new arguments*, or *new evidence in support of patentability*. If reply to an Office action under 35 USC 132 is outstanding, the submission must meet the reply requirements of § 1.111 (see MPEP 706.07)

Examiner has cited particular paragraphs, columns, and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY MEJIA whose telephone number is (571)270-3630. The examiner can normally be reached on Mon-Thur 9:30AM-8:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public

Art Unit: 2451

PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A.M./  
Patent Examiner, Art Unit 2451

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451

<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 1 of 2

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,192,418 B1	02-2001	Hale et al.	719/312
*	B	US-2003/0023839 A1	01-2003	Burkhardt et al.	713/1
*	C	US-2005/0120082 A1	06-2005	Hesselink et al.	709/203
*	D	US-6,963,981 B1	11-2005	Bailey et al.	726/22
*	E	US-2005/0267605 A1	12-2005	Lee et al.	700/019
*	F	US-7,043,537 B1	05-2006	Pratt, Richard W.	709/220
*	G	US-7,107,322 B1	09-2006	Freeny, Jr., Charles C.	709/217
*	H	US-2006/0242395 A1	10-2006	Fausak, Andrew T.	713/001
*	I	US-7,149,814 B2	12-2006	Neufeld et al.	709/248
*	J	US-7,164,907 B2	01-2007	Cochran et al.	455/419
*	K	US-2007/0079385 A1	04-2007	Williams et al.	726/027
*	L	US-2007/0256105 A1	11-2007	Tabe, Joseph Akwo	725/078
*	M	US-7,412,447 B2	08-2008	Hilbert et al.	1/1

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 2 of 2

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-7,681,201 B2	03-2010	Dale et al.	719/313
*	B US-7,970,863 B1	06-2011	Fontaine, Jean-Emmanuel	709/218
*	C US-2011/0283006 A1	11-2011	Ramamurthy, Venkatesh	709/228
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

2010Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		4,779,007	A	Schlanger et al.	10-18-1988	
		4,860,185	A	Brewer et al.	08-22-1989	
		5,086,385	A	Launey et al.	02-04-1992	
		5,519,878		Dolin, Jr.	05-21-1996	
		5,579,197	A	Mengelt et al.	11-26-1996	
		5,963,916	A	Kaplan, Joshua D.	10-05-1999	
		5,991,795		Howard et al.	11-23-1999	
		6,037,991		Thro et al.	03-14-2000	
		6,052,052	A	Delmonaco	04-18-2000	
		6,140,987	A	Stein et al.	10-31-2000	
		6,198,475	B1	Humpleman et al.	03-06-2001	
		6,219,677	B1	Howard	04-17-2001	
		6,286,038		Reichmeyer et al.	09-04-2001	
		6,288,716	B1	Humpleman et al.	09-11-2001	
		6,331,122	B1	Wu	12-18-2001	
		6,353,891	B1	Borella et al.	03-05-2002	
		6,363,417	B1	Howard et al.	03-26-2002	
		6,370,436	B1	Howard et al.	04-09-2002	
		6,377,861	B1	York	04-23-2002	
		6,462,507	B2	Fisher, Jr	10-08-2002	

**FOREIGN PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				
		WO	89/07855		Bavco Manufacturing Company	08-24-1989		
		JP	2003/085258	A	<del>Yamatake Building System Co. Ltd.</del>	<del>09-13-2001</del>		
		JP	2003/141659		Yamatake Building System Co. Ltd.	10-31-2001		
		JP	2004/192659		Sony Corp.	02-27-2004		
		KR	2006/0021605		Daewoo Electronics Corp.	09-03-2004		
		WO	2001/052478		Invensys Controls PLC	07-19-2001		

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2451
		First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		6,462,663		Wilson et al.	10-08-2002	
		6,467,084	B1	Howard et al.	10/15/2002	
		6,480,901	B1	Weber et al.	11-12-2002	
		6,493,020	B1	Stevenson et al.	12-10-2002	
		6,496,927	B1	McGrane	12-17-2002	
		6,529,723	B1	Bentley	03-04-2003	
		6,542,075		Barker et al.	04-01-2003	
		6,563,800		Salo et al.	05-13-2003	
		6,574,234	B1	Myer et al.	06-03-2003	
		6,580,950	B1	Johnson et al.	06-17-2003	
		6,587,736	B2	Howard et al.	07-01-2003	
		6,591,094	B1	Bentley	07-08-2003	
		6,601,086	B1	Howard et al.	07-29-2003	
		6,609,127	B1	Lee et al.	08-19-2003	
		6,615,088	B1	Myer et al.	09-02-2003	
		6,643,652	B2	Helgeson et al.	11-04-2003	
		6,643,669	B1	Novak et al.	11-04-2003	
		6,648,682	B1	Wu	11-18-2003	
		6,658,091		Naidoo et al.	12-02-2003	
		6,721,689		Markle et al.	04-13-2004	

**FOREIGN PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				
		WO	2001/099078		Eutech Cybernetics Inc.	12-27-2001		
		WO	2004/107710		LG Electronics Inc.	12-09-2004		
		WO	2004/004222		Thomson Licensing SA	01-08-2004		
		WO	2005/091218	A2	iControl Networks, Inc. without Search Report	09-29-2005		
		WO	2005/091218	A3	iControl Networks, Inc. Search Report	09-29-2005		

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./  
SecureNet Technologies, LLC Exhibit 1003 Page 131

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

## U.S. PATENT DOCUMENTS

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		6,721,747	B2	Lipkin, Daniel S.	04-13-2004	
		6,756,998		Bilger, Brent	06-29-2004	
		6,789,147	B1	Kessler et al.	09-07-2004	
		6,795,322	B2	Aihara et al.	09-21-2004	
		6,826,233		Oosawa, Hajime	11-30-2004	
		6,865,690	B2	Kocin	03-08-2005	
		6,912,429	B1	Bilger, Brent	06-28-2005	
		6,930,730	B2	Maxon et al.	08-16-2005	
		6,931,445	B2	Davis James S.	08-16-2005	
		6,959,393	B2	Hollis et al.	10-25-2005	
		6,990,591		Pearson, Sterling Michael	01-24-2006	
		7,016,970		Harumoto et al.	03-21-2006	
		7,024,676		Klopfenstein, Scott E.	04-04-2006	
		7,034,681		Yamamoto et al.	04-25-2006	
		7,047,088	B2	Nakamura et al.	05-16-2006	
		7,047,092	B2	Wimsatt, William	05-16-2006	
		7,072,934	B2	Helgeson et al.	07-04-2006	
		7,099,994	B1	Anschultz	08-29-2006	
		7,130,585	B1	Ollis et al.	10-31-2006	
		7,148,810		Bhat, Ishwara A.	12-12-2006	
		7,174,564	B1	Weatherspoon et al.	02-06-2007	
		7,183,907		Simon et al.	02-27-2007	
		7,203,486	B2	Patel, Ashish Raojibhai	04-10-2007	
		7,222,359	B2	Freund et al.	05-22-2007	
		7,237,267	B2	Rayes et al.	06-26-2007	
		7,305,461	B2	Ullmann, Lorin Evan	12-04-2007	
		7,337,217	B2	Wang, Dongyan	02-26-2008	
		7,337,473	B2	Chang et al.	02-26-2008	
		7,343,619	B2	Ofek et al.	03-11-2008	
		7,349,761		Cruse	03-25-2008	
		7,349,967	B2	Wang, Dongyan	03-25-2008	
		7,367,045	B2	Ofek et al.	04-29-2008	
		7,370,115		Bae et al.	05-06-2008	

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./  
SecureNet Technologies, LLC Exhibit 1003 Page 132

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

## U.S. PATENT DOCUMENTS

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		7,383,339	B1	Meenan et al.	06-03-2008	
		7,403,838	B2	Deen et al.	07-22-2008	
		7,409,451	B1	Meenan et al.	08-05-2008	
		7,428,585	B1	Owens et al.	09-23-2008	
		7,430,614		Shen et al.	09-30-2008	
		7,440,434		Chaskar et al.	10-21-2008	
		7,457,869	B2	Kernan, Timothy S.	11-25-2008	
		7,469,139	B2	van de Groenendaal Joannes G.	12-23-2008	
		7,469,294		Luo et al.	12-23-2008	
		7,480,713	B2	Ullmann, Lorin Evan	01-20-2009	
		7,480,724	B2	Zimler et al.	01-20-2009	
		7,506,052	B2	Qian et al.	03-17-2009	
		7,509,687	B2	Ofek et al.	03-24-2009	
		7,526,762		Astala et al.	04-28-2009	
		7,558,379	B2	Winick, Steven	07-07-2009	
		7,577,420	B2	Srinivasan et al.	08-18-2009	
		7,587,464	B2	Moorer et al.	09-08-2009	
		7,634,519	B2	Creamer et al.	12-15-2009	
		2001/0034754	A1	Elwahab et al.	10-25-2001	
		2002/0004828	A1	Davis et al.	01-10-2002	
		2002/0026476	A1	Miyazaki et al.	02-28-2002	
		2002/0029276	A1	Bendinelli et al.	03-07-2002	
		2002/0038380	A1	Brawn et al.	03-28-2002	
		2002/0052913	A1	Yamada et al.	05-02-2002	
		2002/0083342	A1	Webb et al.	06-27-2002	
		2002/0095490		Barker et al.	07-18-2002	
		2002/0103898	A1	Moyer et al.	08-01-2002	
		2002/0103927	A1	Parent, Jesse L.	08/01/2002	
		2002/0107910		Zhao	08-08-2002	
		2002/0111698	A1	Graziano et al.	08-15-2002	
		2002/0112051	A1	Ullmann, Lorin Evan	08-15-2002	
		2002/0112182	A1	Chang et al.	08-15-2002	
		2002/0143923		Alexander, Bruce	10-03-2002	

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./  
SecureNet Technologies, LLC Exhibit 1003 Page 133

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

## U.S. PATENT DOCUMENTS

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		2002/0156564	A1	Preston et al.	10-24-2002	
		2002/0180579	A1	Nagoka et al.	12-05-2002	
		2002/0184301	A1	Parent, Jesse L.	12-05-2002	
		2003/0009552	A1	Benfield et al.	01-09-2003	
		2003/0009553	A1	Benfield et al.	01-09-2003	
		2003/0041167	A1	French et al.	02-27-2003	
		2003/0051009	A1	Shah et al.	03-13-2003	
		2003/0052923	A1	Porter, Swain W.	03-20-2003	
		2003/0062997	A1	Naidoo et al.	04-03-2003	
		2003/0090473	A1	Joshi, Vikas B.	05-15-2003	
		2003/0115345		Chien et al.	06-19-2003	
		2003/0132018	A1	Okita et al.	07-17-2003	
		2003/0174648	A1	Wang, Mea	09-18-2003	
		2003/0187920		Redkar	10-02-2003	
		2003/0210126		Kanazawa	11-13-2003	
		2003/0236841		Epshteyn	12-25-2003	
		2004/0003241		Sengodan et al.	01-01-2004	
		2004/0015572		Kang	01-22-2004	
		2004/0037295	A1	Tanaka et al.	02-26-2004	
		2004/0054789	A1	Breh et al.	03-18-2004	
		2004/0086088	A1	Naidoo et al.	05-06-2004	
		2004/0139227	A1	Takeda, Yutaka	07-15-2004	
		2004/0162902	A1	Davis James S.	08-19-2004	
		2004/0177163	A1	Casey et al.	09-09-2004	
		2004/0243835	A1	Terzis et al.	12-02-2004	
		2004/0267937	A1	Klements, Anders E.	12-30-2004	
		2005/0038326		Mathur	02-17-2005	
		2005/0066045	A1	Johnson et al.	03-24-2005	
		2005/0069098	A1	Kalervo et al.	03-31-2005	
		2005/0079855		Jethi et al.	04-15-2005	
		2005/0086126	A1	Patterson, Russell D.	04-21-2005	
		2005/0108091	A1	Sotak et al.	05-19-2005	
		2005/0108369	A1	Sather et al.	05-19-2005	
		2005/0125083	A1	Kiko	06-09-2005	

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./  
SecureNet Technologies, LLC Exhibit 1003 Page 134

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		2005/0128083	A1	Puzio et al.	06-16-2005	
		2005/0149639	A1	Vrieling et al.	07-07-2005	
		2005/0169288		Kamiwada et al.	08-04-2005	
		2005/0197847		Smith	09-08-2005	
		2005/0216302		Raji et al.	09-29-2005	
		2005/0216580	A1	Raji et al.	09-29-2005	
		2005/0222820	A1	Chung	10-06-2005	
		2005/0231349	A1	Bhat, Ishwara A.	10-20-2005	
		2006/0009863	A1	Lingemann, Ronald R.	01-12-2006	
		2006/0088092	A1	Chen et al.	04-27-2006	
		2006/0105713	A1	Zheng et al.	05-18-2006	
		2006/0181406		Petite et al.	08-17-2006	
		2006/0182100	A1	Li et al.	08-17-2006	
		2006/0187900	A1	Akbar, Imran M.	08-24-2006	
		2006/0200845	A1	Foster et al.	09-07-2006	
		2007/0052675		Chang	03-08-2007	
		2007/0061266	A1	Moore et al.	03-15-2007	
		2007/0106124		Kuriyama et al.	05-10-2007	
		2007/0286210		Gutt et al.	12-13-2007	
		2007/0286369		Gutt et al.	12-13-2007	
		2007/0298772	A1	Owen et al.	12-27-2007	
		2008/0042826	A1	Hevia et al.	02-21-2008	
		2008/0065681	A1	Fontijn et al.	03-13-2008	
		2008/0084296	A1	Kutzik et al.	04-10-2008	
		2008/0147834		Quinn et al.	06-19-2008	
		2008/0180240		Raji et al.	07-31-2008	
		2008/0183842		Raji et al.	07-31-2008	
		2008/0235326		Parsi et al.	09-25-2008	
		2009/0070436	A1	Dawes et al.	03-12-2009	
		2009/0165114	A1	Baum et al.	06-25-2009	
		2009/0204693		Andreev et al.	08-13-2009	
		2009/0240787	A1	Denny, Michael S.	09-24-2009	
		2009/0240814	A1	Brubacher et al.	09-24-2009	
		2010/0082744		Gutt	04-01-2010	

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

**ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./**  
SecureNet Technologies, LLC Exhibit 1003 Page 135

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

U.S. PATENT DOCUMENTS

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		2010/0095111		Gutt	04-15-2010	
		2010/0095369		Gutt	04-15-2010	
		D416,910		Vasquez	11-23-1999	
		D451,529	S	Vasquez	12-04-2001	
		D464,328	S	Vasquez et al.	10-15-2002	
		D464,948	S	Vasquez et al.	10-29-2002	
		2006/0282886	A1	Gaug, Mark	12-14-2006	
		7,627,665	B2	Barker et al.	10-03-2002	
		6,928,148	B2	Simon et al.	12-13-2001	
		7,551,071	B2	Bennett, III et al.	10-05-2006	
		2004/0123149	A1	Tyroler	06-24-2004	

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

**ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./**  
SecureNet Technologies, LLC Exhibit 1003 Page 136



Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**NON PATENT LITERATURE DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		Form PCT/ISA/220, ICON.P011WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, ICON.P011WO, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, ICON.P011WO, "PCT Written Opinion of the International Searching Authority," 8 pgs.	
		Form PCT/ISA/220, ICON.P012WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, ICON.P012WO, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, ICON.P012WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P0014WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, ICON.P014WO, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, ICON.P014WO, "PCT Written Opinion of the International Searching Authority," 7 pgs.	
		Form PCT/ISA/220, ICON.P0015WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, ICON.P015WO, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, ICON.P015WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, PCT/US05/08766, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, PCT/US05/08766, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, PCT/US05/08766, "PCT Written Opinion of the International Searching Authority," 5 pgs.	

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------


\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./  
SecureNet Technologies, LLC Exhibit 1003 Page 137

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2451
		First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia
<b>NON PATENT LITERATURE DOCUMENTS</b>			
Exam. Initial*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		Examination Report under Section 18(3) re UK patent application no. GB0724760.4 dated January 30, 2008 4 pgs	
		Examination Report under Section 18(3) re UK patent application no. GB0724248.0 dated January 30, 2008 4 pgs	
		Examination Report under Section 18(3) re UK patent application no. GB0724248.0 dated June 4, 2008 2 pgs	
		Examination Report under Section 18(3) re UK patent application no. GB0800040.8 dated January 30, 2008 4 pgs	
		Examination Report under Section 18(3) re UK patent application no. GB0620362.4 dated August 13, 2007, 3 pgs	
		Alarm.com - Interactive Security Systems, Product Advantages, printed from website 11/4/2003, 3 pp	
		Alarm.com - Interactive Security Systems, Frequently Asked Questions, printed from website 11/4/2003, 3 pp	
		Alarm.com - Interactive Security Systems, Elders, printed from website 11/4/2003, 1 page	
		Alarm.com - Interactive Security Systems, Overview, printed from website 11/4/2003, 2 pp	
		X10 - ActiveHome, Home Automation Made Easy!, printed from website 11/4/2003, 3 pp	

Examiner Signature	/Anthony Mejia/	Date Considered	09/07/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

<b>Search Notes</b>  	<b>Application/Control No.</b>  12189788	<b>Applicant(s)/Patent Under Reexamination</b>  BAUM ET AL.
	<b>Examiner</b>  ANTHONY MEJIA	<b>Art Unit</b>  2451

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
709	201, 202, 203, 224, 225, 227	9/6/2012	A.M.
717	101, 102	9/6/2012	A.M.
707	203	9/6/2012	A.M.
718	101	9/6/2012	A.M.
726	1	9/6/2012	A.M.
706	46	9/6/2012	A.M.

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
EAST Class Limited w/Text Search (See Search History)	9/6/2012	A.M.
EAST Text Search (See Search History)	9/6/2012	A.M.
EAST Assignee Search (See Search History)	08/23/2010	A.M.
EAST Inventor Search (See Search History)	08/23/2010	A.M.
ALL EAST Searches Using: US-PGPUB, USPAT, USOCR, FPRS, JPO, EPO, DERWENT, IBM_TDB		
NPL Search (See ACM and IEEE Search History)	9/6/2012	A.M.

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
709	200	9/6/2012	A.M.

/A. M./ Examiner.Art Unit 2451	
-----------------------------------	--

IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites



Access provided by:  
United States Patent and  
Trademark Office  
Sign Out



#### SEARCH RESULTS

You searched for: {{{firmware OR "operating system"}} AND upgrading OR updating) AND gateway)

238 Results returned

< First | 1 | 2 | 3 | 4 | 5 | >> Last >

#### Upgrading the cardiac patient record in the coronary care unit into the new millennium

van Domburg, R.T.; Suling, R.; Patijn, M.; van der Putten, M.  
Computers in Cardiology 2001

Digital Object Identifier: 10.1109/CIC.2001.977612

Publication Year: 2001, Page(s): 145 - 148

IEEE CONFERENCE PUBLICATIONS

#### Congestion avoidance with BUC (buffer utilization control) gateways and RFCN (reverse feedback congestion notification)

Ziegler, T.; Clausen, H.D.

Performance, Computing, and Communications Conference, 1997. PCCC 1997., IEEE International

Digital Object Identifier: 10.1109/PCCC.1997.581545

Publication Year: 1997, Page(s): 410 - 418

IEEE CONFERENCE PUBLICATIONS

#### Implementation of an Auto Configuration Method for the Management Home Server

Byounghee Son; Youngchoong Park; Hagbae Kim

Future Generation Communication and Networking Symposia, 2008. FGNCNS '08. Second International Conference on

Volume: 1

Digital Object Identifier: 10.1109/FGNCNS.2008.92

Publication Year: 2008, Page(s): 53 - 56

IEEE CONFERENCE PUBLICATIONS

#### An architecture for component evolution

Ryan, A.; Newmarch, I.

Consumer Communications and Networking Conference, 2005. CCNC. 2005 Second IEEE

Digital Object Identifier: 10.1109/CCNC.2005.1408223

Publication Year: 2005, Page(s): 498 - 503

IEEE CONFERENCE PUBLICATIONS

#### A gateway between MHS (X.400) and SMTP

Tang, D.; Anzenberger, M.; Markovitz, P.; Wallace, M.

Computer Standards Conference, 1988. 'Computer Standards

Evolution: Impact and Imperatives', Proceedings of the

Digital Object Identifier: 10.1109/CSTAND.1988.4753

Publication Year: 1988, Page(s): 7 - 14

IEEE CONFERENCE PUBLICATIONS

#### Mobility management based on Mobile IPv4/v6 translation gateway in mixed IPv4/v6 networks

Zheng Xiang; Zhengming Ma

Systems and Informatics (ICSAI), 2012 International

Conference on

Digital Object Identifier: 10.1109/ICSAL.2012.6223321

Publication Year: 2012, Page(s): 1498 - 1502

IEEE CONFERENCE PUBLICATIONS

**An Effective Gateway Discovery Mechanism in an Integrated Internet-MANET (IIM)**

Khan, Khaleel Ur Rehman; Reddy, A. Venugopal; Zaman, Rafi U.; Kumar, Manish  
*Advances in Computer Engineering (ACE)*, 2010 International Conference on  
 Digital Object Identifier: 10.1109/ACE.2010.27  
 Publication Year: 2010 , Page(s): 24 - 28  
 IEEE CONFERENCE PUBLICATIONS

**Adaptive gateway discovery for mobile ad hoc networks based on the characterisation of the link lifetime**

Yuste, A.J.; Trivifio, A.; Castani, E.; Trujillo, F.D.  
*Communications, IET*  
 Volume: 5 , Issue: 15  
 Digital Object Identifier: 10.1049/iet-com.2010.0692  
 Publication Year: 2011 , Page(s): 2241 - 2249  
 IEEE JOURNALS & MAGAZINES

**An effective gateway discovery mechanism in an integrated Internet-MANET (IIM)**

Khan, F.U.R.; Ehteshami, M.; Kumar, M.; Zaman, F.U.  
*Ultra Modern Telecommunications & Workshops, 2009. ICUMT '09. International Conference on*  
 Digital Object Identifier: 10.1109/ICUMT.2009.5345417  
 Publication Year: 2009 , Page(s): 1 - 7  
 IEEE CONFERENCE PUBLICATIONS

**Hybrid gateway advertisement scheme for connecting mobile ad hoc networks to the Internet**

Jeongkaun Lee; Dongkyun Kim; Garcia-Luna-Aceves, J.J.; Yanghee Choi; Jihyuk Choi; Sangwoo Nam  
*Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semannual*  
 Volume: 1  
 Digital Object Identifier: 10.1109/VETECS.2003.1207528  
 Publication Year: 2003 , Page(s): 191 - 195 vol.1  
 Cited by 5  
 IEEE CONFERENCE PUBLICATIONS

**Gateway discovery and routing in ad hoc networks with NAT-based Internet connectivity**

Jaewook Shin; Haeryong Lee; Jeethyoon Na; Park, A.; Kim, S.  
*Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*  
 Volume: 4  
 Digital Object Identifier: 10.1109/VETECF.2004.1400587  
 Publication Year: 2004 , Page(s): 2883 - 2886 Vol. 4  
 IEEE CONFERENCE PUBLICATIONS

**A Model-Driven Framework for the Generation of Gateways in Distributed Real-Time Systems**

Obermaisser, R.  
*Real-Time Systems Symposium, 2007. RTSS 2007. 28th IEEE International*  
 Digital Object Identifier: 10.1109/RTSS.2007.9  
 Publication Year: 2007 , Page(s): 93 - 104  
 IEEE CONFERENCE PUBLICATIONS

**The Comprehensive Gateway Model for Diverse Environmental Monitoring Upon Wireless Sensor Network**

Hsueh-Chun Lin; Yiso-Chiang Kan; Yao-Ming Hong  
*Sensors Journal, IEEE*  
 Volume: 11 , Issue: 5  
 Digital Object Identifier: 10.1109/JSEN.2010.2088389  
 Publication Year: 2011 , Page(s): 1293 - 1303  
 Cited by 1  
 IEEE JOURNALS & MAGAZINES

---

**Improved Scheme for Adaptive Gateway Discovery in Hybrid MANET**

Yuste, A.J.; Triviño, A.; Trujillo, F.D.; Caslari, E.  
*Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on*  
 Digital Object Identifier: 10.1109/ICDCSW.2010.63  
 Publication Year: 2010 , Page(s): 270 - 275  
 Cited by 2  
**IEEE CONFERENCE PUBLICATIONS**

---

**Introducing Gateway Timeout control in wireless TCP module**

Nanjun Li; Zorn, W.  
*Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*  
 Digital Object Identifier: 10.1109/COMSWA.2008.4554440  
 Publication Year: 2008 , Page(s): 357 - 364  
**IEEE CONFERENCE PUBLICATIONS**

---

**Design of a common gateway between LonWorks and serial bus**

Shuangqing Wang; Jianchun Xing; Ping Wang  
*Multimedia Technology (ICMT), 2011 International Conference on*  
 Digital Object Identifier: 10.1109/ICMT.2011.6002799  
 Publication Year: 2011 , Page(s): 5369 - 5373  
**IEEE CONFERENCE PUBLICATIONS**

---

**Efficient load reduction and congestion control in Internet through multilevel Border Gateway Proxy Caching**

Manikandan, C.V.; Manimozhil, P.; Suganyadevi, B.; Radhika, K.; Asha, M.  
*Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on*  
 Digital Object Identifier: 10.1109/ICCIC.2010.5705859  
 Publication Year: 2010 , Page(s): 1 - 4  
**IEEE CONFERENCE PUBLICATIONS**

---

**Maintaining Gateway Connectivity in Multi-hop Ad hoc Networks**

Brannstrom, R.; Ahlund, C.; Zaslavsky, A.  
*Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on*  
 Digital Object Identifier: 10.1109/LCN.2005.86  
 Publication Year: 2005 , Page(s): 682 - 689  
**IEEE CONFERENCE PUBLICATIONS**

---

**A Gateway Discovery Method for MANET Accessing Internet Based on Overhead Control**

Xin Li; Zhilang Zhu  
*Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*  
 Digital Object Identifier: 10.1109/wicom.2011.6040424  
 Publication Year: 2011 , Page(s): 1 - 4  
**IEEE CONFERENCE PUBLICATIONS**

---

**A non-stop updating technique for device driver programs on the IROS platform**

Araki, H.; Futagami, S.; Nish, K.  
*Communications, 1995. ICC '95 Seattle, 'Gateway to Globalization', 1995 IEEE International Conference on*  
 Volume: 1  
 Digital Object Identifier: 10.1109/ICC.1995.525144  
 Publication Year: 1995 , Page(s): 88 - 92 vol.1  
**IEEE CONFERENCE PUBLICATIONS**

---

**Modeling and Performance Analysis of Telephony Gateway Registration Protocol**

Kumaran, P ; Sahoo, A.

Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on

Digital Object Identifier: 10.1109/LCN.2007.99

Publication Year: 2007 , Page(s): 575 - 582

IEEE CONFERENCE PUBLICATIONS

**Experience with prefix discovery servers and IPSec VPN gateways**

Stax, W.; Hillson, C.; Wollman, W.; Jegers, M.

Military Communications Conference, 2005. MILCOM 2005. IEEE

Digital Object Identifier: 10.1109/MILCOM.2005.1605768

Publication Year: 2005 , Page(s): 725 - 730 Vol. 2

IEEE CONFERENCE PUBLICATIONS

**A novel PSO-based algorithm for gateway placement in wireless mesh networks**

Vinh Trong Le; Nghia Huu Dinh; Nhu Gia Nguyen

Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on

Digital Object Identifier: 10.1109/ICCSN.2011.6013541

Publication Year: 2011 , Page(s): 41 - 45

IEEE CONFERENCE PUBLICATIONS

**A gateway concept for visual exploration and control of building services**

Frauth, S.

Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on

Digital Object Identifier: 10.1109/ETFA.2010.5641204

Publication Year: 2010 , Page(s): 1 - 4

IEEE CONFERENCE PUBLICATIONS

**Improving Delay Performance in UMTS/WLAN Integrated Networks with Global Gateway Router**

Khara, S.; Misra, I. S.; Saha, G.

Advanced Computing and Communications, 2008. ADCCOM 2008. 16th International Conference on

Digital Object Identifier: 10.1109/ADCCOM.2008.4760476

Publication Year: 2008 , Page(s): 374 - 381

IEEE CONFERENCE PUBLICATIONS

< First | 1 | 2 | 3 | 4 | 5 | > Last >

Sign In | Create Account

**IEEE Account**

Change Username/Password

Update Address

**Purchase Details**

Payment Options

Order History

Access Purchased Documents

**Profile Information**

Communications Preferences

Profession and Education

Technical Interests

**Need Help?**

US & Canada: +1 800 678 4313


Worldwide: +1 732 981 9000

Contact & Support

About IEEE Xplore | Contact | Help | Terms of Use | Nondiscrimination Policy | Site Map | Privacy & Opting Out of Cookies

A non-profit organization, IEEE is the world's largest professional association for the advancement of technology.

© Copyright 2012 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

<b>Index of Claims</b> 	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>


N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE									
Final	Original	08/23/2010	04/26/2011	04/29/2011	12/19/2011	09/25/2012					
	1	✓	✓	✓	✓	✓					
	2	✓	✓	✓	✓	✓					
	3	✓	✓	✓	✓	✓					
	4	✓	✓	-	-	-					
	5	✓	✓	✓	✓	✓					
	6	✓	✓	✓	✓	✓					
	7	✓	✓	✓	✓	✓					
	8	✓	✓	✓	✓	✓					
	9	✓	✓	✓	✓	✓					
	10	✓	✓	✓	✓	✓					
	11	✓	✓	✓	✓	✓					
	12	✓	✓	✓	✓	✓					
	13	✓	✓	✓	✓	✓					
	14	✓	✓	✓	✓	✓					
	15	✓	✓	✓	✓	✓					
	16	✓	✓	✓	✓	✓					
	17	✓	✓	✓	✓	✓					
	18	✓	✓	✓	✓	✓					
	19	✓	✓	✓	✓	✓					
	20	✓	✓	✓	✓	✓					
	21	✓	✓	✓	✓	✓					
	22	✓	✓	✓	✓	✓					
	23	✓	✓	✓	✓	✓					
	24	✓	✓	✓	✓	✓					
	25	✓	✓	✓	✓	✓					
	26	✓	✓	✓	✓	✓					
	27	✓	✓	✓	✓	✓					
	28	✓	✓	✓	✓	✓					
	29	✓	✓	✓	✓	✓					
	30	✓	✓	✓	✓	✓					
	31	✓	✓	✓	✓	✓					
	32	✓	✓	✓	✓	✓					
	33	✓	✓	✓	✓	✓					
	34	✓	✓	✓	✓	✓					
	35	✓	✓	✓	✓	✓					
	36	✓	✓	✓	✓	✓					



<b>Index of Claims</b>  	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010	04/26/2011	04/29/2011	12/19/2011	09/25/2012			
	37	✓	✓	✓	✓	✓			
	38	✓	✓	✓	✓	✓			
	39	✓	✓	✓	✓	✓			
	40	✓	✓	✓	✓	✓			
	41	✓	✓	✓	✓	✓			
	42	✓	✓	✓	✓	✓			
	43	✓	✓	✓	✓	✓			
	44	✓	✓	✓	✓	✓			
	45	✓	✓	✓	✓	✓			
	46	✓	✓	✓	✓	✓			
	47	✓	✓	✓	✓	✓			
	48	✓	✓	✓	✓	✓			
	49	✓	✓	✓	✓	✓			
	50	✓	✓	✓	✓	✓			
	51	✓	✓	✓	✓	✓			
	52					✓			

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	2	"7681201".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 15:33
L3	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 15:34
L4	3	"20090077624"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 15:49
L5	0	"20090077624" and (operating adj1 system or OS) near5 gateway	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 15:51
L6	1	"20090077624" and (operating adj1 system or OS) with gateway	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 15:51
L7	2	"20090077624" and gateway	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/27 15:52
S1	2	"20060271695"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:01
S2	18	12/189757	US-PGPUB;	OR	ON	2011/03/27

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:01
S3	45868	709/201.ccls. 709/202.ccls. 709/203.ccls. 709/224.ccls. 709/225.ccls. 709/227.ccls. 717/101.ccls. 717/102.ccls. 707/203.ccls. 718/101.ccls. 726/1.ccls. 706/46.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:05
S4	34837379	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:05
S5	39563	S3 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:06
S6	3955	(automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:06
S7	201056	(generat\$3 creat\$3) near5 (network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S8	797	S6 AND S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S9	659	S8 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S10	797	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)) AND ((generat\$3 creat\$3) near5 (network))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2011/03/27 15:11

			IBM_TDB			
S11	659	S10 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S12	476	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)) AND ((generat\$3 creat\$3) near5 (network)) AND (security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S13	416	S12 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:12
S14	25	(automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors) near5 (security surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:19
S15	23	S14 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:20
S16	3	"7015806".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:24
S17	2	"6756998".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:32
S18	2	"20020103898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 16:49
S19	2	"6686838".pn.	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2011/04/26 19:18

			EPO; JPO; DERWENT; IBM_TDB			
S20	9	"20030062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:29
S21	15	"2003/0062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:30
S22	2	09/969521	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:41
S23	2	"20090077622"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/14 17:37
S24	2	"20040037295"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 11:36
S25	2	"20020103898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 12:11
S26	3	"20040267939"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/03 10:02
S27	383	("20010034754"   "20020004828"   "20020026476"   "20020029276"   "20020038380"   "20020052913"   "20020083342"   "20020095490"   "20020103898"   "20020103927"   "20020107910"   "20020111698"   "20020112051"   "20020112182"   "20020143923"   "20020156564"   "20020180579"   "20020184301"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/08/27 09:42

"20030009552"	"20030009553"	
"20030041167"	"20030052923"	
"20030062997"	"20030090473"	
"20030115345"	"20030132018"	
"20030174648"	"20030187920"	
"20030210126"	"20030236841"	
"20040003241"	"20040015572"	
"20040037295"	"20040054789"	
"20040086088"	"20040123149"	
"20040139227"	"20040162902"	
"20040177163"	"20040243835"	
"20040267937"	"20050038326"	
"20050066045"	"20050069098"	
"20050079855"	"20050086126"	
"20050108091"	"20050108369"	
"20050125083"	"20050128083"	
"20050149639"	"20050169288"	
"20050197847"	"20050216302"	
"20050216580"	"20050222820"	
"20050231349"	"20060009863"	
"20060088092"	"20060105713"	
"20060181406"	"20060182100"	
"20060187900"	"20060200845"	
"20060282886"	"20070052675"	
"20070061266"	"20070106124"	
"20070286210"	"20070286369"	
"20070298772"	"20080042826"	
"20080065681"	"20080084296"	
"20080147834"	"20080180240"	
"20080183842"	"20080235326"	
"20090070436"	"20090165114"	
"20090204693"	"20090240787"	
"20090240814"	"20100082744"	
"20100095111"	"20100095369"	
"4779007"	"4860185"	"5086385"
"5519878"	"5579197"	
"5963916"	"5991795"	"6037991"
"6052052"	"6140987"	
"6198475"	"6219677"	"6286038"
"6288716"	"6331122"	
"6353891"	"6363417"	"6370436"
"6377861"	"6452507"	
"6462663"	"6467084"	"6480901"
"6493020"	"6496927"	
"6529723"	"6542075"	"6563800"
"6574234"	"6580950"	
"6587736"	"6591094"	"6601086"
"6609127"	"6615088"	
"6643652"	"6643669"	"6648682"
"6658091"	"6721689"	
"6721747"	"6756998"	"6789147"
"6795322"	"6826233"	
"6865690"	"6912429"	"6928148"
"6930730"	"6931445"	
"6959393"	"6990591"	"7016970"
"7024676"	"7034681"	
"7047088"	"7047092"	"7072934"
"7099994"	"7130585"	
"7148810"	"7174564"	"7183907"
"7203486"	"7222359"	
"7237267"	"7305461"	"7337217"
"7337473"	"7343619"	
"7349761"	"7349967"	"7367045"
"7370115"	"7383339"	

		"7403838"   "7409451"   "7428585"   "7430614"   "7440434"   "7457869"   "7469139"   "7469294"   "7480713"   "7480724"   "7506052"   "7509687"   "7526762"   "7551071"   "7558379"   "7577420"   "7587464"   "7627665"   "7634519"   "D416910"   "D451529"   "D464328"   "D464948").PN.				
S28	4802	(automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/06 23:45
S29	0	(embedd\$3 stor\$3 sav\$3) near5 (operating ADJ system) near5 (gateway) near5 (client device terminal) near5 (control\$3 mana\$3) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 17:55
S30	107	(embedd\$3 stor\$3 sav\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 17:56
S31	6	(embedd\$3 stor\$3 sav\$3 add\$3) near5 (operating ADJ system) near5 (gateway) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:20
S32	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:22
S33	1	12/187788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:22
S34	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:22
S35	24546	(component widget) near5 (includ\$3 compris\$3) near5 ("OS" operating	US-PGPUB; USPAT;	OR	ON	2012/09/25 18:26

		ADJ system)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S36	1079	(embedd\$3 stor\$3 sav\$3 add\$3) near5 (operating ADJ system) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:28
S37	568	(full) near5 (control\$4 management) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:29
S38	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:29
S39	447	S37 and S38	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:29
S40	10	S36 AND S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:30
S41	631	(full) near5 (control\$4 management functions functionality) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:30
S42	11	S41 and S36	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:30
S43	1143	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:32



S44	216844	(control\$4 management functions functionality) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:32
S45	333	S43 and S44	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:42
S46	269	S45 and S38	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:42
S47	10	S46 and ((security sureveillance) ADJ (system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 18:43
S48	3045	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external) near5 (server device system terminal)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:40
S49	3045	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:41
S50	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:41
S51	2363	S49 AND S50	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:41
S52	335741	(control\$4 manag\$3) near5 (remote external) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2012/09/25 20:43

			DERWENT; IBM_TDB			
S53	782	S49 AND S52	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:43
S54	1144	(gateway) near5 (control\$4 manag\$3) near5 (remote external) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:45
S55	810	S54 AND S50	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:46
S56	4	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 20:56
S57	2	"7970863".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:08
S58	5	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:32
S59	0	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 ("of") near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:33
S60	5	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:33
S61	5	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system (drivers))	US-PGPUB; USPAT; USOCR;	OR	ON	2012/09/25 21:33

		near5 (remote external managed) near5 (server device system terminal component)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S62	4768	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system (drivers)) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:33
S63	4768	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((operating ADJ system) (drivers)) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:34
S64	3741	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:35
S65	0	S64 and (icontrol)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:36
S66	2739	("icontrol")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 21:37
S67	2	("icontrol") near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 22:06
S68	4768	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((drivers)operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 22:10
S69	7	(gateway) near5 (embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3 includ\$3) near5 ((drivers)(operating ADJ system)) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 22:14
S70	631	(full) near5 (control\$4 management	US-PGPUB;	OR	ON	2012/09/25

		functions functionality) near5 (remote) near5 (server device system)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			23:32
S71	3741	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:32
S72	12	S71 and S70	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:32
S73	631	(full all) near5 (control\$4 management functions functionality) near5 (remote) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:33
S74	671	(full all) near5 (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:34
S75	12	S74 AND S71	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:34
S76	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:34
S77	3741	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:35
S78	671	(full all) near5 (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2012/09/25 23:35

			IBM_TDB			
S79	12	S78 AND S77	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:35
S80	114	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)) SAME (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:47
S81	161	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((drivers) operating ADJ system) near5 (remote external managed) near5 (server device system terminal component)) SAME (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:48
S82	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:49
S83	134	S81 AND S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:49
S84	261	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((drivers) operating ADJ system) near5 (remote external managed) near5 (server device system terminal component peripheral)) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:56
S85	266	((embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 ((drivers) operating ADJ system) near5 (remote external managed) near5 (device system terminal component peripheral)) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:56
S86	200	S85 AND S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/25 23:57
S87	0	(gateway gw) near5 ((embedd\$3	US-PGPUB;	OR	ON	2012/09/25

		stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (device system terminal component peripheral)) near5 (server)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			23:59
S88	2	S86 AND ((Security surveillance camera) ADJ (system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:00
S89	555302	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (drivers) operating ADJ system (mini ADJ (operating ADJ system)) near5 (remote external managed) near5(server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:03
S90	167257	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ((drivers) operating ADJ system (mini ADJ (operating ADJ system)) near5 (remote external managed) near5(server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:03
S91	1644566	((drivers) operating ADJ system (mini ADJ (operating ADJ system)) near5 (remote external managed) near5(server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:04
S92	1644566	((drivers) (operating ADJ system) (mini ADJ (operating ADJ system)) near5 (remote external managed) near5 (server))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:05
S93	95	(mini ADJ (operating ADJ system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:06
S94	71	S93 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:06
S95	0	(mini ADJ (operating ADJ system)) near5 (remote\$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2012/09/26 00:08

			IBM_TDB			
S96	162	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (remote external managed) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:08
S97	107	S96 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:09
S98	4651	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (operating ADJ system) near5 (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:19
S99	256	S98 AND ((Security surveillance camera) ADJ (system))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:19
S100	199	S99 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:20
S101	16	(full all) near5 (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system) SAME (Operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 00:21
S102	54	(embedd\$3 stor\$3 sav\$3 add\$3 copy\$3 sav\$3) near5 (operating ADJ systems) near5 (remote external managed) near5 (server device system terminal component)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 01:03
S103	32	S102 and S82	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 01:03
S104	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2012/09/26 02:14

			EPO; JPO; DERWENT; IBM_TDB			
S105	199	(touchscreen interface gw gateway) same (reduced footprint mini) same ((operating ADJ system) Linux windows) same (remote)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:17
S106	35087855	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:18
S107	148	S105 AND S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:18
S108	147	(touchscreen interface gw gateway) same (reduced footprint mini) same ((operating ADJ system) Linux) same (remote)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:19
S109	113	S108 and S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:19
S110	360	(touchscreen interface gw gateway) same (reduced footprint mini) same ((operating ADJ system) Linux) same (host remote)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:20
S111	6	(touchscreen interface gw gateway) same (reduced footprint mini) same ((operating ADJ system) Linux) same (remote ADJ (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/09/26 02:23
S112	2	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (reduced footprint mini) same ((operating ADJ system) Linux) same (remote ADJ (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:24
S113	2	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (minature reduced	US-PGPUB; USPAT;	OR	ON	2012/09/26 02:24



		footprint mini) same ((operating ADJ system) Linux) same (remote ADJ (server host))	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S114	838	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (minature reduced footprint mini) same ((operating ADJ system) Linux)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:25
S115	667	S114 and S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:25
S116	445	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (compact minature reduced footprint mini) near5 ((operating ADJ system) Linux)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:31
S117	671	(full all) near5 (control\$4 management functions functionality) near5 (remote\$2) near5 (server device system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:32
S118	0	S116 and S117	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:32
S119	334	S116 and S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:32
S120	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:35
S121	157	ihub "ihub" "ihub client"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:36

S122	254370	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (compact minature reduced footprint mini minios)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:48
S123	8	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ( minios)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 02:48
S124	9	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ((minature reduced footprint mini) ADJ ((operating ADJ system) Linux)).CLM.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:02
S125	0	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ((minature reduced footprint mini) ADJ ((operating ADJ system) "OS") near5 (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:04
S126	12971	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 ((operating ADJ system) "OS") near5 (server host)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:04
S127	64	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (locally) near5 ((operating ADJ system) "OS") near5 (server host)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:05
S128	24	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (locally) near5 ((operating ADJ system) "OS") near5 (remote\$2 external\$2) near5 (server host)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:05
S129	64	(embedd\$3 stor\$3 sav\$3 copy\$3 sav\$3) near5 (locally) near5 ((operating ADJ system) "OS") near5 (server host)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:07
S130	37	S129 AND S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2012/09/26 03:08

			DERWENT; IBM_TDB			
S131	46	((minature reduced footprint mini) ADJ ((operating ADJ system) "OS") near5 (server host))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:09
S132	26	S131 AND S106	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:10
S133	2	"6192418".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:16
S134	2	"6963981".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:19
S135	2	"20070256105"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:24
S136	2	"7681201".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 03:28
S137	2	"20070256105"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/26 16:40

**EAST Search History (Interference)**

&lt;This search history is empty&gt;

**9/ 27/ 2012 4:10:58 PM****C:\Users\amejia\Documents\EAST\Workspaces\12189757A.wsp**

IN THE UNITED STATES PATENT OFFICE

In Re Application of: )  
 )  
 Marc Baum, et al. ) Examiner: Anthony Mejia  
 ) Art Unit: 2451  
 )  
 Application No.: 12/189,788 )  
 )  
 Filed: August 12, 2008 )  
 )  
 For: FORMING A SECURITY NETWORK )  
 INCLUDING INTEGRATED SECURITY )  
 SYSTEM COMPONENTS AND NETWORK )  
 DEVICES )

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

PROPOSED CLAIM AMENDMENTS FOR DISCUSSION

Sir:

Attached is a proposed claim amendment for consideration by and/or discussion with Examiner MEJIA.

PROPOSED AMENDMENTS

IN THE CLAIMS

1. (Currently amended) A method comprising:
  - coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components;
  - automatically discovering the plurality of security system components at the gateway and establishing communications between the gateway and the plurality of security system components;
  - automatically discovering a plurality of premise devices at the gateway and establishing communications between the gateway and the plurality of premise devices;
  - and
  - forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein the forming of the security network includes embedding ~~an a security system~~ operating system ~~of the security system~~ in a component of the gateway and executing the security system operating system on a gateway operating system of the gateway, wherein the security system operating system is required for basic operation of the security system, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server.
  
2. (Original) The method of claim 1, comprising controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device.

3. (Original) The method of claim 2, wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

Claim 4 (Canceled).

5. (Previously presented) The method of claim 1, comprising using protocols of the security system to discover the security system components, wherein the gateway includes the protocols of the security system.

6. (Previously presented) The method of claim 1, comprising the gateway receiving protocols of the security system from the security server in response to a request, wherein the gateway uses the protocols received to discover the security system components.

7. (Original) The method of claim 1, wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components.

8. (Original) The method of claim 7, wherein the connection management component automatically discovers the premise devices.

9. (Original) The method of claim 7, wherein the connection management component automatically installs the premise devices in the security network.

10. (Original) The method of claim 7, wherein the connection management component automatically configures the premise devices for operation in the security network.

11. (Original) The method of claim 1, wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices.
12. (Original) The method of claim 1, wherein the gateway includes a device connect component that includes definitions of the security system components and the premise devices.
13. (Original) The method of claim 1, wherein the premise local area network is coupled to a wide area network via a premise router.
14. (Original) The method of claim 1, wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network.
15. (Original) The method of claim 1, wherein the gateway is coupled to the premise devices using a wireless coupling.
16. (Original) The method of claim 1, wherein the gateway is coupled to the security server via the internet.
17. (Original) The method of claim 1, wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location.
18. (Original) The method of claim 1, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link.

19. (Original) The method of claim 18, comprising transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link.

20. (Original) The method of claim 19, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

21. (Original) The method of claim 18, comprising transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable.

22. (Original) The method of claim 18, wherein the secondary communication link includes a broadband coupling.

23. (Original) The method of claim 18, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling.

24. (Original) The method of claim 18, comprising transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link.

25. (Original) The method of claim 24, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

26. (Original) The method of claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.



27. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.
28. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the premise devices.
29. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.
30. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the premise devices.
31. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the security system components.
32. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the premise devices.
33. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the security system components.
34. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the premise devices.
35. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices.

36. (Original) The method of claim 1, wherein the security server manages communications with the security system components.
37. (Original) The method of claim 1, wherein the security server manages communications with the premise devices.
38. (Original) The method of claim 1, wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data.
39. (Original) The method of claim 38, wherein the notifications include one or more of short message service messages and electronic mail messages.
40. (Original) The method of claim 38, wherein the event data is event data of the security system components.
41. (Original) The method of claim 38, wherein the event data is event data of the premise devices.
42. (Original) The method of claim 1, wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link.
43. (Original) The method of claim 1, wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.
44. (Original) The method of claim 1, wherein the premise device is an Internet Protocol device.

45. (Original) The method of claim 1, wherein the premise device is a camera.

46. (Original) The method of claim 1, wherein the premise device is a touchscreen.

47. (Original) The method of claim 1, wherein the premise device is a device controller that controls an attached device.

48. (Original) The method of claim 1, wherein the premise device is a sensor.

49. (Currently amended) A method comprising:

forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location; and automatically discovering a plurality of premise devices at the gateway and establishing a coupling between the gateway and the plurality of premise devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the gateway and the security network, wherein the integrating includes embedding ~~an a~~ security system operating system of the security system in a component of the gateway and executing the security system operating system on a gateway operating system of the gateway, wherein the security system operating system is required for basic operation of the security system, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server.

50. (Currently amended) A method comprising:

automatically discovering a security system at a gateway and establishing communications between the gateway and the security system in a facility, wherein the

security system includes a plurality of security system components that are proprietary to the security system; and

automatically discovering a plurality of network devices at the gateway and establishing communications between the gateway and the plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating into the gateway communications and functions of the plurality of network devices and the plurality of security system components, wherein the integrating includes embedding ~~an~~ a security system operating system of the security system in a component of the gateway and executing the security system operating system on a gateway operating system of the gateway, wherein the security system operating system is required for basic operation of the security system, wherein objects corresponding to at least one of the plurality of security system components and the plurality of network devices are maintained on a remote server.

51. (Currently amended) A method comprising:

forming a security network by automatically discovering a security system at a gateway and establishing communications between the gateway and the security system, the security system including security system components installed at a facility, wherein the gateway is located at a first location, wherein the gateway is coupled to a security server at a second location different than the first location;

automatically discovering a plurality of network devices at the gateway and establishing communications between the security network and the plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the gateway and the security network, wherein the integrating includes embedding ~~an~~ a security system operating system of the security system in a component of the gateway and executing the security system operating system on a gateway operating system of the

gateway, wherein the security system operating system is required for basic operation of the security system; and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the plurality of network devices, wherein objects corresponding to at least one of the security system components and the plurality of network devices are maintained on the security server.

Claim 52 (Canceled).

REMARKS

In view of the foregoing amendments, Applicants respectfully submit that the previously-entered rejections under 35 U.S.C. §103 have been overcome, and their withdrawal is respectfully requested. Applicants submit that claims 1-3 and 5-51 are in condition for allowance. The allowance of the claims is earnestly requested. If there are any issues that remain to be resolved prior to allowance of the claims, Examiner MEJIA is encouraged to email (rick@iprlaw.com) or call (408.821.8080) Rick Gregory.

Respectfully submitted,  
GREGORY & SAWRIE LLP

Date: September 25, 2012

---

Richard L. Gregory, Jr., Reg. No. 42,607  
Telephone: 408.821.8080

GREGORY & SAWRIE LLP  
2018 Bissonnet Street  
Houston, Texas 77005  
Fax: 713-364-1397

Searching for: (firmware and OS and gateway and security and integrated) and (updating or upgrading or update or upgrade) ([start a new search](#))

Found **56** within *The ACM Guide to Computing Literature* (Bibliographic citations from major publishers in computing)

**Limit your search** to Publications from ACM and Affiliated Organizations (Full-Text collection: 350,153 items)

## REFINE YOUR SEARCH

## ▼ Refine by Keywords

## ▼ Refine by People

[Names](#)  
[Institutions](#)  
[Authors](#)  
[Reviewers](#)

## ▼ Refine by Publications

[Publication Year](#)  
[Publication Names](#)  
[ACM Publications](#)  
[All Publications](#)  
[Content Formats](#)  
[Publishers](#)

## ▼ Refine by Conferences

[Sponsors](#)  
[Events](#)  
[Proceeding Series](#)

## ADVANCED SEARCH

[Advanced Search](#)

## FEEDBACK

[Please provide us with feedback](#)

Found **56** of 2,001,070

Search Results

Related Journals

Related Magazines

Related SIGs

Related Conferences

Results 1 - 20 of 56

Sort by relevance

in expanded form

Result page: [1](#) [2](#) [3](#) [next](#)1 [MIDAS: an integrated e-commerce solution for Australian transport industries](#)

[Manish Malhotra](#), [Zahir Tari](#)

September 2004

**International Journal of Web Engineering and Technology**, Volume 1 Issue 3

**Publisher:** Inderscience Publishers

**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

MIDAS provides an autonomous delivery management system from client orders to the electronic proof of deliv for the Australian transport industry. To accomplish this, MIDAS utilises different technologies, including global positioning system (GPS), ...

**Keywords:** Australia, binary tree, delivery management, global positioning system, internet procurement, logit applications, mobile e-commerce, palm applications, routing, scheduling, supply chain management, transport applications, web services, wireless application protocol

2 [Wireless mesh networks: a survey](#)

[Ian F. Akvildiz](#), [Xudong Wang](#), [Weilin Wang](#)

March 2005

**Computer Networks: The International Journal of Computer and Telecommunications Networking**, Volume 47 Issue 4

**Publisher:** Elsevier North-Holland, inc.

**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

Wireless mesh networks (WMNs) consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. They provide network access for both mesh and conventional clients. The integration of WMNs with other networks ...

**Keywords:** Ad hoc networks, Medium access control, Power management and control, Routing protocol, Scalability, Security, Timing synchronization, Transport protocol, Wireless mesh networks, Wireless sensor networks

3 [Information Assurance: Dependability and Security in Networked Systems](#)

[Yi Qian](#), [David Tipper](#), [Prashant Krishnamurthy](#), [James Joshi](#)

November 2007

Information Assurance: Dependability and Security in Networked Systems

**Publisher:** Morgan Kaufmann Publishers Inc.

Full text available: [The ACM Learning Center](#), [PDF](#) (4.15 MB)

**Bibliometrics:** Downloads (6 Weeks): 25, Downloads (12 Months): 90, Downloads (Overall): 90, Citation Count: 0

In today's fast paced, infocentric environment, professionals increasingly rely on networked information technology to do business. Unfortunately, with the advent of such technology came new and complex problems that continue to threaten the availability, ...


**Keywords:** Networking

4 [Experiences in deploying a wireless mesh network testbed for traffic control](#)

Kun-chen Lan, Zhe Wang, Mahbub Hassan, Tim Moors, Rodney Berriman, Lavy Libman, Maximilian Ott, Björn Landfeldt, Zainab Zeidi

October 2007 **SIGCOMM Computer Communication Review**, Volume 37 Issue 5

**Publisher:** ACM

Full text available:  Pdf (809.67 KB)

**Bibliometrics:** Downloads (6 Weeks): 2, Downloads (12 Months): 43, Downloads (Overall): 786, Citation Count: 2

Wireless mesh networks (WMN) have attracted considerable interest in recent years as a convenient, flexible and low-cost alternative to wired communication infrastructures in many contexts. However, the great majority of research on metropolitan-scale ...




**Keywords:** deployment, traffic control, wireless mesh network

#### 5 [Securing Citrix Presentation Server in the Enterprise](#)

[Tara Azad](#)

June 2008 **Securing Citrix Presentation Server in the Enterprise**

**Publisher:** Syngress Publishing

Full text available:  The ACM Learning Center,  ePub (11.25 MB),  PDF (25.46 MB)

**Bibliometrics:** Downloads (6 Weeks): 12, Downloads (12 Months): 41, Downloads (Overall): 41, Citation Count: 0

Citrix Presentation Server allows remote users to work off a network server as if they weren't remote. That means: Incredibly fast access to data and applications for users, no third party VPN connection, and no latency issues. All of these features ...

**Keywords:** Applied, Computer Science, Computers, Security



#### 6 [How to Cheat at Securing Your Network](#)

[Ido Dubrawsky](#)

October 2007

**How to Cheat at Securing Your Network**

**Publisher:** Syngress Publishing


Full text available:  The ACM Learning Center,  PDF (8.35 MB)

**Bibliometrics:** Downloads (6 Weeks): 16, Downloads (12 Months): 72, Downloads (Overall): 72, Citation Count: 0

Most System Administrators are not security specialists. Keeping the network secure is one of many responsibilities, and it is usually not a priority until disaster strikes. How to Cheat at Securing Your Network is the perfect book for this audience. ...


**Keywords:** Security

#### 7 [RAP: protecting commodity wi-fi networks from rogue access points](#)

 [Liran Ma](#), [Amin Y. Teymorian](#), [Zuozhen Cheng](#), [Min Song](#)

August 2007 **QSHINE '07: The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness & Workshops**


**Publisher:** ACM 

Full text available:  Pdf (86.77 KB)

**Bibliometrics:** Downloads (6 Weeks): , Downloads (12 Months): 5, Downloads (Overall): 52, Citation Count: 0

We first give a comprehensive taxonomy of rogue access points (APs), which includes a new class of rogue APs never addressed in the literature before. Then, we propose an efficient rogue AP protection system termed as RAP for commodity Wi-Fi networks. ...


#### 8 [Framework for security and privacy in automotive telematics](#)

 [Sastry Duri](#), [Marco Gruteser](#), [Xuan Liu](#), [Paul Moskowitz](#), [Ronald Perez](#), [Moninder Singh](#), [Jung-Mu Tang](#)

September 2002

**WMC '02: Proceedings of the 2nd international workshop on Mobile commerce**

**Publisher:** ACM

Full text available:  Pdf (203.71 KB)

**Bibliometrics:** Downloads (6 Weeks): 12, Downloads (12 Months): 85, Downloads (Overall): 1990, Citation Count:

Automotive telematics may be defined as the information-intensive applications that are being enabled for vehicles by a combination of telecommunications and computing technology. Telematics by its nature requires the capture of sensor data, storage ...

**Keywords:** automotive telematics, privacy, privacy policies, security

#### 9 [Netcat Power Tools](#)




[Jan Karsliiz, Jr.](#)

June 2008

**Netcat Power Tools**

**Publisher:** Syngress Publishing



Full text available:  [The ACM Learning Center](#),  [ePub \(4.91 MB\)](#),  [PDF \(10.83 MB\)](#)

**Bibliometrics:** Downloads (6 Weeks): 15, Downloads (12 Months): 83, Downloads (Overall): 83, Citation Count: 0

Netcat is one of the most commonly used anti-hacking tools in the world. It reads and writes data across network connections, using the TCP/IP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other ...

**Keywords:** Internet, Security


10 [Internet Security Glossary](#)

[R. Shirsy](#)

May 2000

Internet Security Glossary

**Publisher:** RFC Editor

Full text available:  [Text \(489.29 KB\)](#)

**Bibliometrics:** Downloads (6 Weeks): , Downloads (12 Months): 24, Downloads (Overall): 750, Citation Count: 23

This Glossary (191 pages of definitions and 13 pages of references) provides abbreviations, explanations, and recommendations for use of information system security terminology. The intent is to improve the comprehensibility of writing that deals with ...



11 [TechnoSecurity's Guide to E-Discovery and Digital Forensics: A Comprehensive Handbook](#)

[Jack Wiles](#)

October 2007

TechnoSecurity's Guide to E-Discovery and Digital Forensics: A Comprehensive Handbook

**Publisher:** Syngress Publishing

Full text available:  [The ACM Learning Center](#),  [PDF \(9.51 MB\)](#)

**Bibliometrics:** Downloads (6 Weeks): 10, Downloads (12 Months): 42, Downloads (Overall): 42, Citation Count: 0

This book provides IT security professionals with the information (hardware, software, and procedural requirements) needed to create, manage and sustain a digital forensics lab and investigative team that can accurately and effectively analyze forensic ...

**Keywords:** Security

12 [Bringing the internet to all electronic devices](#)

[Michael Howard](#), [Christopher S. Sontag](#)

March 1999

**WOES'99:** Proceedings of the Workshop on Embedded Systems on Workshop on Embedded Systems

**Publisher:** USENIX Association

**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

In order to develop appropriate solutions for embedded device networking, we must understand the benefits offered to the end user of the device as well as the costs involved with delivering a solution. As proponents of networking technology, it is tempting ...

13 [Enhancing availability with service automation and a trusted support partner](#)

[R. Hastata](#), [S. Fredericksen](#), [E. Burns](#), [L. Braga](#), [K.W. Eastley](#), [J. Bird](#)

October 2008

**IBM Systems Journal**, Volume 47 Issue 4

**Publisher:** IBM Corp.

**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

Since the onset of the computer age, customers have been searching for ways to increase systems availability, maximizing the return on their investment and keeping their systems running continuously as much as possible. Traditionally, customers have ...

14 [A computer system for predictive maintenance of wind generators](#)

[Inácio Fonseca](#), [Torres Farinha](#), [Márcio Barbosa](#)

July 2008

**ICCOMP'08:** Proceedings of the 12th WSEAS international conference on Computers

**Publisher:** World Scientific and Engineering Academy and Society (WSEAS)



**Bibliometrics:** Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

Wind generators maintenance can be performed in a systematic way because they are built with equipments with known reliability and maintenance parameters known that can be used in the planned maintenance. However, it is possible to increase the reliability ...




**Keywords:** maintenance management, predictive maintenance, wind generators

- 15 [Systemic issues in the hart intercivic and premier voting systems: reflections on project EVEREST](#)  
Kevin Butler, William Enck, Herri Hursti, Stephen McLaughlin, Patrick Traynor, Patrick McDaniel  
July 2008 **EVT'08**: Proceedings of the conference on Electronic voting technology  
**Publisher**: USENIX Association  
**Bibliometrics**: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

The State of Ohio commissioned the EVEREST study in late summer of 2007. The study participants were charged with an analysis of the usability, stability, and security of all voting systems used in Ohio elections. This paper details the approach and ...

- 16 [Windows Forensic Analysis DVD Toolkit](#)  
Harlan Carvey  
April 2007 Windows Forensic Analysis DVD Toolkit  
**Publisher**: Syngress Publishing  
Full text available:  [The ACM Learning Center](#),  PDF (6.31 MB)  
**Bibliometrics**: Downloads (6 Weeks): 16, Downloads (12 Months): 60, Downloads (Overall): 60, Citation Count: 2

The only book available on the market that addresses and discusses in-depth forensic analysis of Windows systems. Windows Forensic Analysis DVD Toolkit takes the reader to a whole new, undiscovered level of forensic analysis for Windows systems, providing ...  
**Keywords**: Computer Science, Security




- 17 [Architecture and Patterns for IT Service Management, Resource Planning, and Governance. Making Shoes for the Cobbler's Children: Making Shoes for the Cobbler's Children, 2nd edition](#)  
Charles T. Betz  
November 2006 Architecture and Patterns for IT Service Management, Resource Planning, and Governance. Making Shoes for the Cobbler's Children: Making Shoes for the Cobbler's Children, 2nd edition  
**Publisher**: Morgan Kaufmann Publishers Inc.  
Full text available:  [The ACM Learning Center](#),  ePub (8.06 MB),  PDF (3.66 MB)  
**Bibliometrics**: Downloads (6 Weeks): 27, Downloads (12 Months): 105, Downloads (Overall): 105, Citation Count:

How would you feel if you visited your financial planner's office and saw past-due credit card notices on their desk? Would you trust an auto mechanic whose car backfires and produces black smoke? A dentist with bad teeth? A banker in shabby clothes? ...  
**Keywords**: Business Software, Database Management

- 18 [Unified Link Layer API: A generic and open API to manage wireless media access](#)  
Mahesh Soorivandana, Tim Farnham, Costas Efthymiou, Matthias Wellens, Janna Riihijärvi, Petri Mähönen, Alain Geffaut, José Antonio Galache, Diego Meloignano, Arthur van Rooijen  
March 2008 **Computer Communications**, Volume 31 Issue 5  
**Publisher**: Elsevier Science Publishers B. V.  
**Bibliometrics**: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:


We present the Unified Link Layer API (ULLA) framework: an open and extensible API framework that incorporates a number of requirements related to a wide range of applications, including multi-mode and cross-layer optimisation scenarios. This work has ...

**Keywords**: API, Link layer abstraction, Wireless applications

- 19 [Securing Windows Server 2008: Prevent Attacks from Outside and Inside Your Organization](#)  
Aron Tiensivu  
May 2008 Securing Windows Server 2008: Prevent Attacks from Outside and Inside Your Organization  
**Publisher**: Syngress Publishing  
Full text available:  [The ACM Learning Center](#),  ePub (5.45 MB),  PDF (15.87 MB)  
**Bibliometrics**: Downloads (6 Weeks): 15, Downloads (12 Months): 71, Downloads (Overall): 71, Citation Count: 0

Microsoft hails the latest version of its flagship server operating system, Windows Server 2008, as "the most secure Windows Server ever". However, to fully achieve this lofty status, system administrators and security professionals must install, configure, ...

**Keywords**: Applied, Computer Science, Computers, Security

- 20 [SAMPL: a simple aggregation and message passing layer for sensor networks](#)  
Anthony Rowe, Karthik Lakshmanan, Rajeev R. R. Raikumar  
November 2008 **WICON '08**: Proceedings of the 4th Annual International Conference on Wireless Internet  
**Publisher**: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)  
Full text available:  PDF (839.81 KB)





**Bibliometrics:** Downloads (6 Weeks): 1, Downloads (12 Months): 28, Downloads (Overall): 127, Citation Count: 1

In recent years, wireless sensor networking has shown great promise in applications ranging from industrial control, environmental monitoring and inventory tracking. Given the resource-constrained nature of sensor dev and the dynamic wireless channel ...

**Keywords:** deployment, network management, sensor networks, tree routing, wireless sensor networks

Result page: [1](#) [2](#) [3](#) [next](#)

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2012 ACM, Inc.  
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned

**U.S. PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		4,754,261		Marino, Francis C.	06-28-1988	
		4,833,449	A	Gaffigan, Robert J.	05-23-1989	
		4,993,059	A	Smith, et al.	02-12-1991	
		5,907,279	A	Bruins, et al.	05-25-1999	
		6,060,994		Chen, Scanner	05-09-2000	
		6,134,591		Nickles, Alfred E.	10-17-2000	
		6,281,790		Kimmel, et al.	08-28-2001	
		6,351,829		Dupont, et al.	02-26-2002	
		6,385,772		Courtney, Jonathan D.	05-07-2002	
		6,400,265	B1	Saylor, et al.	06-04-2002	
		6,621,827		Rezvani, et al.	09-16-2003	
		6,658,091		Naidoo, et al.	12-03-2003	
		6,661,340		Saylor, et al.	12-09-2003	
		6,686,838		Rezvani, et al.	02-03-2004	
		6,690,411		Naidoo, et al.	02-10-2004	
		6,693,545		Brown, et al.	02-17-2004	
		6,738,824	B1	Blair, Dana	05-18-2004	
		6,756,998		Bilger, Brent	06-29-2004	
		6,778,085		Faulkner, et al.	08-17-2004	
		6,781,509		Oppedahl, et al.	08-24-2004	

**FOREIGN PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned

**U.S. PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		6,798,344		Faulkner, et al.	09-28-2004	
		6,891,838		Petite, et al.	05-10-2005	
		6,928,148		Simon, et al.	08-09-2005	
		6,930,599		Naidoo, et al.	08-16-2005	
		6,943,681		Rezvani, et al.	09-13-2005	
		6,965,313		Saylor, et al.	11-15-2005	
		6,970,183		Monroe, David A.	11-29-2005	
		6,972,676		Kimmel, et al.	12-06-2005	
		6,975,220		Foodman et al.	12-13-2005	
		6,990,591		Pearson, Sterling Michael	01-24-2006	
		7,030,752		Tyroler, Dan	04-18-2006	
		7,032,002		Rezvani, et al.	04-18-2006	
		7,039,391		Rezvani, et al.	05-02-2006	
		7,079,020		Stilp, Louis A.	07-18-2006	
		7,080,046		Rezvani, et al.	07-18-2006	
		7,085,937		Rezvani, et al.	08-01-2006	
		7,103,152		Naidoo, et al.	09-05-2006	
		7,106,176		La, et al.	09-12-2006	
		7,113,090	B1	Saylor, et al.	09-26-2006	
		7,113,099		Tyroler, et al	09-26-2006	

**FOREIGN PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				

Examiner Signature	/Anthony Mejja/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		7,120,232		Naidoo, et al.	10-10-2006	
		7,120,233		Naidoo, et al.	10-10-2006	
		7,130,383	B2	Naidoo, et al.	10-31-2006	
		7,149,798		Rezvani, et al.	12-12-2006	
		7,183,907		Simon, et al.	02-27-2007	
		7,218,217		Adonailo, et al.	05-15-2007	
		7,250,854		Rezvani, et al.	07-31-2007	
		7,254,779		Rezvani, et al.	08-07-2007	
		7,262,690		Heaton, et al.	08-28-2007	
		2001/0016501	A1	King, Joseph D.	08-23-2001	
		2006/0009863	A1	Lingemann, Ronald R.	01-12-2006	
		2006/0111095	A1	Weigand, David L.	05-25-2006	
		2006/0206220	A1	Amundson, John B.	09-14-2006	
		2006/0271695	A1	Lavian, Yoel	11-30-2006	
		2007/0061266	A1	Moore, et al.	03-15-2007	
		2007/0142022	A1	Madonna, et al.	06-21-2007	
		2007/0256105	A1	Tabe, Joseph A.	11-01-2007	

**FOREIGN PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./  
SecureNet Technologies, LLC Exhibit 1003 Page 182

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned
<b>NON PATENT LITERATURE DOCUMENTS</b>			
Exam. Initial*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc ), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		Form PCT/ISA/220, ICON.P001WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, ICON.P001WO, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, ICON.P001WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P002WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, ICON.P002WO, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, ICON.P002WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P003WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, ICON.P003WO, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, ICON.P003WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P005WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		<del>Form PCT/ISA/210, ICON.P005WO, "PCT International Search Report," 2 pgs.</del>	
		Form PCT/ISA/237, ICON.P005WO, "PCT Written Opinion of the International Searching Authority," 7 pgs.	

Examiner Signature	/Anthony Mejia/	Date Considered	09/25/2012
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609 Draw line through citation if not in conformance and not considered  
 Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.M./  
 SecureNet Technologies, LLC Exhibit 1003 Page 183

**IN THE UNITED STATES PATENT OFFICE**

In Re Application of: )  
 )  
 Marc Baum, et al. ) Examiner: Anthony Mejia  
 ) Art Unit: 2451  
 )  
 Application No.: 12/189,788 )  
 )  
 Filed: August 12, 2008 )  
 )  
 For: FORMING A SECURITY NETWORK )  
 INCLUDING INTEGRATED SECURITY )  
 SYSTEM COMPONENTS AND NETWORK )  
 DEVICES )

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE

Sir:

Applicant respectfully requests consideration of the following amendments and remarks contained herein in response to the Office Action mailed July 17, 2012.



AMENDMENTS

IN THE CLAIMS

1. (Previously presented) A method comprising:
  - coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components;
  - automatically discovering the plurality of security system components at the gateway and establishing communications between the gateway and the plurality of security system components;
  - automatically discovering a plurality of premise devices at the gateway and establishing communications between the gateway and the plurality of premise devices;
  - and
  - forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server.
  
2. (Original) The method of claim 1, comprising controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device.
  
3. (Original) The method of claim 2, wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

Claim 4 (Canceled).

5. (Previously presented) The method of claim 1, comprising using protocols of the security system to discover the security system components, wherein the gateway includes the protocols of the security system.

6. (Previously presented) The method of claim 1, comprising the gateway receiving protocols of the security system from the security server in response to a request, wherein the gateway uses the protocols received to discover the security system components.

7. (Original) The method of claim 1, wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components.

8. (Original) The method of claim 7, wherein the connection management component automatically discovers the premise devices.

9. (Original) The method of claim 7, wherein the connection management component automatically installs the premise devices in the security network.

10. (Original) The method of claim 7, wherein the connection management component automatically configures the premise devices for operation in the security network.

11. (Original) The method of claim 1, wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices.

12. (Original) The method of claim 1, wherein the gateway includes a device connect component that includes definitions of the security system components and the premise devices.

13. (Original) The method of claim 1, wherein the premise local area network is coupled to a wide area network via a premise router.
14. (Original) The method of claim 1, wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network.
15. (Original) The method of claim 1, wherein the gateway is coupled to the premise devices using a wireless coupling.
16. (Original) The method of claim 1, wherein the gateway is coupled to the security server via the internet.
17. (Original) The method of claim 1, wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location.
18. (Original) The method of claim 1, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link.
19. (Original) The method of claim 18, comprising transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link.
20. (Original) The method of claim 19, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

21. (Original) The method of claim 18, comprising transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable.
22. (Original) The method of claim 18, wherein the secondary communication link includes a broadband coupling.
23. (Original) The method of claim 18, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling.
24. (Original) The method of claim 18, comprising transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link.
25. (Original) The method of claim 24, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.
26. (Original) The method of claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.
27. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.
28. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the premise devices.

29. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.
30. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the premise devices.
31. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the security system components.
32. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the premise devices.
33. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the security system components.
34. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the premise devices.
35. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices.
36. (Original) The method of claim 1, wherein the security server manages communications with the security system components.
37. (Original) The method of claim 1, wherein the security server manages communications with the premise devices.
38. (Original) The method of claim 1, wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data.

39. (Original) The method of claim 38, wherein the notifications include one or more of short message service messages and electronic mail messages.
40. (Original) The method of claim 38, wherein the event data is event data of the security system components.
41. (Original) The method of claim 38, wherein the event data is event data of the premise devices.
42. (Original) The method of claim 1, wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link.
43. (Original) The method of claim 1, wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.
44. (Original) The method of claim 1, wherein the premise device is an Internet Protocol device.
45. (Original) The method of claim 1, wherein the premise device is a camera.
46. (Original) The method of claim 1, wherein the premise device is a touchscreen.
47. (Original) The method of claim 1, wherein the premise device is a device controller that controls an attached device.
48. (Original) The method of claim 1, wherein the premise device is a sensor.

49. (Previously presented) A method comprising:  
forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location; and  
automatically discovering a plurality of premise devices at the gateway and establishing a coupling between the gateway and the plurality of premise devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the gateway and the security network, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server.

50. (Previously presented) A method comprising:  
automatically discovering a security system at a gateway and establishing communications between the gateway and the security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system; and  
automatically discovering a plurality of network devices at the gateway and establishing communications between the gateway and the plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating into the gateway communications and functions of the plurality of network devices and the plurality of security system components, wherein objects corresponding to at least one of the plurality of security system components and the plurality of network devices are maintained on a remote server.

51. (Previously presented) A method comprising:  
forming a security network by automatically discovering a security system at a gateway and establishing communications between the gateway and the security system,

the security system including security system components installed at a facility, wherein the gateway is located at a first location, wherein the gateway is coupled to a security server at a second location different than the first location;

automatically discovering a plurality of network devices at the gateway and establishing communications between the security network and the plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the gateway and the security network; and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the plurality of network devices, wherein objects corresponding to at least one of the security system components and the plurality of network devices are maintained on the security server.

52. (New) The method of claim 1, the forming a security network including embedding an operating system of the security system in a component of the gateway.



REMARKS

Claims 1-3 and 5-51 were pending in the application. Claims 1-3 and 5-51 were rejected. New claim 52 is added herein.

Petition For Extension Of Time

A Petition For Extension Of Time Under 37 CFR 1.136(a) is submitted herewith along with the appropriate fee amount for a three (3) month extension of time.

Rejections under 35 U.S.C. §103

Claims 1-3, 5-9, 11, 12, 15-25, 28, 30-45 and 48 were rejected under 35 U.S.C. §103(a) as being anticipated by United States (US) Patent Application Publication No. US 2003/0062997 A1 ("Naidoo") in view of United States Patent No. 6,756,998 ("Bilger") and further in view of United States Patent No. 6,686,838 ("Rezvani").

Applicant respectfully submits that the claims as amended herein are patentably distinct from Naidoo, Bilger and/or Rezvani. Moreover, Naidoo, Bilger and/or Rezvani fail to teach each and every element of claims 1-3, 5-9, 11, 12, 15-25, 28, 30-45, 48 and 52 as presented herein.

The Examiner at page 6 of the Office Action states that Naidoo does not explicitly teach the step of "automatically discovering security system components". Applicant agrees.

The Examiner at page 7 of the Office Action states that Naidoo and Bilger do not explicitly teach the step of "automatically discovering a plurality of premise devices at a gateway". Applicant agrees.

Regarding claim 1 as amended herein, Applicant respectfully submits that Naidoo describes a system and method for distributed monitoring and remote verification of conditions surrounding an alarm condition in a security system (abstract). Naidoo describes that the security system includes a security gateway, which is typically located at the desired premises to be monitored, and a monitoring client, typically located at a central station and operatively coupled to security gateway through a network. Naidoo describes that often, the security gateway is located at the target site, however, on some occasions, some or all components of security gateway may be located remotely, but

remain operatively coupled to security sensors and video cameras which are at the premises (paragraph 0028).

Naidoo describes that the security gateway is a processor-based device that functions to detect alarm conditions at a target site and to capture information relating to such alarm conditions (paragraph 0032). Naidoo describes that, upon detection of an alarm condition, the security gateway captures video (usually through an attached video camera) of the target site, and sends the video to security system server in real time (paragraph 0028).

Naidoo describes that a monitoring client is generally a software program that may be used to display some or all of the information provided by security gateway. Monitoring client may be a stand-alone program or integrated into one or more existing software programs. Naidoo describes that one or more operators may then use this information to evaluate whether the alarm condition corresponds to an actual alarm condition and then take additional action, if desired, such as alerting the appropriate authorities (paragraph 0032).

Naidoo describes that the security system includes one or more sensors coupled to security gateway for the purpose of detecting alarm conditions. The security system is not limited to any specific type or model of sensor. Any sensor may be used, depending on the desired type and level of protection. Alarm sensors may be wired directly into an alarm control panel built into the security gateway or they may be wirelessly connected (paragraph 0033). Naidoo describes that the security system also includes one or more video cameras that are operable to capture video data of monitored premises. Naidoo describes that the security gateway may be configured to create an association between one or more sensors and an associated video camera (paragraph 0034).

Regarding claim 1, as amended, Applicant respectfully submits that Naidoo does not disclose coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

As set forth above, Naidoo describes that the security gateway is a processor-based device that functions to detect alarm conditions at a target site and to capture information relating to such alarm conditions (paragraph 0032). Naidoo describes that, upon detection of an alarm condition, the security gateway captures video (usually through an attached video camera) of the target site, and sends the video to security system server in real time (paragraph 0028).

Naidoo describes that a monitoring client is generally a software program that may be used to display some or all of the information provided by security gateway. Monitoring client may be a stand-alone program or integrated into one or more existing software programs. Naidoo describes that one or more operators may then use this information to evaluate whether the alarm condition corresponds to an actual alarm condition and then take additional action, if desired, such as alerting the appropriate authorities (paragraph 0032). Therefore, Naidoo simply describes a security gateway that detects alarm conditions at a target site and forwards the detected conditions and related information to a security system server whereupon a monitoring client displays some or all of alarm condition information. Naidoo nowhere teaches coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

The Examiner disagrees with Applicant's position set forth above and argues at page 4 of the Office Action that Naidoo's disclosure of remote user access to features of a base station teaches wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server. Applicant respectfully disagrees. Applicant submits that Naidoo describes functionality to allow access to security gateway 115 and security system server 131 using a remote station 155 operatively coupled to security gateway 115 and security system server 131. Remote user 155 must first be authenticated by security system server 131. It is noted that an embodiment contemplates the use of any authentication technique. Once

authenticated, remote user may access some or all of the features of base station 115. These features may include, without limitation, arming or disarming the security system; adjusting sensitivities of sensors (if present); adjusting alarm condition detection sensitivity; remote surveillance; adjusting camera settings; and reviewing alarms and recordings. These functions may also include remote surveillance, referred to as "lifestyle video" (paragraph 0040).

Applicant respectfully submits that paragraph 0040 of Naidoo describes functionality of the security server in authenticating the remote user. Once the remote user is authenticated, Naidoo only teaches that the remote user may access some or all of the features of base station. Naidoo therefore only teaches the participation of the security server in providing a remote user access to features of the base station. Accordingly, Naidoo does not disclose coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

Further regarding claim 1, Naidoo describes that application server 734 (component of security server) generally provides or facilitates all of the functionality that is accessible to remote clients 155 (paragraph 0102). Naidoo describes that application server 734 may access automation system server 720 to obtain account information and issue commands ultimately destined for security gateway 115. Communication between application server 734 and automation system server 720 may take the form of calls to stored procedures defined in the master database maintained by automation system server 720 (paragraph 0103). The issuance of commands and stored procedures destined for the security gateway facilitates remote client access to security gateway features but does not teach maintaining on the security server objects corresponding to at least one of the security system components and the plurality of premise devices. Accordingly, Naidoo does not disclose coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway

communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

Naidoo further teaches that remote user 155 may connect to security system server 131 and base station 115 (after authentication) through network 120. Because a remote user does not necessarily need real-time access to alarm video, a low bandwidth connection may be used to connect remote station 155 to security system server 131 and base station 115. After authentication, security system server 131 may be configured to create a data connection between remote station 155 and security gateway 115 such that communications between remote station 155 and security gateway 115 bypass security system server 131 (paragraph 0041). Naidoo clearly teaches that after authentication, remote user may communicate with security gateway directly, thereby bypassing security system server. Accordingly Naidoo teaches directly away from maintaining on the security server objects corresponding to at least one of the security system components and the plurality of premise devices. Accordingly, Naidoo does not disclose coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

Further regarding claim 1, Applicant submits that Naidoo describes (with reference to FIG. 8) a flowchart diagram illustrating operation of an embodiment in authenticating and allowing remote access to features of security system (paragraph 0108). Naidoo describes that in step 905, remote terminal 155 may connect to the website (paragraph 0109). In step 910, remote user 155 provides the website with identification information, for example a username and password (paragraph 0110). The website interfaces with authentication system server 720 to verify the identification information in step 920 (paragraph 0111). If the information is correct, the user may access the account portion of the website 940 (paragraph 0112). In addition, in step 950, media

handler 715 provides the remote client 157 with an access token that is digitally signed by the media handler 715 (paragraph 0113).

Naidoo describes that the remote client 155 may then connect directly to security gateway 115 and provide security gateway 115 with the access token 955. It is noted that the term "direct connection" means that communications between the remote client 155 and security gateway 115 do not pass through security system server 131. The security gateway 115 inspects the token and is configured to trust valid digital signatures of the security system server. Accordingly, the presence of the token in the web page allows the remote client 157 to access audio and video from the customer's security gateway 115 without the need for all communication to be transmitted through data center 132 (paragraph 0114). Accordingly, the remote user may then connect directly to security gateway 115 to perform remote surveillance through security gateway 115, check the system status, initiate a two-way audio conference, and/or any other features made available by security gateway 115 and falling within the user's permissions (paragraph 0115). As indicated above, Naidoo again discloses an embodiment teaching a remote user communicating directly with security gateway, thereby bypassing a security system server. Accordingly Naidoo teaches directly away from maintaining on the security server objects corresponding to at least one of the security system components and the plurality of premise devices. Accordingly, Naidoo does not disclose coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo. Applicant finds no teaching in Bilger to overcome the deficiencies of Naidoo set forth above.

Applicant respectfully submits that Bilger describes a home automation system interface and method for interfacing with a system that automatically controls controlled devices throughout a home. A unique architecture of occupancy sensors includes

entry/exit sensors for detecting movement through doorways that separate rooms in the home, room motion sensors for detecting room occupancy, spot sensors to detect occupancy of specific locations within the rooms, and house status sensors to detect the status of certain parameters of the home. A central controller communicates with the sensors and controlled objects over a communications network, where the sensors and controlled objects can be added to the system in a 'plug and play manner (abstract).

FIG. 7 A illustrates the preferred configuration for network 14, which includes a control/sensor network 52 wired to each "room" 4 in the house. Control/sensor network 52 is a single set of wires bused throughout the house, preferably while the house is under initial construction. Once the AC power lines are installed but before the walls are completed, the network wiring can be easily installed in just one day, often times using the same holes, conduit and/or junction boxes as the AC lines. The control/sensor network 52 is connected to all the sensors 10 and controlled objects 12, as well as to the central controller 16 (column 9, lines 56-66).

FIG. 7A illustrates a random configuration for control/sensor network 52. FIGS. 7B-7D illustrate alternate configurations for routing control/sensor network 52 through the house. A single set of wires can be woven throughout the house in a straight bus or daisy chain configuration, as illustrated in FIG. 7B. The central controller could have one 15 or more central hubs 58 that have individual communications lines 60 each connected to a single sensor 10 or controlled object 12, as illustrated in FIG. 7C. The advantage of this embodiment is that the sensors 10 and controlled objects 12 can use standard Ethernet twisted pair connectors and hubs, but the drawback is that the system is less versatile, and more costly to wire. Alternately, the control/sensor network 52 could be wireless, where each sensor 10 and controlled object 12 including a transceiver 54 that communicates with one or more central transceivers 56 of the central controller 16 (as illustrated in FIG. 7D), or with other transceivers 54 in a token bus configuration (as illustrated in FIG. 7E). Lastly, control/sensor network 52 could be a powerline based system (e.g. X-10 system), where the sensors 10 controlled objects 12 and central controller 16 communicate with each other over the existing AC power lines in the house (column 10, lines 9-31). None of these embodiments teach coupling a gateway to a local area network located in a first location and a security server in a second location

(emphasis added). Therefore, Bilger clearly does not teach coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo in view of Bilger. Applicant finds no teaching in Rezvani to overcome the deficiencies of Naidoo in view of Bilger.

Applicant respectfully submits that Rezvani describes systems and methods for providing registration at a remote site that may include, for example, a monitoring module that may communicate with a remote site (abstract). Devices at one or more locations may interface with the monitoring modules. Rezvani describes that one or more monitoring modules and their associated interfaced devices may be referred to as "installations." Devices may include, for example, video cameras, still cameras, motion sensors, audible detectors, any suitable household appliances, or any other suitable device. Rezvani describes that monitoring modules may be stand-alone devices, software applications, any suitable combination of software and hardware, or any other suitable architecture (column 1, lines 41-50).

Rezvani describes that monitoring modules may communicate with one or more remote sites via a suitable communications network using any suitable communications protocol. The monitoring modules and remote sites may use a registration protocol to transmit registration information. The registration information may get stored in a database at the remote site (column 1, lines 51-56).

Rezvani describes that an installation, any of its components, or both may be associated with a particular user account (column 1, lines 59-60). Association of an installation, installation elements, or both with corresponding user accounts may take place at the remote site. The remote site may make the association using any suitable database construct that may serve to cross reference the installation, installation elements, or both with user accounts (column 1, line 65 to column 2, line 3).



Rezvani describes that devices may be automatically detected by a monitoring module (column 2, lines 37-38). Rezvani describes that as new devices are added to a registered monitoring module, the monitoring module may automatically (i.e., without any user interaction) detect the presence of the new devices and automatically notify remote site of the presence of the new devices. Remote site may, in turn, add the new devices to the database (column 21, lines 5-11).

Although Rezvani discloses the automatic detection of devices, the detected device information is directed to and registered at a remote site. Rezvani teaches automatically detecting a device at an installation, extracting registration information from the device, communicating the registration information to a remote site that does not have requisite registration information associated with the device using a communications network, registering the device with the remote site based on the registration information, and associating the device at the remote site with a user account based on the registration information (claim 1, column 21, lines 41-53). Rezvani therefore teaches the automatic detection and extraction of registration information from devices at a first location (an installation), the communication of the registration information to a remote location, registration of devices at the remote location using the extracted information and the association of the devices at the remote site with a user account. However, the association of devices with a user account does not disclose (and Rezvani does not otherwise teach) coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani.

As claims 2-3, 5-9, 11, 12, 15-25, 28, 30-45, 48 and 52 depend from amended claim 1 and include further limitations thereon, and since amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani, Applicant submits that claims 2-3, 5-9, 11, 12, 15-25, 28, 30-45, 48 and 52 are patentable over by Naidoo in

view of Bilger and further in view of Rezvani.

Claims 10 and 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Tanaka et al., US Patent Application Publication number US 2004/0037295 A1 ("Tanaka").

At page 16 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the connection management component automatically configures the premise devices for operation in the security network". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claims 10 and 29 which depend from amended claim 1, Applicant does not find any teaching in Tanaka that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 10 and 29 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Tanaka and respectfully requests that the rejection be withdrawn and allowance thereof.

Claim 26 was rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Patterson, US Patent Application Publication number US 2005/0086126 A1 ("Patterson").

At page 18 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the security server creates, modifies and terminates users corresponding to the security system". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claim 26 which depends from amended claim 1, Applicant does not find any teaching in Patterson that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits

that claim 26 is patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Patterson and respectfully requests that the rejection be withdrawn and allowance thereof.

Claim 27 was rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moyer et al., US Patent Application Publication number US 2002/0103898 A1 (“Moyer”).

At page 19 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the security server creates, modifies and terminates couplings between the gateway and the security system components". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claim 27 which depends from amended claim 1, Applicant does not find any teaching in Moyer that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claim 27 is patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moyer and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 46-47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Lingemann, US Patent Application Publication number US 2006/0009863 A1 (“Lingemann”).

At page 20 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the network device is a touchscreen". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claims 46-47 which depend from amended claim 1, Applicant does not find any teaching in Lingemann that overcomes the deficiencies in Naidoo in view of Bilger and

Attorney Docket No. ICON.P001D3

further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 46-47 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Lingemann and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 13-14 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moore et al., US Patent Application Publication number US 2007/0061266 A1 ("Moore").

At page 21 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "the premise local area network is coupled to a wide area network via a premise router". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claims 13-14 which depend from amended claim 1, Applicant does not find any teaching in Moore that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 13-14 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moore and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 49-51 were rejected as being unpatentable over Naidoo in view of Rezvani.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo in view of Rezvani does not teach or suggest each and every limitation of amended claim 49 and, as such, amended claim 49 is patentable over Naidoo in view of Rezvani. For at least these reasons, Applicant submits that amended claim 49 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and allowance therefore.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo in view of Rezvani does not teach or suggest each and every limitation of amended claim 50 and, as such, amended claim 50 is patentable over Naidoo

Attorney Docket No. ICON.P001D3

in view of Rezvani. For at least these reasons, Applicant submits that amended claim 50 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and allowance therefore.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo in view of Rezvani does not teach or suggest each and every limitation of amended claim 51 and, as such, amended claim 51 is patentable over Naidoo in view of Rezvani. For at least these reasons, Applicant submits that amended claim 51 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and allowance therefore.

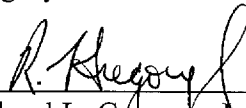
Further regarding claims 49-51, the Office Action states at pages 23, 25 and 26 that Naidoo does not explicitly teach the step of "automatically discovering the plurality of network devices at the gateway". Applicant agrees.

#### Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully submit that the rejections under 35 U.S.C. §103 have been overcome, and their withdrawal is respectfully requested. Applicants submit that claims 1-3 and 5-52 are in condition for allowance. The allowance of the claims is earnestly requested. If in the opinion of Examiner Mejia a telephone conference would expedite the prosecution of the subject application, or if there are any issues that remain to be resolved prior to allowance of the claims, Examiner Mejia is encouraged to call Rick Gregory at 408.821.8080.

Respectfully submitted,  
Gregory & Sawrie LLP

Date: July 17, 2012

  
Richard L. Gregory, Jr., Reg. No. 42,607  
Telephone: 408.821.8080

Gregory & Sawrie LLP  
2018 Bissonnet Street  
Houston, Texas 77005  
Fax: 713-364-1397

Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> <b>FY 2009</b> <i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i>		Docket Number (Optional) ICON.P001D3	
Application Number 12/189,788		Filed August 12, 2008	
For Forming A Security Network Including Integrated Security System Components and Network Devices			
Art Unit 2451		Examiner MEJIA, Anthony	
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.			
The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):			
		<u>Fee</u>	<u>Small Entity Fee</u>
<input type="checkbox"/>	One month (37 CFR 1.17(a)(1))	\$130	\$65 \$ _____
<input type="checkbox"/>	Two months (37 CFR 1.17(a)(2))	\$490	\$245 \$ _____
<input checked="" type="checkbox"/>	Three months (37 CFR 1.17(a)(3))	\$1110	\$555 \$ <u>635</u>
<input type="checkbox"/>	Four months (37 CFR 1.17(a)(4))	\$1730	\$865 \$ _____
<input type="checkbox"/>	Five months (37 CFR 1.17(a)(5))	\$2350	\$1175 \$ _____
<input checked="" type="checkbox"/>	Applicant claims small entity status. See 37 CFR 1.27.		
<input type="checkbox"/>	A check in the amount of the fee is enclosed.		
<input checked="" type="checkbox"/>	Payment by credit card. Form PTO-2038 is attached.		
<input type="checkbox"/>	The Director has already been authorized to charge fees in this application to a Deposit Account.		
<input type="checkbox"/>	The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number _____.		
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>			
I am the	<input type="checkbox"/>	applicant/inventor.	
	<input type="checkbox"/>	assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).	
	<input checked="" type="checkbox"/>	attorney or agent of record. Registration Number <u>42,607</u>	
	<input type="checkbox"/>	attorney or agent under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____	
<u>/Richard L. Gregory, Jr./</u>		<u>July 17, 2012</u>	
Signature		Date	
<u>Richard L. Gregory, Jr.</u>		<u>408-821-8080</u>	
Typed or printed name		Telephone Number	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.			
<input checked="" type="checkbox"/>	Total of <u>1</u> forms are submitted.		

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12189788
<b>Filing Date:</b>	12-Aug-2008
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Filer:</b>	Richard L. Gregory/David Sawrie
<b>Attorney Docket Number:</b>	ICON.P001D3

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
Claims in excess of 20	2202	1	30	30

**Miscellaneous-Filing:**

**Petition:**

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

**Extension-of-Time:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 3 months with \$0 paid	2253	1	635	635
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>665</b>



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	13276596
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	98195
<b>Filer:</b>	Richard L. Gregory/David Sawrie
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	17-JUL-2012
<b>Filing Date:</b>	12-AUG-2008
<b>Time Stamp:</b>	21:54:46
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$665
RAM confirmation Number	6851
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / zip (if appl.)	Pages (if appl.)
SecureNet Technologies, LLC Exhibit 1003 Page 209					

1		ICON_P001D3_filed_response_17JUL2012.pdf	3383745 dee23aa6b91b4bf5978cd11669eed01698b1872b	yes	23
<b>Multipart Description/PDF files in .zip description</b>					
		<b>Document Description</b>	<b>Start</b>	<b>End</b>	
		Amendment/Req. Reconsideration-After Non-Final Reject	1	1	
		Claims	2	9	
		Applicant Arguments/Remarks Made in an Amendment	10	22	
		Extension of Time	23	23	
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (SB06)	fee-info.pdf	32186 007175df1025ffcbed1ca4a51f471f9e04343dd7	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			3415931		
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/189,788</b>	Filing Date <b>08/12/2008</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	<b>07/17/2012</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 51	Minus ** 51	= 0	X \$30 =	0	OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus ***4	= 0	X \$125 =	0	OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE	<b>0</b>	OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	X \$ =		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	X \$ =		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /MARSHA RICHARDS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

2010Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		4,779,007	A	Schlanger et al.	10-18-1988	
		4,860,185	A	Brewer et al.	08-22-1989	
		5,086,385	A	Launey et al.	02-04-1992	
		5,519,878		Dolin, Jr.	05-21-1996	
		5,579,197	A	Mengelt et al.	11-26-1996	
		5,963,916	A	Kaplan, Joshua D.	10-05-1999	
		5,991,795		Howard et al.	11-23-1999	
		6,037,991		Thro et al.	03-14-2000	
		6,052,052	A	Delmonaco	04-18-2000	
		6,140,987	A	Stein et al.	10-31-2000	
		6,198,475	B1	Humpleman et al.	03-06-2001	
		6,219,677	B1	Howard	04-17-2001	
		6,286,038		Reichmeyer et al.	09-04-2001	
		6,288,716	B1	Humpleman et al.	09-11-2001	
		6,331,122	B1	Wu	12-18-2001	
		6,353,891	B1	Borella et al.	03-05-2002	
		6,363,417	B1	Howard et al.	03-26-2002	
		6,370,436	B1	Howard et al.	04-09-2002	
		6,377,861	B1	York	04-23-2002	
		6,462,507	B2	Fisher, Jr	10-08-2002	

**FOREIGN PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				
		WO	89/07855		Bavco Manufacturing Company	08-24-1989		
		JP	2003/085258	A	Yamatate Building System Co. Ltd.	09-13-2001		
		JP	2003/141659		Yamatate Building System Co. Ltd.	10-31-2001		
		JP	2004/192659		Sony Corp.	02-27-2004		
		KR	2006/0021605		Daewoo Electronics Corp.	09-03-2004		
		WO	2001/052478		Invensys Controls PLC	07-19-2001		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2451
		First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		6,462,663		Wilson et al.	10-08-2002	
		6,467,084	B1	Howard et al.	10/15/2002	
		6,480,901	B1	Weber et al.	11-12-2002	
		6,493,020	B1	Stevenson et al.	12-10-2002	
		6,496,927	B1	McGrane	12-17-2002	
		6,529,723	B1	Bentley	03-04-2003	
		6,542,075		Barker et al.	04-01-2003	
		6,563,800		Salo et al.	05-13-2003	
		6,574,234	B1	Myer et al.	06-03-2003	
		6,580,950	B1	Johnson et al.	06-17-2003	
		6,587,736	B2	Howard et al.	07-01-2003	
		6,591,094	B1	Bentley	07-08-2003	
		6,601,086	B1	Howard et al.	07-29-2003	
		6,609,127	B1	Lee et al.	08-19-2003	
		6,615,088	B1	Myer et al.	09-02-2003	
		6,643,652	B2	Helgeson et al.	11-04-2003	
		6,643,669	B1	Novak et al.	11-04-2003	
		6,648,682	B1	Wu	11-18-2003	
		6,658,091		Naidoo et al.	12-02-2003	
		6,721,689		Markle et al.	04-13-2004	

**FOREIGN PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				
		WO	2001/099078		Eutech Cybernetics Inc.	12-27-2001		
		WO	2004/107710		LG Electronics Inc.	12-09-2004		
		WO	2004/004222		Thomson Licensing SA	01-08-2004		
		WO	2005/091218	A2	iControl Networks, Inc. without Search Report	09-29-2005		
		WO	2005/091218	A3	iControl Networks, Inc. Search Report	09-29-2005		

Examiner Signature	Date Considered
--------------------	-----------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		6,721,747	B2	Lipkin, Daniel S.	04-13-2004	
		6,756,998		Bilger, Brent	06-29-2004	
		6,789,147	B1	Kessler et al.	09-07-2004	
		6,795,322	B2	Aihara et al.	09-21-2004	
		6,826,233		Oosawa, Hajime	11-30-2004	
		6,865,690	B2	Kocin	03-08-2005	
		6,912,429	B1	Bilger, Brent	06-28-2005	
		6,930,730	B2	Maxon et al.	08-16-2005	
		6,931,445	B2	Davis James S.	08-16-2005	
		6,959,393	B2	Hollis et al.	10-25-2005	
		6,990,591		Pearson, Sterling Michael	01-24-2006	
		7,016,970		Harumoto et al.	03-21-2006	
		7,024,676		Klopfenstein, Scott E.	04-04-2006	
		7,034,681		Yamamoto et al.	04-25-2006	
		7,047,088	B2	Nakamura et al.	05-16-2006	
		7,047,092	B2	Wimsatt, William	05-16-2006	
		7,072,934	B2	Helgeson et al.	07-04-2006	
		7,099,994	B1	Anschultz	08-29-2006	
		7,130,585	B1	Ollis et al.	10-31-2006	
		7,148,810		Bhat, Ishwara A.	12-12-2006	
		7,174,564	B1	Weatherspoon et al.	02-06-2007	
		7,183,907		Simon et al.	02-27-2007	
		7,203,486	B2	Patel, Ashish Raojibhai	04-10-2007	
		7,222,359	B2	Freund et al.	05-22-2007	
		7,237,267	B2	Rayes et al.	06-26-2007	
		7,305,461	B2	Ullmann, Lorin Evan	12-04-2007	
		7,337,217	B2	Wang, Dongyan	02-26-2008	
		7,337,473	B2	Chang et al.	02-26-2008	
		7,343,619	B2	Ofek et al.	03-11-2008	
		7,349,761		Cruse	03-25-2008	
		7,349,967	B2	Wang, Dongyan	03-25-2008	
		7,367,045	B2	Ofek et al.	04-29-2008	
		7,370,115		Bae et al.	05-06-2008	

Examiner Signature	Date Considered
--------------------	-----------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

## U.S. PATENT DOCUMENTS

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		7,383,339	B1	Meenan et al.	06-03-2008	
		7,403,838	B2	Deen et al.	07-22-2008	
		7,409,451	B1	Meenan et al.	08-05-2008	
		7,428,585	B1	Owens et al.	09-23-2008	
		7,430,614		Shen et al.	09-30-2008	
		7,440,434		Chaskar et al.	10-21-2008	
		7,457,869	B2	Kernan, Timothy S.	11-25-2008	
		7,469,139	B2	van de Groenendaal Joannes G.	12-23-2008	
		7,469,294		Luo et al.	12-23-2008	
		7,480,713	B2	Ullmann, Lorin Evan	01-20-2009	
		7,480,724	B2	Zimler et al.	01-20-2009	
		7,506,052	B2	Qian et al.	03-17-2009	
		7,509,687	B2	Ofek et al.	03-24-2009	
		7,526,762		Astala et al.	04-28-2009	
		7,558,379	B2	Winick, Steven	07-07-2009	
		7,577,420	B2	Srinivasan et al.	08-18-2009	
		7,587,464	B2	Moorer et al.	09-08-2009	
		7,634,519	B2	Creamer et al.	12-15-2009	
		2001/0034754	A1	Elwahab et al.	10-25-2001	
		2002/0004828	A1	Davis et al.	01-10-2002	
		2002/0026476	A1	Miyazaki et al.	02-28-2002	
		2002/0029276	A1	Bendinelli et al.	03-07-2002	
		2002/0038380	A1	Brawn et al.	03-28-2002	
		2002/0052913	A1	Yamada et al.	05-02-2002	
		2002/0083342	A1	Webb et al.	06-27-2002	
		2002/0095490		Barker et al.	07-18-2002	
		2002/0103898	A1	Moyer et al.	08-01-2002	
		2002/0103927	A1	Parent, Jesse L.	08/01/2002	
		2002/0107910		Zhao	08-08-2002	
		2002/0111698	A1	Graziano et al.	08-15-2002	
		2002/0112051	A1	Ullmann, Lorin Evan	08-15-2002	
		2002/0112182	A1	Chang et al.	08-15-2002	
		2002/0143923		Alexander, Bruce	10-03-2002	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2451
		First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

## U.S. PATENT DOCUMENTS

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		2002/0156564	A1	Preston et al.	10-24-2002	
		2002/0180579	A1	Nagoka et al.	12-05-2002	
		2002/0184301	A1	Parent, Jesse L.	12-05-2002	
		2003/0009552	A1	Benfield et al.	01-09-2003	
		2003/0009553	A1	Benfield et al.	01-09-2003	
		2003/0041167	A1	French et al.	02-27-2003	
		2003/0051009	A1	Shah et al.	03-13-2003	
		2003/0052923	A1	Porter, Swain W.	03-20-2003	
		2003/0062997	A1	Naidoo et al.	04-03-2003	
		2003/0090473	A1	Joshi, Vikas B.	05-15-2003	
		2003/0115345		Chien et al.	06-19-2003	
		2003/0132018	A1	Okita et al.	07-17-2003	
		2003/0174648	A1	Wang, Mea	09-18-2003	
		2003/0187920		Redkar	10-02-2003	
		2003/0210126		Kanazawa	11-13-2003	
		2003/0236841		Epshteyn	12-25-2003	
		2004/0003241		Sengodan et al.	01-01-2004	
		2004/0015572		Kang	01-22-2004	
		2004/0037295	A1	Tanaka et al.	02-26-2004	
		2004/0054789	A1	Breh et al.	03-18-2004	
		2004/0086088	A1	Naidoo et al.	05-06-2004	
		2004/0139227	A1	Takeda, Yutaka	07-15-2004	
		2004/0162902	A1	Davis James S.	08-19-2004	
		2004/0177163	A1	Casey et al.	09-09-2004	
		2004/0243835	A1	Terzis et al.	12-02-2004	
		2004/0267937	A1	Klements, Anders E.	12-30-2004	
		2005/0038326		Mathur	02-17-2005	
		2005/0066045	A1	Johnson et al.	03-24-2005	
		2005/0069098	A1	Kalervo et al.	03-31-2005	
		2005/0079855		Jethi et al.	04-15-2005	
		2005/0086126	A1	Patterson, Russell D.	04-21-2005	
		2005/0108091	A1	Sotak et al.	05-19-2005	
		2005/0108369	A1	Sather et al.	05-19-2005	
		2005/0125083	A1	Kiko	06-09-2005	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.



Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		2005/0128083	A1	Puzio et al.	06-16-2005	
		2005/0149639	A1	Vrieling et al.	07-07-2005	
		2005/0169288		Kamiwada et al.	08-04-2005	
		2005/0197847		Smith	09-08-2005	
		2005/0216302		Raji et al.	09-29-2005	
		2005/0216580	A1	Raji et al.	09-29-2005	
		2005/0222820	A1	Chung	10-06-2005	
		2005/0231349	A1	Bhat, Ishwara A.	10-20-2005	
		2006/0009863	A1	Lingemann, Ronald R.	01-12-2006	
		2006/0088092	A1	Chen et al.	04-27-2006	
		2006/0105713	A1	Zheng et al.	05-18-2006	
		2006/0181406		Petite et al.	08-17-2006	
		2006/0182100	A1	Li et al.	08-17-2006	
		2006/0187900	A1	Akbar, Imran M.	08-24-2006	
		2006/0200845	A1	Foster et al.	09-07-2006	
		2007/0052675		Chang	03-08-2007	
		2007/0061266	A1	Moore et al.	03-15-2007	
		2007/0106124		Kuriyama et al.	05-10-2007	
		2007/0286210		Gutt et al.	12-13-2007	
		2007/0286369		Gutt et al.	12-13-2007	
		2007/0298772	A1	Owen et al.	12-27-2007	
		2008/0042826	A1	Hevia et al.	02-21-2008	
		2008/0065681	A1	Fontijn et al.	03-13-2008	
		2008/0084296	A1	Kutzik et al.	04-10-2008	
		2008/0147834		Quinn et al.	06-19-2008	
		2008/0180240		Raji et al.	07-31-2008	
		2008/0183842		Raji et al.	07-31-2008	
		2008/0235326		Parsi et al.	09-25-2008	
		2009/0070436	A1	Dawes et al.	03-12-2009	
		2009/0165114	A1	Baum et al.	06-25-2009	
		2009/0204693		Andreev et al.	08-13-2009	
		2009/0240787	A1	Denny, Michael S.	09-24-2009	
		2009/0240814	A1	Brubacher et al.	09-24-2009	
		2010/0082744		Gutt	04-01-2010	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		2010/0095111		Gutt	04-15-2010	
		2010/0095369		Gutt	04-15-2010	
		D416,910		Vasquez	11-23-1999	
		D451,529	S	Vasquez	12-04-2001	
		D464,328	S	Vasquez et al.	10-15-2002	
		D464,948	S	Vasquez et al.	10-29-2002	
		2006/0282886	A1	Gaug, Mark	12-14-2006	
		7,627,665	B2	Barker et al.	10-03-2002	
		6,928,148	B2	Simon et al.	12-13-2001	
		7,551,071	B2	Bennett, III et al.	10-05-2006	
		2004/0123149	A1	Tyroler	06-24-2004	

Examiner Signature	Date Considered
-----------------------	-----------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2451
	First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**NON PATENT LITERATURE DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		Form PCT/ISA/220, ICON.P011WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P011WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P011WO, "PCT Written Opinion of the International Searching Authority," 8 pgs.	
		Form PCT/ISA/220, ICON.P012WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P012WO, "PCT International Search Report," 2 pgs	
		Form PCT/ISA/237, ICON.P012WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P0014WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P014WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P014WO, "PCT Written Opinion of the International Searching Authority," 7 pgs.	
		Form PCT/ISA/220, ICON.P0015WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P015WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P015WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, PCT/US05/08766, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, PCT/US05/08766, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, PCT/US05/08766, "PCT Written Opinion of the International Searching Authority," 5 pgs.	

Examiner Signature	Date Considered
--------------------	-----------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.** If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2451
		First Named Inventor: Marc Baum	Examiner Name: Anthony Mejia

**NON PATENT LITERATURE DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		Examination Report under Section 18(3) re UK patent application no. GB0724760.4 dated January 30, 2008 4 pgs	
		Examination Report under Section 18(3) re UK patent application no. GB0724248.0 dated January 30, 2008 4 pgs	
		Examination Report under Section 18(3) re UK patent application no. GB0724248.0 dated June 4, 2008 2 pgs	
		Examination Report under Section 18(3) re UK patent application no. GB0800040.8 dated January 30, 2008 4 pgs	
		Examination Report under Section 18(3) re UK patent application no. GB0620362.4 dated August 13, 2007, 3 pgs	
		Alarm.com - Interactive Security Systems, Product Advantages, printed from website 11/4/2003, 3 pp	
		Alarm.com - Interactive Security Systems, Frequently Asked Questions, printed from website 11/4/2003, 3 pp	
		Alarm.com - Interactive Security Systems, Elders, printed from website 11/4/2003, 1 page	
		Alarm.com - Interactive Security Systems, Overview, printed from website 11/4/2003, 2 pp	
		X10 - ActiveHome, Home Automation Made Easy!, printed from website 11/4/2003, 3 pp	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification 4 : <b>H02J 9/06, H05B 41/04</b></p>	<p><b>AI</b></p>	<p>(11) International Publication Number: <b>WO 89/ 07855</b> (43) International Publication Date: 24 August 1989 (24.08.89)</p>
--	------------------	--

(21) International Application Number: PCT/US88/00515  
 (22) International Filing Date: 22 February 1988 (22.02.88)

(71) Applicant: BAVCO MANUFACTURING COMPANY  
 [US/US]; 14 Buenavista Street, Saugus, MA 01906 (US).

(72) Inventor: BAVARO, Joseph, P. ; 14 Buenavista Street, Saugus, MA 01906 (US).

(74) Agent: KRANSDORF, Ronald, J.; Wolf, Greenfield & Sacks, Federal Reserve Plaza, 600 Atlantic Avenue, Boston, MA 02210 (US).

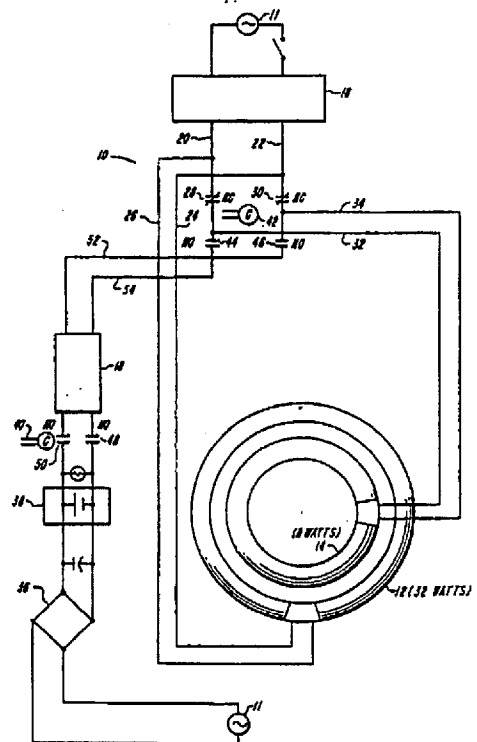
(81) Designated States: AT (European patent), BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent).

**Published**  
*With international search report.*

(54) Title: **BACKUP ELECTRICAL SYSTEM FOR LAMPS**

(57) Abstract

A backup power system is provided for fluorescent or other gas discharge lamps which energizes one of the lamps when normal AC mains power is not available. The circuit operates with a standard lamp fixture which contains two or more fluorescent lamps. When AC mains current is available, both lamps are operational so that the lighting fixture produces a maximum brightness. The AC mains current also trickle-charges a low-voltage battery contained in the lighting fixture. When mains current is not available, the battery maintains only one of the lamps lighted. Consequently, although the lighting fixture produces a reduced output, the battery life is extended. In one embodiment both fluorescent lamps are powered directly from the AC line. When AC power is not available, a relay disconnects the AC line from both lamps and connects one lamp to a DC/AC inverter which is powered by the internal battery. In another embodiment, one lamp is powered directly from the AC line and the other lamp is powered by a DC/AC inverter which receives power either from a DC power supply operating off the AC line or from the internal low-voltage battery. In a third embodiment, during normal operating conditions, both lamps are powered by separated DC/AC inverters driven from a power supply that operates off the AC line. When the AC voltage is not present, the DC/AC inverter for one lamp is powered by the internal low-voltage battery.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FR	France	ML	Mali
AU	Australia	GA	Gabon	MR	Mauritania
BB	Barbados	GB	United Kingdom	MW	Malawi
BE	Belgium	HU	Hungary	NL	Netherlands
BG	Bulgaria	IT	Italy	NO	Norway
BJ	Benin	JP	Japan	RO	Romania
BR	Brazil	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	LI	Liechtenstein	SN	Senegal
CH	Switzerland	LK	Sri Lanka	SU	Soviet Union
CM	Cameroon	LU	Luxembourg	TD	Chad
DE	Germany, Federal Republic of	MC	Monaco	TG	Togo
DK	Denmark	MG	Madagascar	US	United States of America
FI	Finland				

## BACKUP ELECTRICAL SYSTEM FOR LAMPS

Field of the Invention

This invention relates to a backup system for lamps, particularly an electrical backup system for ballast powered lamps.

The Prior Art

Attempts have been made in the prior art to provide emergency or backup lighting where the normal lighting is supplied by fluorescent lamps and the normal power is alternating current from a commercial utility source.

Examples of such attempts are USP 4,454,452 to Feldstein (1984) and USP 4,486,689 to Davis (1984). Both these references teach the use of a hard-to-find emergency lamp in place of a regular fluorescent lamp in which a considerable portion of the lamp tube is taken up by self-contained components such as a battery package and an electrical sensing and switching assembly, leaving but a portion of the tube to house a reduced sized lamp or a series of even smaller lights with consequent diminished lighting power.

These emergency lamps moreover run off a regular ballast which powers one or more regularly

-2-

used lamps, which ballast can burn out, (i.e. the emergency or standby lamp does not have its own standby ballast).

Accordingly, there is a need and market for an emergency or standby lighting system which employs easy-to-find standard sized ballast powered lamps and which substantially overcomes the above prior art shortcomings.

There has now been developed a backup lighting system for ballast powered lamps which employs standard available lamps. By "ballast powered" lamps, as used herein, is meant fluorescent lamps, mercury vapor lamps or high-pressure sodium lamps.

#### Summary of the Invention

Broadly, the present invention provides a backup power system for two or more fluorescent lamps in which several lamps are lighted during normal operating conditions when AC line power is present. When AC power is not present, only one lamp is lighted by means of an internal battery-driven, high-frequency DC/AC inverter. The high-frequency inverter operates one lamp with high efficiency thereby extending battery life and reducing heat buildup which can damage the internal battery.



-3-

In one embodiment of the invention, one or more lamps are powered by the AC line current through a standard A.C. line ballast. Another lamp is connected through relay contacts to the ballast so that when the AC line current is available, the lamp is powered by the AC line current. When the AC line current is removed, the relay releases and connects the other lamp to a DC/AC inverter which is in turn driven by a low voltage DC battery located in the lamp fixture.

In another embodiment of the invention, one or more fluorescent lamps is driven by a standard AC line ballast as in the previous embodiment. However, the other "emergency" lamp is driven by high-frequency AC current from a DC/AC inverter which is, in turn, operated from a low-voltage power supply powered from the AC line current. When the AC line current disappears, an AC line voltage sensor connects a low voltage internal battery to the DC/AC inverter which continues to power the emergency fluorescent lamp.

In yet a third embodiment, all of the lamps are powered with high-frequency AC current from DC/AC inverters. The inverters are, in turn, driven by a low-voltage rectified power supply which is operates off the AC line voltage. As with the previous embodiment, during an emergency situation, a line voltage sensor connects the internal battery to one of the DC/AC converters to power one lamp.

-4-

Brief Description of the Drawings

The invention will become more apparent from the following detailed specification and drawings.

Fig. 1 is a schematic diagram of a backup power system for fluorescent lamps with an AC power supply and with a backup D/C power source, embodying the invention.

Fig. 2 is a bottom plan view of the physical layout of the components of the backup power system for fluorescent lamps as shown in Fig. 1.

Fig. 3 is an electrical schematic diagram of a two-lamp embodiment of the invention in which one fluorescent lamp is powered from a standard AC line ballast while the second fluorescent lamp is powered from a DC/AC inverter.

Fig. 4 is an electrical schematic diagram of a two-lamp embodiment of the invention in which both fluorescent lamps are powered by DC/AC inverters.

Fig. 5 is a more detailed electrical schematic diagram of the D.C. power supply and wall switch control used in certain embodiments of the present invention.

Fig. 6 is a more detailed electrical schematic diagram of the battery charging circuit and the line

-5-

voltage sensor used in certain embodiments of the present invention.

#### Detailed Description

Referring in more detail to the drawings, the lighting fixture 10 includes a pair of circle fluorescent lamps in which the outer circle lamp 12 draws 32 watts and the inner circle lamp 14 draws 8 watts, as shown in Fig. 1. A regular ballast 16 drives the two circle lamps, powered by 115 volts AC, while a DC/AC inverter 18 powers the inner circle lamp 14 in the event of interruption of the 115 volts AC, as indicated in Fig. 1.

DC/AC inverter 18 is a conventional and well-known device which converts low-voltage DC power into AC power. It may illustratively consist of a one transistor or two transistor blocking or relaxation oscillator or other similar oscillating circuit. The oscillating circuit operates from a low voltage DC power source and drives a step-up transformer to increase the low voltage to a suitable higher voltage value to drive the fluorescent lamps. Advantageously, the oscillation frequency is relatively high (15-30 KHz) which high frequency allows the fluorescent lamps to operate efficiently, thereby reducing heat buildup.

More specifically, the circuitry is connected as follows. 115 volts AC from power supply 11 is

-6-

applied to the regular ballast 16, which outputs a signal on conductors 20, 22, 24 and 26 to illuminate circle lamp 12, while outputting a signal across normally closed switches 28 and 30 and conductors 32 and 34 to illuminate inner circle lamp 14, as shown in Fig. 1. At the same time 115 volts AC is applied across a trickle charger 36 to apply 12 volts DC to charge backup battery 38, as indicated by monitor light 13, as shown in Fig. 1. The charger 36 includes a transformer connected to a bridge diode, as indicated in Fig. 1.

When the 115 volt AC power supply goes down, coil relays 40 and 42 depower, causing normally closed switches 28 and 30 to open and normally open switches 44, 46, 48 and 50 to close, whereupon the battery 38 delivers 12 volts DC to the DC/AC inverter 18 which outputs a high-frequency AC signal on conductors 52, 54, 32 and 34 to illuminate circle lamp 14, to provide a battery-powered backup lamp for several hours.

When the power supply is restored, the relay coils 40 and 42 are again energized, closing normally closed switches 28 and 30 and opening normally open switches 44, 46, 48 and 50 to power the two circle lamps 14 and 12 by the regular 115 volts AC power supply while disconnecting the DC/AC inverter 18 and reapplying a charging voltage to the battery 38 as before, as shown in Fig. 1.

-7-

Similar push-to-test buttons can be connected across conductors 20 and 22 and across the conductors of the coils of relay switches 28, 30, 44, 46, 48 and 50 to simulate the discontinuance of the AC house current and connect the battery 38 to the DC/AC inverter 18 and the DC/AC inverter 18 in turn, to the standby circle lamp 14, to illuminate such lamp on a test basis.

Accordingly, when the power supply or house current is interrupted, in the case of Fig. 1, the outer circle lamp goes out but the inner circle lamp continues to be illuminated by battery power providing emergency lighting for several hours.

The backup power system of the invention applies to one or more lamps which can be straight or circular, as desired. That is, one lamp can be employed in the circular embodiment shown in Fig. 1, e.g. by removing circle lamp 12 therefrom and by employing the 8-watt circle lamp shown in Fig. 1, or replacing it with a lamp, either circular or straight of different wattage, as desired.

Preferably, however, two or more lamps are employed in the backup power system embodying the invention.

The backup or standby lamp can be of any desired wattage. However, the lower the wattage,

-8-

the longer it can be illuminated by a 12-volt battery. For example, a 32-watt lamp powered by such battery will give illumination for about one and one half hours, while an 8-watt lamp will give illumination for about four hours on such battery.

The backup power systems of the invention can illuminate various types of lamps such as fluorescent lamps, mercury vapor lamps and high pressure sodium lamps. The only change required for such various circuits is in the ratings of the components employed in the power systems of the invention, e.g. the ballast for a fluorescent lamp differs in rating from that of the mercury vapor and high pressure sodium lamps and can be replaced accordingly, but the respective circuits of the invention, e.g. as shown in Fig. 1, apply per the invention.

Moreover, the backup power systems embodying the invention can be employed with an on-off timer or a manual switch per the invention as long as the respective relay coils and battery chargers are supplied with constant AC power when such timer or manual switch turns off the lamps, to prevent false triggering of the standby circuit and lamps.

An example of the compact layout of the embodiment of the invention is shown in Fig. 2. Thus, backup lamp system housing 100 supports a

-9-

regular ballast 102, e.g. a 32 watt circular lamp 104 and a push-to-test, line AC voltage interrupter switch 105, as shown in Fig. 1. In addition, the housing 100 supports a battery charger 106, a battery 108, an N/O relay switch 109, a DC/AC inverter 110 and, e.g., an 8-watt circular lamp 112.

Thus, compact units of the backup lamp systems of the invention can be readily mounted in various rooms of a building, including windowless rooms.

Fig. 3 shows an additional embodiment of the invention in which two fluorescent lamps (shown schematically as lamps 400 and 402) are provided in one fixture. During normal operation, when A.C. line power is available, both lamps receive power from A.C. line 404. More specifically, AC line 404 is connected through a conventional wall switch 406 to a standard AC line ballast, 408, which, in turn, powers fluorescent lamp 400.

AC line 404 is also connected to primary winding 412 of an isolation/step-down transformer 410. Transformer 410 has a tapped secondary winding 418 consisting of two sections 414 and 416. Section 414 supplies AC power to a conventional low-voltage DC power supply 420. Power supply 420 (shown in detail in Fig. 5) may illustratively consist of a simple bridge rectifier and filtering circuit or may include a voltage limiter and regulator of

-10-

well-known design. A typical DC power supply 420 would receive an alternating current voltage of approximately 15-20 volts AC from winding 414 and produce a low-voltage (for example, 12 volts) DC output across output leads 421.

The DC voltage on leads 421 is applied to wall switch sensing unit 422. Unit 422 is connected in series with wall switch 406 across AC line 404 by sensing leads 424. When wall switch 406 is closed, the AC line voltage appears across leads 424, which voltage is detected by unit 422. Unit 422 thereupon connects the output of DC power supply 420 to inverter unit 424.

Inverter unit 424 is a standard DC/AC inverter which, as discussed above, may consist of a conventional oscillator and transformer circuit. When DC power is applied to such a circuit, it oscillates at high-frequency and produces a high frequency AC output at a voltage suitable to operate a fluorescent lamp. The high-frequency AC output is applied to a second fluorescent lamp 402.

Thus, during normal operation, lamp 401 is lighted directly from AC line 404 via line ballast 408 and fluorescent lamp 402 is driven by DC/AC inverter 424 which, in turn, receives DC power from power supply 420. Since both lights are on, the fixture produces maximum brightness.



-11-

In addition, during the normal operating cycle, a second section 416 of secondary winding 418 of transformer 410 is connected to battery charge circuit 426. Circuit 426 contains a conventional low-voltage power supply which generates a low-voltage trickle-charge current. This circuit may be as simple as a bridge rectifier with output filtering or may optionally include well-known regulation circuits.

Conventional battery charging circuits also include current limiting and overcharge protection circuitry. An illustrative battery charging circuit is shown in Fig. 7 and will be described further herein.

The output of the battery charger circuit is applied to a small low-voltage alkaline or gelatine-cell battery. Such a battery is small enough to be mounted entirely within the fluorescent fixture. However, because the battery output voltage is converted into high-frequency AC by inverter circuit 424, even a small battery is sufficient to drive lamp 402 for at least one and one-half hours because lamp 402 operates efficiently at high-frequencies.

The battery output on lead 428 is applied to a line voltage sensing circuit 430. This circuit (described in detail in connection with Fig. 6)

-12-

disconnects the battery output 428 from the input of the inverter circuit 424 during normal conditions when AC line voltage is present. Circuit 430 checks for the presence of AC line voltage by monitoring the DC battery-charging voltage produced by the battery charger 426. Since battery charger 326 operates from AC line 404, via transformer 410, the presence of the battery charging voltage indicates that the AC line voltage is present.

During an emergency, when the AC line voltage (and, consequently, the DC battery charging voltage) disappears, line voltage sensing circuit 430 connects the battery output 428 from the internal battery 426 through lead 432 to inverter 424. Thus, the battery 426 drives the inverter in place of the power supply 420. Thus, lamp 402 remains lighted. Lamp 400, of course, which operates through the standard line ballast 408 is not lighted in emergency situation. Advantageously, since only one lamp is lighted, the current drain on the internal battery is reduced, allowing it to operate for a longer period. Battery operation is further enhanced, as previously mentioned, by the fact that the inverter circuit 424 operates at a high-frequency in a high-efficiency mode.

Fig. 4 shows another embodiment of the present invention which also incorporates two fluorescent lamps, 500 and 502. The circuitry in Fig. 4 is similar to that shown in Fig. 3 and the

-13-

corresponding components are designated with similar numerals. As in the previous embodiment, AC line voltage on AC line 504 is provided to primary winding 512 of transformer 510. The secondary winding 518 is divided into two sections 514 and 516. Section 514 drives a low-voltage power supply, 520, and section 516 drives a battery charger which, in turn, is connected to an internal battery 526.

The output 521 of low-voltage power supply 520 is connected, via a wall switch sensing unit 522, to a pair of DC/AC inverters, 524 and 525. Thus, during normal operation, when A.C. line voltage is present, the D.C. output from power supply 520 drives both inverter 524 and 525 to light lamps 500 and 502, respectively. This embodiment has an advantage over the embodiment shown in Fig. 3 in that a standard line ballast is not used. Inverters 524 and 525 operate the lamps 500 and 502 more efficiently than a standard ballast and, thus, the heat which would be generated by a standard ballast is reduced. Since excess heat can reduce battery life, the embodiment shown in Fig. 4 extends battery life.

As shown in Fig. 4, the AC line voltage used to charge the internal 12 volt battery unit 526 is monitored by line-voltage sensing circuit 530. During an emergency situation (as discussed in the previous embodiment), the DC battery charging

-14-

voltage on lead 531 disappears, causing line voltage sensing unit 530 to connect the battery output on lead 528, via lead 532, to inverter 525. Inverter 525 is therefore powered by the internal battery to light fluorescent lamp 502. Fluorescent lamp 500 does not receive power from either the battery or the DC power supply 520 (which is now disabled because of the lack of AC line voltage) and, accordingly, lamp 500 does not light. Battery power is thereby conserved.

Fig. 5 shows a more detailed electrical schematic of a wall switch sensor which utilizes an electro-optical isolator. Portions of the circuitry shown in Fig. 5 are shown in block schematic form in Figs. 3 and 4 and those portions are designated with similar numerals in Fig. 5. In particular, the DC power supply (shown as element 420 in Fig. 3 and element 520 in Fig. 4) is comprised of a full-wave bridge rectifier 640 driven by the secondary winding 614 of transformer 610. The rectified DC output of bridge 640 is smoothed by a low-pass filter consisting of capacitor 644, choke 646 and resistor 648. The D.C. output of this circuitry is provided to a phototransistor 650 which, in the absence of any light, is held "off" by resistor 652.

Phototransistor 650 is operated by light-emitting diode 654 which is, in turn, controlled by wall switch 606. More particularly,

-15-

when wall switch 606 is closed, the AC line current is rectified by means of resistor 660 and diode 658. The rectified voltage is smoothed by capacitor 656 and applied to light-emitting diode 654. Light-emitting diode 654, in turn, operates transistor 650 to connect the output of DC power supply 620 to the DC/AC inverters shown in Figs. 3 and 4.

When wall switch 606 is opened, the current flow through diode 654 ceases and transistor 650 disconnects D.C. power supply from the inverters.

As shown in Figs. 3 and 4, the voltage produced by secondary winding, 616, of transformer 610 is provided, via lead 642 and diode 643 to the battery charging circuit.

The battery charging circuit and line voltage monitor is shown in more detail in Fig. 6. In Fig. 6, the battery charging voltage (provided through diode 643 shown in Fig. 5) is filtered by capacitor 704 and applied, via resistor 706, diode 710 and resistor 712, to battery 700.

Battery 700 is prevented from overcharging by means of a voltage regulator circuit consisting of resistor 714, transistor 716, potentiometer 720 and Zener diode 718. Zener diode 718 and potentiometer 720 maintain the base of transistor 716 at a

-16-

predetermined potential relative to the battery potential. If, during the charging operation, the battery voltage increases the potential at the base of transistor 716 will also increase. Transistor 716 thus begins to conduct more heavily, drawing charging current away from the battery.

During normal operation, the battery charging voltage is also applied through resistor 708 to the base of transistor 702. The emitter of transistor 702 is connected to battery 700. Since the battery charging voltage is typically higher than the battery voltage and since transistor 702 is a PNP-type transistor, transistor 702 will be back-biased during normal operation and thus transistor 702 will be held in a non-conducting state. Consequently, battery 700 will not be connected to output lead 748.

Because transistor 702 is not conducting, the voltage on lead 748 falls to ground level due to resistors 734 and 736. However, the battery charging voltage on lead 706 is applied to the base of transistor 730 by means of the voltage divider consisting of resistors 738, 736 and 734. The values of these resistors are chosen so that transistor 730 is turned-on in the normal condition.

During emergency situation, the charging voltage on lead 706 disappears, allowing transistor

-17-

702 to turn on. When transistor 702 turns on, battery 700 is connected to lead 748. The voltage on lead 748 holds transistor 730 "on" via the voltage divider consisting of resistors 734 and 736. Turned-on transistor 730 grounds the base of transistor 702 via resistor 732 and maintains transistor 702 in the "on" condition.

Transistor 740 is provided with an optional photocell circuit which turns transistor 702 off (via transistor 730) if the ambient light is bright enough so that emergency lighting is not needed. In particular, the potential at the base of transistor 740 is controlled by a voltage divider consisting of potentiometer 742, photocell 744 and resistor 746. Normally, this potential is adjusted so that, during emergency situation, when battery voltage appears on lead 748, transistor 740 will be in its non-conducting state. As the ambient light intensity increases, however, the resistance of photocell 744 decreases and the potential at the base of transistor 740 increases. Eventually, transistor 740 turns "on" and effectively grounds the base of transistor 730 which transistor, in turn, turns "off" opening the ground connection to the base of transistor 702. Transistor 702 thus disconnects battery 700 from the inverter circuits (not shown in Figure 7) so that battery power is not wasted when emergency lighting is not needed. Capacitor 750 insures that transistors 730 and 702 turn off before transistor 740.

-18-

As is conventional, the resistive voltage divider formed by resistors 734 and 736 also monitors the battery voltage and shuts off transistor 702, via transistor 730, when the output voltage on lead 748 drops below a predetermined minimum voltage. This latter action prevents battery 700 from being severely discharged, a situation which makes recharging difficult after repeated recharges.

All of the embodiments have the advantage that the battery which powers the emergency lighting is contained within the lighting fixture. This arrangement allows easy retrofitting of the fixture without extensive rewiring. In addition the DC battery and charging circuit is isolated from the AC line - a condition which is required to meet electrical code requirements in many locations.



-19-

## CLAIMS

1. A back-up power system for a lighting fixture which operates at least two lamps from an AC mains line comprising

means for powering all of said lamps from the AC mains line,

a low-voltage battery located in said fixture,

a battery charging circuit powered from said AC mains line and connected to said battery for generating a battery charging current for charging said battery,

a DC/AC inverter connected to one of said lamps, and

means connected to said AC mains line and responsive to the absence of AC mains power for disconnecting said one lamp from said AC mains and for connecting said battery to said DC/AC inverter to power said one of said lamps.

2. A back-up power system according to claim 1 wherein said powering means comprises an AC line ballast for powering one or more lamps from said AC mains line.

3. A back-up power system according to claim 2 wherein said powering means further comprises a DC

-20-

power supply operating from said AC mains line to produce a DC output voltage and means connecting said DC output voltage to said inverter to operate said one of said lamps when AC mains voltage is not present.

4. A back-up power system according to Claim 1 wherein said disconnecting means comprises means responsive to the absence of AC mains power for disconnecting said DC output from said DC/AC inverter.

5. A back-up power system according to Claim 4 wherein said disconnecting means further comprises means responsive to the absence of said battery charging current for connecting said battery to said DC/AC inverter to power said one of said lamps.

6. A back-up power system according to Claim 1 further comprising means responsive to said AC mains power for disconnecting said inverter from said one of said lamps when AC mains power is present.

7. A back-up power system according to Claim 1 wherein said powering means comprises at least two DC/AC inverters, means for connecting said one lamp to one of said inverters and means connecting all of the remaining lamps to the other inverter.

8. A back-up power system according to Claim 7 wherein said powering means further comprises a DC

-21-

power supply operating from said AC mains line to produce a DC output voltage and means connecting said DC output voltage to all of said inverters to operate said lamps when AC mains voltage is present.

9. A back-up power system according to Claim 8 wherein said disconnecting means comprises means responsive to the absence of AC mains power for disconnecting said DC output from said DC/AC inverters.

10. A back-up power system according to Claim 9 wherein said disconnecting means further comprises means responsive to the absence of said battery charging current for connecting said battery to one of said DC/AC inverters to power said one of said lamps.

11. A back-up power system for lamps which operate from AC house current, said back-up system comprising,

an AC ballast connected to said AC house current,

at least one first lamp connected to said AC ballast so that said first lamp operates from said AC house current,

an AC relay having a coil connected to said AC house current, two N/C contacts, a first set of two N/O contacts and a second set of N/O contacts,

-22-

at least one second lamp electrically connected in series with said N/C relay contacts to said AC ballast,

a DC/AC inverter,

means connecting said second lamp electrically in series with said first set of N/O relay contacts to said DC/AC inverter,

a low-voltage battery,

means connecting said DC/AC inverter electrically in series with said second set of N/O contacts to said battery, so that when said AC house current is present, both said first lamp and said second lamp are operated from said AC ballast, and, when said AC house current is not present, said N/C contacts are opened and said N/O contacts are closed so that said DC/AS inverter is connected to said battery and to said second lamp whereby said second lamp is powered by said battery.

2. The backup power system of claim 1 wherein said AC house current is 115 volts AC and said battery delivers 12 volts DC.

12. The backup power system of claim 11 wherein said AC house current is 115 volts AC and said battery delivers 12 volts DC.

13. The backup power system of claim 11 wherein said lamps are fluorescent lamps and said first lamp is rated at 8 watts and said second lamp is rated at 32 watts.

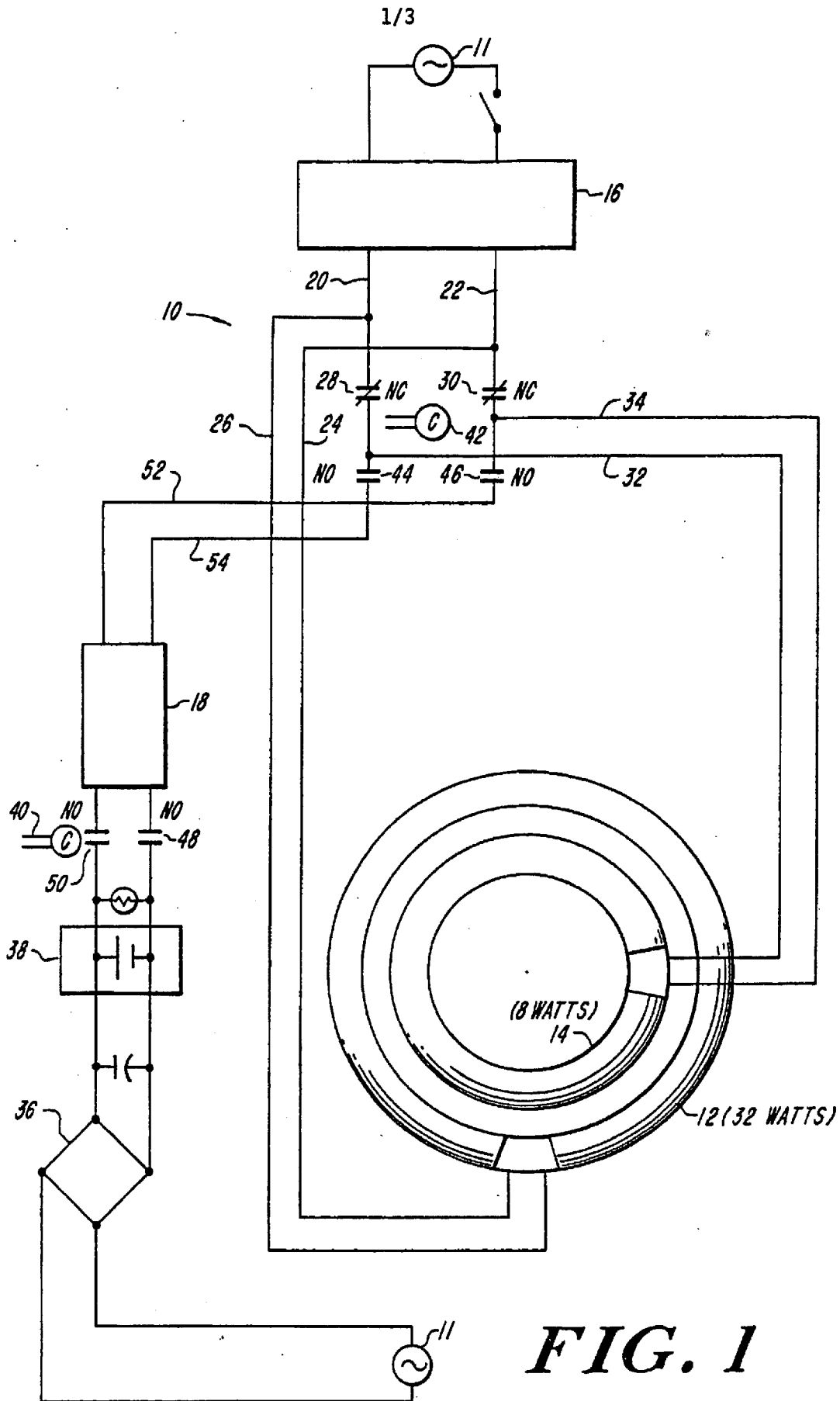
-23-

14. The backup power system of claim 13 wherein said lamps have a rounded tubular or straight tubular shape.

15. The backup power system of claim 14 wherein said battery has a pilot light attached thereto.

16. The backup power system of claim 11 wherein said lamps are lamps selected from the group consisting of fluorescent lamps, mercury vapor lamps and high pressure sodium lamps.

17. The backup power system of claim 11 wherein a battery charger is connected to AC house current and said battery to provide a DC charge to said battery.



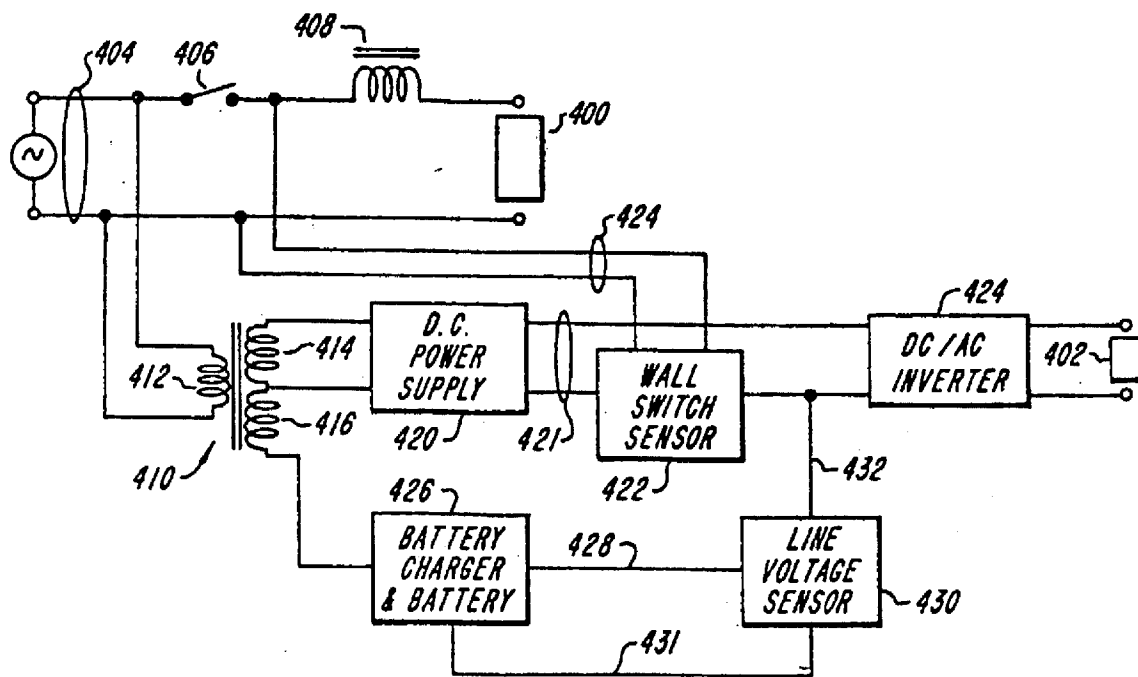
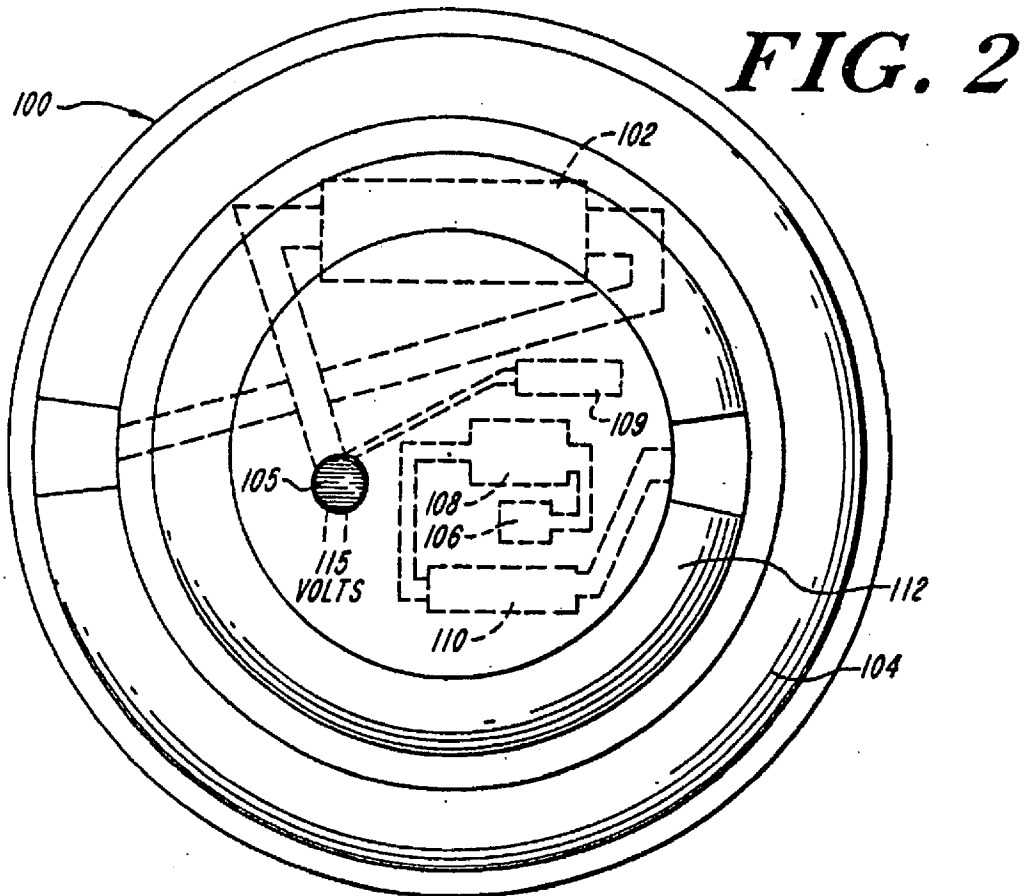
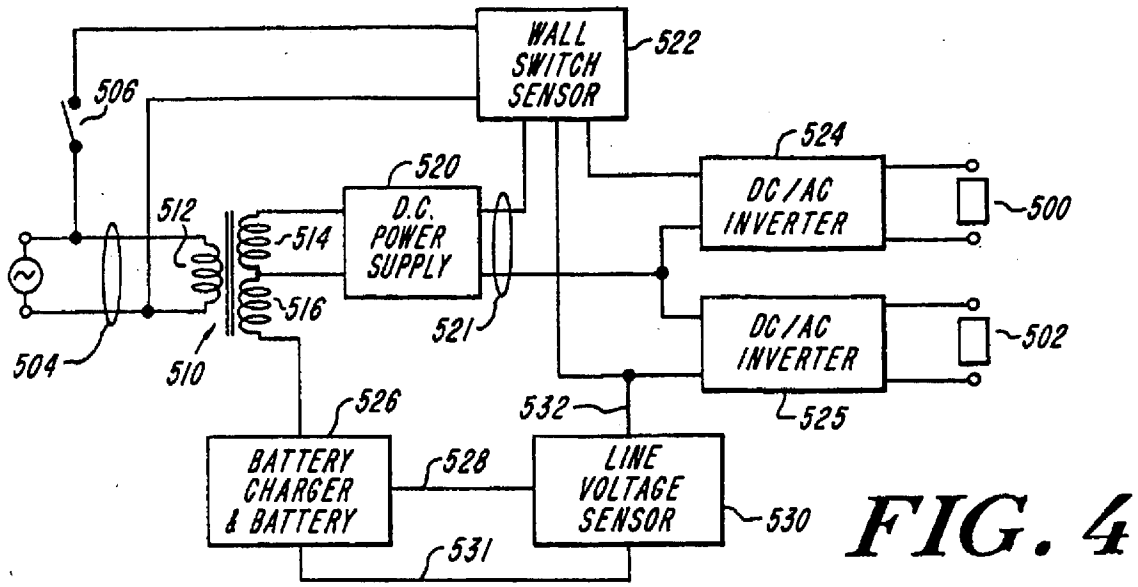
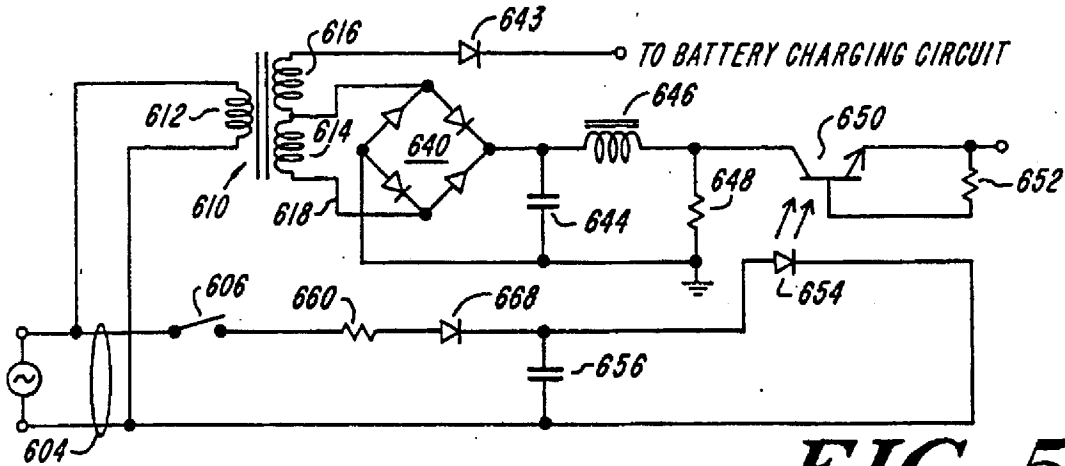


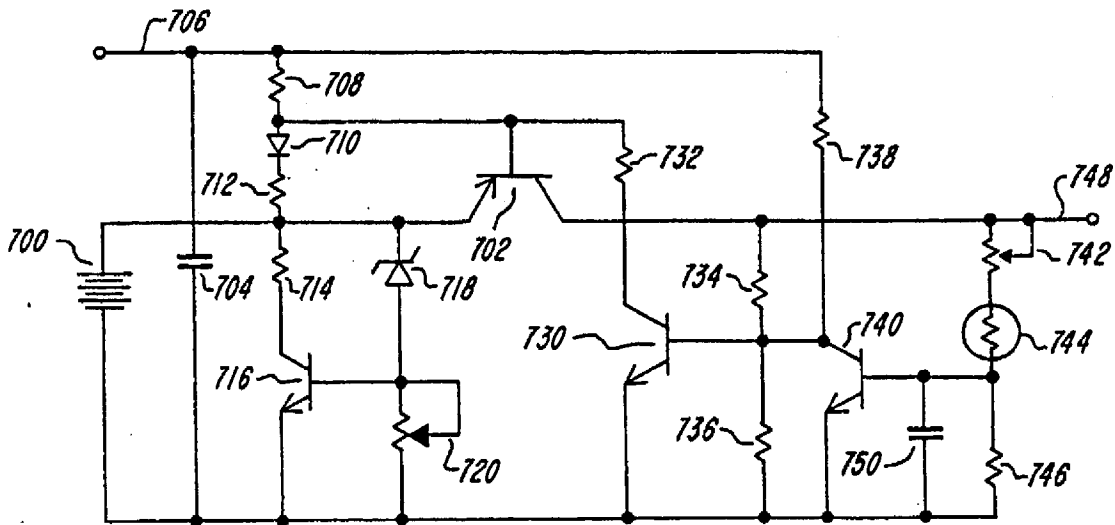
FIG. 3



**FIG. 4**



**FIG. 5**

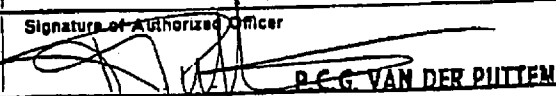


**FIG. 6**



**INTERNATIONAL SEARCH REPORT**

International Application No PCT/US 88/00515

<b>I. CLASSIFICATION OF SUBJECT MATTER</b> (If several classification symbols apply, indicate all) <sup>6</sup>		
According to International Patent Classification (IPC) or to both National Classification and IPC		
IPC <sup>4</sup> : H 02 J 9/06; H 05 B 41/04		
<b>II. FIELDS SEARCHED</b>		
Minimum Documentation Searched <sup>7</sup>		
Classification System	Classification Symbols	
IPC <sup>4</sup>	H 02 J; H 05 B	
Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched <sup>8</sup>		
<b>III. DOCUMENTS CONSIDERED TO BE RELEVANT <sup>9</sup></b>		
Category <sup>10</sup>	Citation of Document, <sup>11</sup> with indication, where appropriate, of the relevant passages <sup>12</sup>	Relevant to Claim No. <sup>13</sup>
X	GB, A, 2072439 (KAUFEL GROUP LTD) 30 September 1981, see page 2, line 56 - page 4, line 10; figure 5	1-6
A	--	11-17
X	US, A, 3684891 (SIERON) 15 August 1972, see column 3, line 7 - column 7, line 6; figure 1	1-6
A	--	11
Y	US, A, 3659179 (J.S.N. BARKER et al.) 25 April 1972, see column 1, line 53 - column 2, line 74; figure 3	1-8,11-17
Y	US, A, 4349863 (PETERSEN) 14 September 1982, see column 3, line 5 - column 4, line 51; figure 1	1-8,11-17
A	US, A, 4057750 (R.T. ELMS) 8 November 1977, see column 3, line 18 - column 6, line 46; figures 1-6	1-3,11
-----		
<p><sup>10</sup> Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>		
<b>IV. CERTIFICATION</b>		
Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report	
5th October 1988	08.11.88	
International Searching Authority	Signature of Authorized Officer	
EUROPEAN PATENT OFFICE	 P.C.G. VAN DER PUTTEN	

ANNEX TO THE INTERNATIONAL SEARCH REPORT  
ON INTERNATIONAL PATENT APPLICATION NO.

US 8800515  
SA 21190

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 21/10/88. The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB-A- 2072439	30-09-81	US-A- 4297614 DE-A- 3108739	27-10-81 28-01-82
US-A- 3684891	15-08-72	None	
US-A- 3659179	25-04-72	NL-A- 7008469 LU-A- 61111 DE-A- 2028848 FR-A- 2051067 GB-A- 1307366 BE-A- 751821	15-12-70 12-08-70 17-12-70 02-04-71 21-02-73 11-12-70
US-A- 4349863	14-09-82	None	
US-A- 4057750	08-11-77	JP-A- 52137172 CA-A- 1064097	16-11-77 09-10-79

EPO FORM 10379

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

© EPODOC / EPO

PN - JP2003085258 A 20030320  
 OPD - 2001-09-13  
 PA - YAMATAKE BUILDING SYS CO LTD  
 IN - YAMAMOTO TAKESHI  
 TI - FACILITY MANAGEMENT SUPPORTING DEVICE  
 AB - PROBLEM TO BE SOLVED: To quickly acquire detailed information of a desired control point by a simple operation from a summary graph. SOLUTION: A desired control point is designated in a summary graph displayed at a display, and a mouse is right-clicked (a step 401). Then, all pictures controlled by a central monitoring device and a building management system relevant to the control point are picked up, and the list of the picked-up pictures is displayed as a picture list (a step 402). When the desired list item in the picture list is designated, and the mouse is left-clicked, the real picture of the picture corresponding to the list item is called, and displayed at the display (a step 403).  
 FI - G05B23/02&V; G06F17/60&122C; G06F3/00&656A  
 FT - 5E501/AA02; 5E501/AC15; 5E501/CA03; 5E501/CB02; 5E501/CB09; 5E501/EA13; 5E501/FA13; 5E501/FA14; 5E501/FA22; 5E501/FA42; 5H223/AA11; 5H223/AA19; 5H223/DD03; 5H223/DD09; 5H223/EE06; 5H223/EE29; 5H223/FF03  
 IC - G06F17/60; G05B23/02; G06F3/00  
 ICAI - G06Q50/00; G05B23/02; G06F3/00; G06F3/048  
 ICCI - G06Q50/00; G05B23/02; G06F3/00; G06F3/048  
 AP - JP20010277710 20010913  
 PR - JP20010277710 20010913  
 FAMN - 19102192  
 PD - 2003-03-20

© WPI / Thomson

AN - 2003-284933 [28]  
 OPD - 2001-09-13  
 PD - 2003-03-20  
 AP - JP20010277710 20010913  
 PA - (YAMA-N) YAMATAKE KEISO KK  
 CPY - YAMA-N  
 IN - YAMAMOTO T  
 TI - Facility management assistance apparatus e.g. for factory, hospital, displays list of operation control information of various equipments and operation control information of desired equipment, selectively  
 AB - NOVELTY :  
 A display screen displays a list of information related to the operation control of various equipments in a facility, in response to the right-click operation of mouse. The mouse is left clicked to display the information related to operation control of a desired equipment, in the display screen.  
 - USE :  
 For assisting management of equipments such as air conditioner and power supply equipment in commercial facility, such as flats, hospital and factories.  
 - ADVANTAGE :  
 Enables efficient and reliable management of facilities, even by an unskilled operator.  
 - DESCRIPTION OF DRAWINGS :

The figure shows a flowchart illustrating the facility management assistance process. (Drawing includes non-English language text).

PN - JP2003085258 A 20030320 DW200328  
NC - 1  
IW - FACILITY MANAGEMENT ASSIST APPARATUS FACTORY HOSPITAL DISPLAY LIST OPERATE  
CONTROL INFORMATION VARIOUS EQUIPMENT SELECT  
IC - G06F17/60; G05B23/02; G06F3/00  
MC - S05-G02 T01-C04 T01-J07B1 T01-J12B1 T04-H T06-A08 X27-E01B  
DC - S05 T01 T04 T06 X27

\* NOTICES \*

**JPO and INPIT are not responsible for any damages caused by the use of this translation.**

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is used for institutions, such as an intelligent building, a commercial complex, collective housing, a hospital, and a factory, and relates to a suitable facility management support device.

[0002]

[Description of the Prior Art] Various kinds of equipment is arranged in institutions, such as an intelligent building, a commercial complex, collective housing, a hospital, and a factory. For example, equipment systems, such as an air conditioner, a power equipment, security installations, and disaster prevention equipments, are mentioned as the equipment, and the total system is built by these. In the institution, the management point is formed as a point which acquires the information about the operation control of various kinds of equipment.

[0003] For example, in the intelligent building, the central monitoring system which supervises equipment, and BIRUMANEJIMENTOSHISUTEMU which manages equipment are provided in the central monitoring room. A summary graph can be called to the display of a central monitoring system, and the present information on the various management points in a building, including current temperature, preset temperature, the ON/OFF state of an air conditioning machine, an alarm, etc., can be displayed. By displaying the information on various management points in a graph, it becomes possible to grasp the environment in a building, and the state of equipment visually.

[0004] Generally, a summary graph is divided and displayed for every equipment and every floor. For example, if the first floor floor is chosen, the top view of the first floor floor will be displayed on a display, and the information on various management points, such as current temperature, preset temperature, an ON/OFF state of an air conditioning machine, and an alarm, will be displayed into this top view.

[0005]

[Problem(s) to be Solved by the Invention] In the conventional system, detailed information, such as a maintenance history, a preservation history, etc. of a specific management point, was not able to be immediately acquired from the summary graph currently displayed on the display of the central monitoring system. This is because not a central monitoring system but BIRUMANEJIMENTOSHISUTEMU has managed a maintenance history, a preservation history, etc. of equipment or apparatus. Therefore, in order to acquire detailed information, BIRUMANEJIMENTOSHISUTEMU is accessed first, The possible screen of following a tree form route from the first menu, and acquiring desired information

according to the hierarchy of the menu of application, must be chosen, and it must go, For example, when an alarm occurred in a specific management point, information needed was not able to be immediately acquired from a summary graph. This is not restricted at the time of an alarm occurrence, the operation condition of an air conditioning machine, etc. are the same, for example to check the total of the stored data, analysis, a tendency, etc., operation until it acquires the target information was complicated, and appointment of the operator which became skilled was required for it.

[0006] There is a place which it was made in order that this invention might solve such a technical problem, and is made into the purpose in providing the possible facility management support device of acquiring the detailed information of a desired management point from a summary graph immediately by easy operation.

[0007]

[Means for Solving the Problem] In order to attain such a purpose, this invention is characterized by comprising the following:

A management point information display means which displays information on various management points in an institution on a corresponding predetermined field on a screen.

A setting means which makes a desired management point with which information was displayed specify on a screen.

A screen list display means to display a list of screens managed with application relevant to a specified management point.

A real screen displaying means which displays a real screen of a screen by which selected designation was carried out from a displayed screen list.

According to this invention, in a screen (summary graph) on which information on various management points in an institution was displayed, if a desired management point is specified, a list of screens managed with application relevant to that management point will be displayed. And if a desired list item is specified from this screen list, a real screen of a screen corresponding to that specified list item will be displayed, and detailed information will appear.

[0008]

[Embodiment of the Invention] Hereafter, this invention is explained in detail based on a drawing. Drawing 1 is a block diagram showing the hardware constitutions of the facility management support device concerning the 1 embodiment of this invention. In the figure -- 1 -- CPU and 2 -- as for a mouse, and 6-9, ROM and 4 are [ external storages, such as HDD, and 11 ] bus lines an interface and 10 a mouse operation type display and 5 RAM and 3.

[0009] CPU1 acquires the various input (data from various management points) from the system given via the interface 8, and it performs various processing operation according to the program stored in ROM3, accessing RAM2. The various processing information on CPU1 is outputted to the display 4 via the interface 6 according to specification by operation of the mouse 5 on the screen in the display 4.

[0010] CPU1 can access the external storage 10 via the interface 9, and it controls a various device by the BIRUMANEJIMENTO program which resides in RAM2 permanently, and records the information on various management points on the external storage 10.

[0011] In this facility management support device 100, a menu bar is displayed on the initial screen (not shown) displayed on the display 4. "BIRUMANEJIMENTO" is provided in this menu bar as one of the menu items. If this "BIRUMANEJIMENTO" is chosen, the facility management support device 100 will display the various menus

of BIRUMANEJIMENTO, and will operate as BIRUMANEJIMENTOSHISUTEMU which manages the state of various equipment established in the institution.

[0012]The "summary graph" is formed in the menu bar of the above-mentioned initial screen as one of the menu items. If this "summary graph" is chosen, the facility management support device 100 will display a summary graph on the display 4, and will operate as a central monitoring system which supervises the present situation of a management point established in the institution.

[0013]The menus for every equipment and every floor are provided in the "summary graph." For example, if the first floor floor is chosen from the menu for every floor, the top view of the first floor floor will be displayed on the display 4, The information on various management points, such as an ON/OFF state of the current temperature, the preset temperature, and the air conditioning machine which are obtained from the sensor and controller which were formed in various management points via the interface 8, and an alarm, is displayed into this top view.

[0014]The summary graph of the first floor floor displayed on drawing 2 by the display 4 is illustrated. In this example, the first floor floor is constituted by a "shared part", "office \*\*", and "office \*\*", and the ON/OFF state of that indoor current temperature, preset temperature, and an air conditioning machine is displayed into the top view showing a "shared part", "office \*\*", and "office \*\*" as a summary graph.

[0015]That is, the current temperature and preset temperature in a shared part are displayed on field S1<sub>1</sub> of a "shared part" among a summary graph. These are the information on a measuring point established in the actual shared part, and are kinds of the information on a management point. The icon which shows the ON/OFF state of the air conditioning machine in a shared part is displayed on field S1<sub>2</sub> and S1<sub>3</sub>. These are information (information on a state point) which shows the state of a actual shared part, and these are also kinds of the information on a management point. Similarly, the current temperature and preset temperature in office \*\* are displayed on field S2<sub>1</sub> by "office \*\*" as information on a measuring point, and the icon which shows the ON/OFF state of the air conditioning machine in office \*\* to field S2<sub>2</sub> as information on a state point is displayed on it. The current temperature and preset temperature in office \*\* are displayed on field S3<sub>1</sub> by "office \*\*" as information on a measuring point, and the icon which shows the ON/OFF state of the air conditioning machine in office \*\* to field S3<sub>2</sub> as information on a state point is displayed on it. The ON/OFF state of an air conditioning machine is expressed as the color of the icon.

[0016]If leakage of water occurs in "office \*\*" during the display of summary graph F1 of the first floor floor of this, that information will be given to the facility management support device 100 from the sensor which detected this leakage of water. then, the character as information on an alarm point that the sensor was installed in field S2<sub>3</sub> in the top view of "office \*\*" in the facility management support device 100 as shown in drawing 3 "leakage of water" -- for example, it is indicated by red. The information on such an alarm point is also one of the information on a management point. When such an alarm occurred, in the conventional device, detailed information, such as a maintenance history, a preservation history, etc. of the alarm point, was not able to be acquired immediately. On the other hand, at this embodiment, desired information can be immediately acquired from summary graph F1 by the easy following mouse operation.

[0017][A display of a screen list] The mouse 5 is operated, and the mouse pointer P1 on the display 4 is set by field S2<sub>3</sub>, and is right-clicked. That is, the generating point (alarm point) of leakage of water is specified, and the mouse 5 is right-clicked (Step

401 shown in drawing 4). Then, CPU1 takes up all the screens managed by the central monitoring system and BIRUMANEJIMENTOSHISUTEMU relevant to the above-mentioned alarm point specified on summary graph F1, and it displays the list of this screen that took up as a screen list (Step 402). The name of an alarm point is used as a key in this case, for example, and the screen where this key is contained is listed. A related screen becomes what is listed automatically by this, and it can conform to an addition and deletion of a new screen.

[0018]In this case, as shown in drawing 5 (a), the screen list L1 which makes a list item a "graph", a "monthly report", an "alarm history", an "alarm monthly report", "an alarm total", and a "correspondence state" is displayed. A "graph", a "monthly report", the "alarm history", the "alarm monthly report", the "alarm total", and the "correspondence state" are matched with screen NO. (maintenance management, maintenance engineering, etc.) which a central monitoring system and BIRUMANEJIMENTOSHISUTEMU have managed during this screen list L1.

[0019]When a desired list item is specified and the mouse 5 is left-clicked in the screen list L1, CPU1, The screen of screen NO. matched with the list item which accessed a central monitoring system and BIRUMANEJIMENTOSHISUTEMU and was specified as them according to the program, i.e., the specified real screen of a screen, is called, and it displays on the display 4 (Step 403). In this case, although the real screen which switched and called the screen is displayed, it may be made to display in a window.

[0020]When an "alarm monthly report" is chosen as drawing 6 in the screen list L1, the example of a real screen displayed on the display 4 is shown. The information on the equipment etc. which an alarm name, occurrence time, return time, and an alarm generated is displayed on this real screen G1 as a monthly report. When "an alarm total" is chosen as drawing 7 in the screen list L1, the example of a real screen displayed on the display 4 is shown. Total data, such as a pie chart according to equipment of the alarm data which totaled to the month unit, and generating frequency, is displayed on this real screen G2 as an alarm total. When a "correspondence state" is chosen as drawing 8 in the screen list L1, the example of a real screen displayed on the display 4 is shown. Taking over information is displayed on this real screen G3 including off-line input etc.

[0021]In \*\*\*, although the example which acquires the detailed information of an alarm point from summary graph F1 explained, it is possible to acquire detailed information from summary graph F1 similarly about a measuring point or a state point.

[0022]For example, among the top view of "office \*\*" of summary graph F1, if field S2<sub>1</sub> as which the information on a measuring point is displayed is specified and the mouse 5 is right-clicked, as shown in drawing 5 (b), the screen list L2 which makes a list item a "graph", a "monthly report", and an "operation history" will be displayed. During this screen list L2, if a desired list item is specified and the mouse 5 is left-clicked, the real screen of the screen corresponding to that specified list item will be called, and it will be displayed on the display 4.

[0023]Similarly, among the top view of "office \*\*" of summary graph F1, if field S2<sub>2</sub> as which the information on a state point is displayed is specified and the mouse 5 is right-clicked, as shown in drawing 5 (c), the screen list L3 which makes a list item a "graph", a "monthly report", and an "operation history" will be displayed. During this screen list L3, if a desired list item is specified and the mouse 5 is left-clicked, the real screen of the screen corresponding to that specified list item will be called, and it will be displayed on the display 4. The example of a real screen displayed when a



"monthly report" is chosen as drawing 9 in the screen list L3 is shown. The data which totaled operation time is displayed on this real screen G4 as a monthly report. [0024]Although a screen list is displayed and it was made to display the real screen of the screen corresponding to the list item selected by left-clicking the mouse 5 by a screen list by right-clicking the mouse 5 in the embodiment mentioned above, A screen list is displayed and it may be made to display the real screen of the screen corresponding to the list item selected by a screen list by right-clicking the mouse 5 by left-clicking the mouse 5. A touch pen etc. may be used instead of a mouse.

[0025]

[Effect of the Invention]In the screen (summary graph) on which the information on the various management points in an institution was displayed according to this invention so that clearly from having explained above, If a desired management point is specified, the list of screens managed with the applications (a central monitoring system, BIRUMANEJIMENTOSHISUTEMU, etc.) relevant to the management point will be displayed, If a desired list item is specified from this screen list, the real screen of the screen corresponding to that specified list item will be displayed, it will become that in which detailed information appears, and it will become possible to acquire the detailed information of a desired management point from a summary graph immediately by easy operation. Thereby, even if the operator is not skilled in operation, it can acquire desired information promptly.

[Claim(s)]

[Claim 1]A facility management support device comprising:

A management point information display means which displays information on various management points in an institution on a predetermined field corresponding to each of said management point on a screen.

A setting means which makes a desired management point with which information was displayed specify on said screen by this management point information display means.

A screen list display means to display a list of screens managed with application relevant to a management point specified by this setting means.

A real screen displaying means which displays a real screen of a screen by which selected designation was carried out from a screen list displayed by this screen list display means.

[Claim 2]In a facility management support device indicated to claim 1, said screen list display means, A facility management support device taking up all the screens managed with application relevant to a specified management point, and displaying a list of this screen that took up as said screen list.

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-85258

(P2003-85258A)

(43)公開日 平成15年3月20日(2003.3.20)

(51)Int.Cl.	識別記号	F I	ターム(参考)
G 0 6 F 17/60	1 2 2	C 0 6 F 17/60	1 2 2 C 5 E 5 0 1
G 0 5 B 23/02		C 0 5 B 23/02	V 5 H 2 2 3
G 0 6 F 3/00	6 5 6	C 0 6 F 3/00	6 5 6 A

審査請求 未請求 請求項の数 2 O L (全 10 頁)

(21)出願番号 特願2001-277710(P2001-277710)

(22)出願日 平成13年9月13日(2001.9.13)

(71)出願人 595123535

山武ビルシステム株式会社

東京都港区芝浦4丁目3番4号

(72)発明者 山本 毅

東京都港区芝浦4丁目3番4号 山武ビルシステム株式会社内

(74)代理人 100064621

弁理士 山川 政樹

Fターム(参考) 5E501 AA02 AC15 CA03 CB02 CB09

EA13 FA13 FA14 FA22 FA42

5H223 AA11 AA19 DD03 DD09 EE06

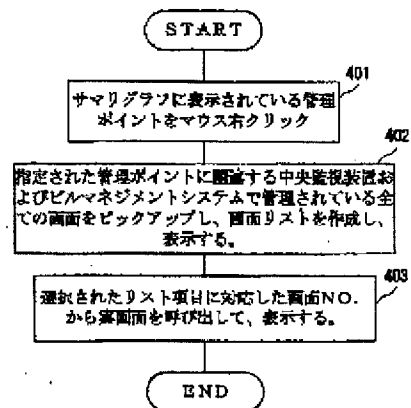
EE29 FF03

(54)【発明の名称】 施設管理支援装置

(57)【要約】

【課題】 サマリグラフから簡単な操作で即座に所望の管理ポイントの詳細情報を取得できるようにする。

【解決手段】 ディスプレイに表示されているサマリグラフにおいて、所望の管理ポイントを指定し、マウスを右クリックする(ステップ401)。すると、その管理ポイントに関連する中央監視装置およびビルマネジメントシステムが管理している全ての画面がピックアップされ、このピックアップされた画面のリストが画面リストとして表示される(ステップ402)。この画面リスト中、所望のリスト項目を指定してマウスを左クリックすると、そのリスト項目に対応する画面の実画面が呼び出され、ディスプレイに表示される(ステップ403)。



## 【特許請求の範囲】

【請求項1】 施設における各種管理ポイントの情報を画面上の前記管理ポイントのそれぞれに対応する所定の領域に表示する管理ポイント情報表示手段と、

この管理ポイント情報表示手段によって情報が表示された所望の管理ポイントを前記画面上において指定させる指定手段と、

この指定手段によって指定された管理ポイントに関連するアプリケーションで管理されている画面のリストを表示する画面リスト表示手段と、

この画面リスト表示手段によって表示された画面リストから選択指定された画面の実画面を表示する実画面表示手段とを備えたことを特徴とする施設管理支援装置。

【請求項2】 請求項1に記載された施設管理支援装置において、

前記画面リスト表示手段は、指定された管理ポイントに関連するアプリケーションで管理されている全ての画面をピックアップし、このピックアップした画面のリストを前記画面リストとして表示することを特徴とする施設管理支援装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、インテリジェントビル、複合商業施設、集合住宅、病院、工場などの施設に用いて好適な施設管理支援装置に関するものである。

## 【0002】

【従来の技術】インテリジェントビル、複合商業施設、集合住宅、病院、工場などの施設においては、各種の設備が配置されている。例えば、その設備として空調設備、電力設備、防犯設備、防災設備などの設備系統が挙げられ、これらによってトータルシステムが構築されている。また、施設内には、各種の設備の運転制御に関する情報を取得するポイントとして管理ポイントが設けられている。

【0003】例えば、インテリジェントビルでは、中央の監視室に、設備を監視する中央監視装置と、設備を管理するビルマネジメントシステムが設けられている。中央監視装置のディスプレイにはサマリグラフを呼び出してビル内の各種管理ポイントの現在の情報（現在温度、設定温度、空調機のON/OFF状態、警報など）を表示することができる。各種管理ポイントの情報をグラフで表示することにより、ビル内の環境や設備の状態を視覚的に把握することが可能となる。

【0004】一般に、サマリグラフは、設備ごと、フロアごとなどに分けて表示される。例えば、1階フロアを選択すれば、ディスプレイに1階フロアの平面図が表示され、この平面図中に現在温度、設定温度、空調機のON/OFF状態、警報などの各種管理ポイントの情報が表示される。

## 【0005】

【発明が解決しようとする課題】従来のシステムでは、中央監視装置のディスプレイに表示されているサマリグラフからは、特定の管理ポイントの保守履歴や保全履歴などの詳細情報を即座に得ることができなかった。これは、設備や機器の保守履歴や保全履歴などは、中央監視装置ではなく、ビルマネジメントシステムが管理しているためである。したがって、詳細情報を得るためには、まずビルマネジメントシステムにアクセスし、アプリケーションのメニューの階層に従って、すなわち最初のメニューからツリー状のルートをとって所望の情報を得ることの可能な画面を選択して行かなければならず、例えば特定の管理ポイントにおいて警報が発生した場合には、サマリグラフから欲しい情報を即座に取得することができなかった。これは警報発生時に限られるものではなく、例えば空調機の運転状況など、蓄積されたデータの集計、分析、傾向などを確認したい場合も同様であり、目的の情報を得るまでのオペレーションが複雑で、習熟したオペレータの登用が必要であった。

【0006】本発明はこのような課題を解決するためになされたもので、その目的とするところは、サマリグラフから簡単な操作で即座に所望の管理ポイントの詳細情報を取得することの可能な施設管理支援装置を提供することにある。

## 【0007】

【課題を解決するための手段】このような目的を達成するために本発明は、施設における各種管理ポイントの情報を画面上の対応する所定の領域に表示する管理ポイント情報表示手段と、情報が表示された所望の管理ポイントを画面上において指定させる指定手段と、指定された管理ポイントに関連するアプリケーションで管理されている画面のリストを表示する画面リスト表示手段と、表示された画面リストから選択指定された画面の実画面を表示する実画面表示手段とを設けたものである。この発明によれば、施設における各種管理ポイントの情報が表示された画面（サマリグラフ）において、所望の管理ポイントを指定すると、その管理ポイントに関連するアプリケーションで管理されている画面のリストが表示される。そして、この画面リストから所望のリスト項目を指定すると、その指定したリスト項目に対応する画面の実画面が表示され、詳細情報が現れる。

## 【0008】

【発明の実施の形態】以下、本発明を図面に基づいて詳細に説明する。図1はこの発明の一実施の形態にかかる施設管理支援装置のハードウェア構成を示すブロック図である。同図において、1はCPU、2はRAM、3はROM、4はマウス操作式ディスプレイ、5はマウス、6～9はインターフェイス、10はHDDなどの外部記憶装置、11は母線である。

【0009】CPU1は、インターフェイス8を介して

与えられるシステムからの各種入力情報(各種管理ポイントからのデータ)を得て、ROM3に格納されたプログラムに従って、RAM2にアクセスしながら各種処理動作を行う。CPU1での各種処理情報は、ディスプレイ4における画面上でのマウス5の操作による指定に応じて、インターフェイス6を介してディスプレイ4に出力される。

【0010】また、CPU1は、インターフェイス9を介して外部記憶装置10にアクセスすることができ、RAM2に常駐するビルマネジメントプログラムによって、各種装置を制御し、また各種管理ポイントの情報を外部記憶装置10に記録する。

【0011】この施設管理支援装置100において、ディスプレイ4に表示される初期画面(図示せず)には、メニューバーが表示される。このメニューバーには、メニュー項目の1つとして、「ビルマネジメント」が設けられている。この「ビルマネジメント」を選択すると、施設管理支援装置100は、ビルマネジメントの各種メニューを表示し、施設内に設けられた各種設備の状態を管理するビルマネジメントシステムとして動作する。

【0012】また、上記初期画面のメニューバーには、メニュー項目の1つとして、「サマリグラフ」が設けられている。この「サマリグラフ」を選択すると、施設管理支援装置100は、ディスプレイ4上にサマリグラフを表示し、施設内に設けられた管理ポイントの現在の状況を監視する中央監視装置として動作する。

【0013】「サマリグラフ」には、設備ごと、フロアごとなどのメニューが設けられている。例えば、フロア毎のメニューから1階フロアを選択すれば、ディスプレイ4に1階フロアの平面図が表示され、この平面図中に各種管理ポイントに設けられたセンサやコントローラからインターフェイス8を介して得られる現在温度、設定温度、空調機のON/OFF状態、警報などの各種管理ポイントの情報が表示される。

【0014】図2にディスプレイ4に表示される1階フロアのサマリグラフを例示する。この例では、1階フロアが「共用部」と「事務室①」と「事務室②」とにより構成されており、サマリグラフとして「共用部」、「事務室①」、「事務室②」を示す平面図中に、その室内の現在温度、設定温度、空調機のON/OFF状態が表示されている。

【0015】すなわち、サマリグラフ中、「共用部」の領域S1<sub>1</sub>に共用部内の現在温度および設定温度が表示される。これらは、実際の共用部内に設けられた計測ポイントの情報であって、管理ポイントの情報的一种である。また、領域S1<sub>2</sub>およびS1<sub>3</sub>には共用部内の空調機のON/OFF状態を示すアイコンが表示される。これらは、実際の共用部の状態を示す情報(状態ポイントの情報)であって、これらもまた管理ポイントの情報的一种である。同様に、「事務室①」には、領域S2<sub>1</sub>に

計測ポイントの情報として事務室①内の現在温度および設定温度が表示され、領域S2<sub>2</sub>に状態ポイントの情報として事務室①内の空調機のON/OFF状態を示すアイコンが表示される。また、「事務室②」には、領域S3<sub>1</sub>に計測ポイントの情報として事務室②内の現在温度および設定温度が表示され、領域S3<sub>2</sub>に状態ポイントの情報として事務室②内の空調機のON/OFF状態を示すアイコンが表示される。なお、空調機のON/OFF状態は、そのアイコンの色で表示される。

【0016】この1階フロアのサマリグラフF1の表示中、例えば「事務室①」に漏水が発生すると、この漏水を検知したセンサから施設管理支援装置100にその情報が伝えられる。すると、施設管理支援装置100では、図3に示すように、「事務室①」の平面図中の領域S2<sub>2</sub>にセンサが設置された警報ポイントの情報として「漏水」という文字が例えば赤色表示される。このような警報ポイントの情報も管理ポイントの情報のひとつである。このような警報が発生した場合、従来の装置では、その警報ポイントの保守履歴や保全履歴などの詳細情報を即座に得ることができなかった。これに対し、本実施の形態では、次のような簡単なマウス操作で、サマリグラフF1から即座に所望の情報を得ることができ

る。

【0017】〔画面リストの表示〕マウス5を操作し、ディスプレイ4上のマウスポインタP1を領域S2<sub>2</sub>に合わせ、右クリックする。すなわち、漏水の発生ポイント(警報ポイント)を指定して、マウス5を右クリックする(図4に示すステップ401)。すると、CPU1は、サマリグラフF1上で指定された上記警報ポイントに関連する中央監視装置およびビルマネジメントシステムで管理されている全ての画面をピックアップし、このピックアップした画面のリストを画面リストとして表示する(ステップ402)。なお、この場合、例えば警報ポイントの名称をキーとし、このキーが含まれている画面をリストアップする。これにより、関連する画面が自動的にリストアップされるものとなり、新しい画面の追加や削除に即応することができる。

【0018】この場合、図5(a)に示すように、「グラフ」、「月報」、「警報履歴」、「警報月報」、「警報集計」、「対応状況」をリスト項目とする画面リストL1が表示される。この画面リストL1中、「グラフ」、「月報」、「警報履歴」、「警報月報」、「警報集計」、「対応状況」は、中央監視装置およびビルマネジメントシステムが管理(メンテナンス管理、保全管理など)している画面NO.と対応づけられている。

【0019】画面リストL1において、所望のリスト項目を指定してマウス5を左クリックすると、CPU1は、プログラムにしたがって中央監視装置およびビルマネジメントシステムにアクセスし、指定されたリスト項目に対応づけられている画面NO.の画面、すなわち指

定された画面の実画面を呼び出し、ディスプレイ4に表示する(ステップ403)。この場合、画面を切り換えて呼び出した実画面を表示するが、ウィンドウ内に表示するようにしてもよい。

【0020】図6に画面リストL1において「警報月報」を選択した場合にディスプレイ4に表示される実画面例を示す。この実画面G1には、警報名称、発生日時、復帰日時、警報が発生した設備などの情報が、月報として表示される。図7に画面リストL1において「警報集計」を選択した場合にディスプレイ4に表示される実画面例を示す。この実画面G2には、月単位に集計したアラームデータの設備別円グラフや発生回数などの集計データが、警報集計として表示される。図8に画面リストL1において「対応状況」を選択した場合にディスプレイ4に表示される実画面例を示す。この実画面G3には、引継ぎ情報が、オフライン入力情報なども含めて表示される。

【0021】なお、上述においては、サマリグラフF1から警報ポイントの詳細情報を取得する例で説明したが、計測ポイントや状態ポイントについても同様にしてサマリグラフF1から詳細情報を取得することが可能である。

【0022】例えば、サマリグラフF1の「事務室①」の平面図中、計測ポイントの情報が表示されている領域S2<sub>1</sub>を指定してマウス5を右クリックすると、図5(b)に示すように、「グラフ」、「月報」、「操作履歴」をリスト項目とする画面リストL2が表示される。この画面リストL2中、所望のリスト項目を指定してマウス5を左クリックすると、その指定されたリスト項目に対応する画面の実画面が呼び出され、ディスプレイ4に表示される。

【0023】同様にして、サマリグラフF1の「事務室②」の平面図中、状態ポイントの情報が表示されている領域S2<sub>2</sub>を指定してマウス5を右クリックすると、図5(c)に示すように、「グラフ」、「月報」、「操作履歴」をリスト項目とする画面リストL3が表示される。この画面リストL3中、所望のリスト項目を指定してマウス5を左クリックすると、その指定されたリスト項目に対応する画面の実画面が呼び出され、ディスプレイ4に表示される。図9に画面リストL3において「月報」を選択した場合に表示される実画面例を示す。この実画面G4には、運転時間を集計したデータが、月報として表示される。

【0024】また、上述した実施の形態では、マウス5を右クリックすることによって画面リストを表示させ、マウス5を左クリックすることによって画面リストで選択したリスト項目に対応する画面の実画面を表示させるようにしたが、マウス5を左クリックすることによって画面リストを表示させ、マウス5を右クリックすることによって画面リストで選択したリスト項目に対応する画

面の実画面を表示させるようにしてもよい。また、マウスの代わりにタッチペンなどを用いてもよい。

【0025】

【発明の効果】以上説明したことから明らかなように本発明によれば、施設における各種管理ポイントの情報が表示された画面(サマリグラフ)において、所望の管理ポイントを指定すると、その管理ポイントに関連するアプリケーション(中央監視装置やビルマネジメントシステムなど)で管理されている画面のリストが表示され、この画面リストから所望のリスト項目を指定すると、その指定したリスト項目に対応する画面の実画面が表示され、詳細情報が現れるものとなり、サマリグラフから簡単な操作で即座に所望の管理ポイントの詳細情報を得ることが可能となる。これにより、オペレータは、操作を習熟していなくても、迅速に所望の情報を取得することができるようになる。

【図面の簡単な説明】

【図1】 本発明の一実施の形態にかかる施設管理支援装置のハードウェア構成を示すブロック図である。

【図2】 この施設管理支援装置のディスプレイに表示される1階フロアのサマリグラフを例示する図である。

【図3】 「事務室①」に漏水が発生した場合の1階フロアのサマリグラフを例示する図である。

【図4】 サマリグラフから画面リストを表示させての所望の画面への移行操作を説明するフローチャートである。

【図5】 警報ポイント、計測ポイントおよび状態ポイントを指定してのマウス操作により表示される画面リストL1、L2およびL3を例示する図である。

【図6】 画面リストL1において「警報月報」を選択した場合にディスプレイに表示される実画面例を示す図である。

【図7】 画面リストL1において「警報集計」を選択した場合にディスプレイに表示される実画面例を示す図である。

【図8】 画面リストL1において「対応状況」を選択した場合にディスプレイに表示される実画面例を示す図である。

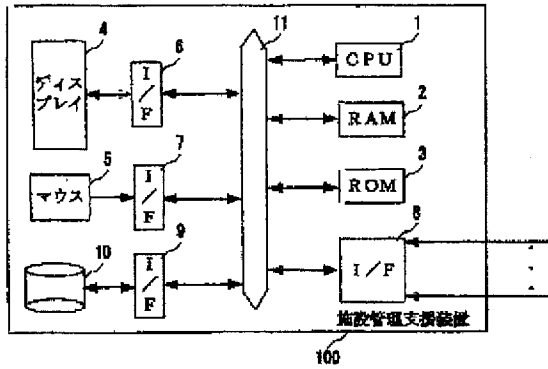
【図9】 画面リストL3において「月報」を選択した場合にディスプレイに表示される実画面例を示す図である。

【符号の説明】

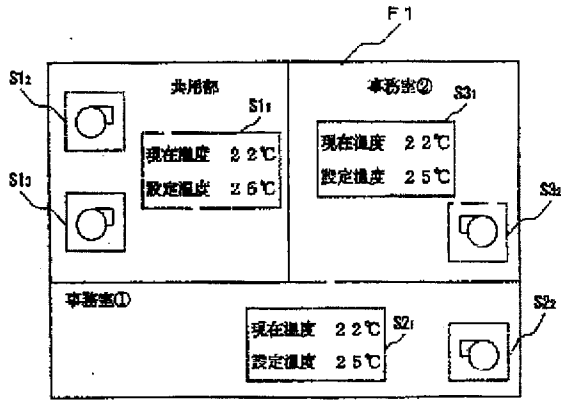
1…CPU、2…RAM、3…ROM、4…ディスプレイ、5…マウス、6～9…インターフェイス、10…外部記憶装置、11…母線、F1…1階フロアのサマリグラフ、S1<sub>1</sub>、S2<sub>1</sub>、S3<sub>1</sub>…計測ポイントの情報の表示領域、S1<sub>2</sub>、S1<sub>3</sub>、S2<sub>2</sub>、S3<sub>2</sub>…状態ポイントの情報の表示領域、S2<sub>3</sub>…警報ポイントの情報の表示領域、L1…警報ポイントの画面リスト、L2…計測ポイントの画面リスト、L3…状態ポイントの画面リ

スト、G1~G4…実画面、P1…マウスポインタ、1 00…施設管理支援装置

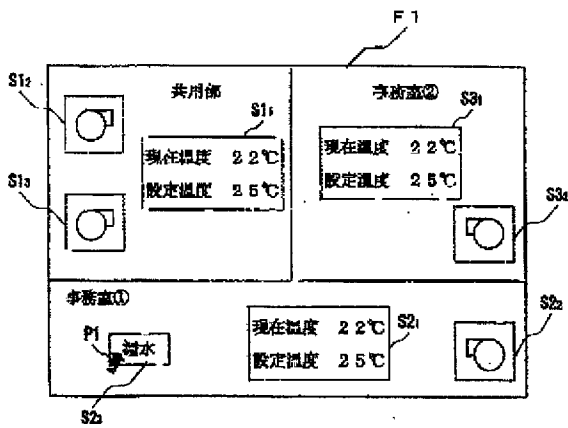
【図1】



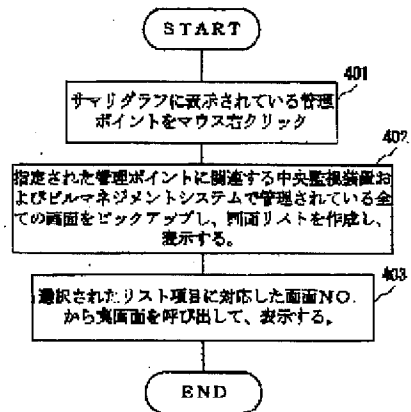
【図2】



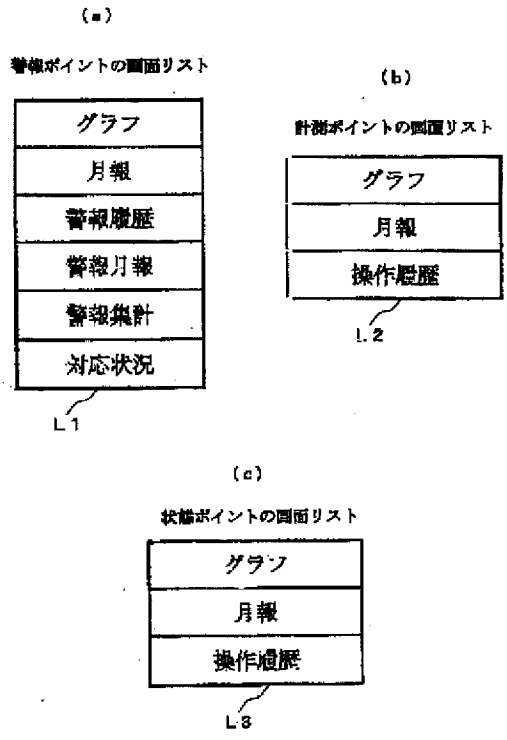
【図3】



【図4】



【図5】

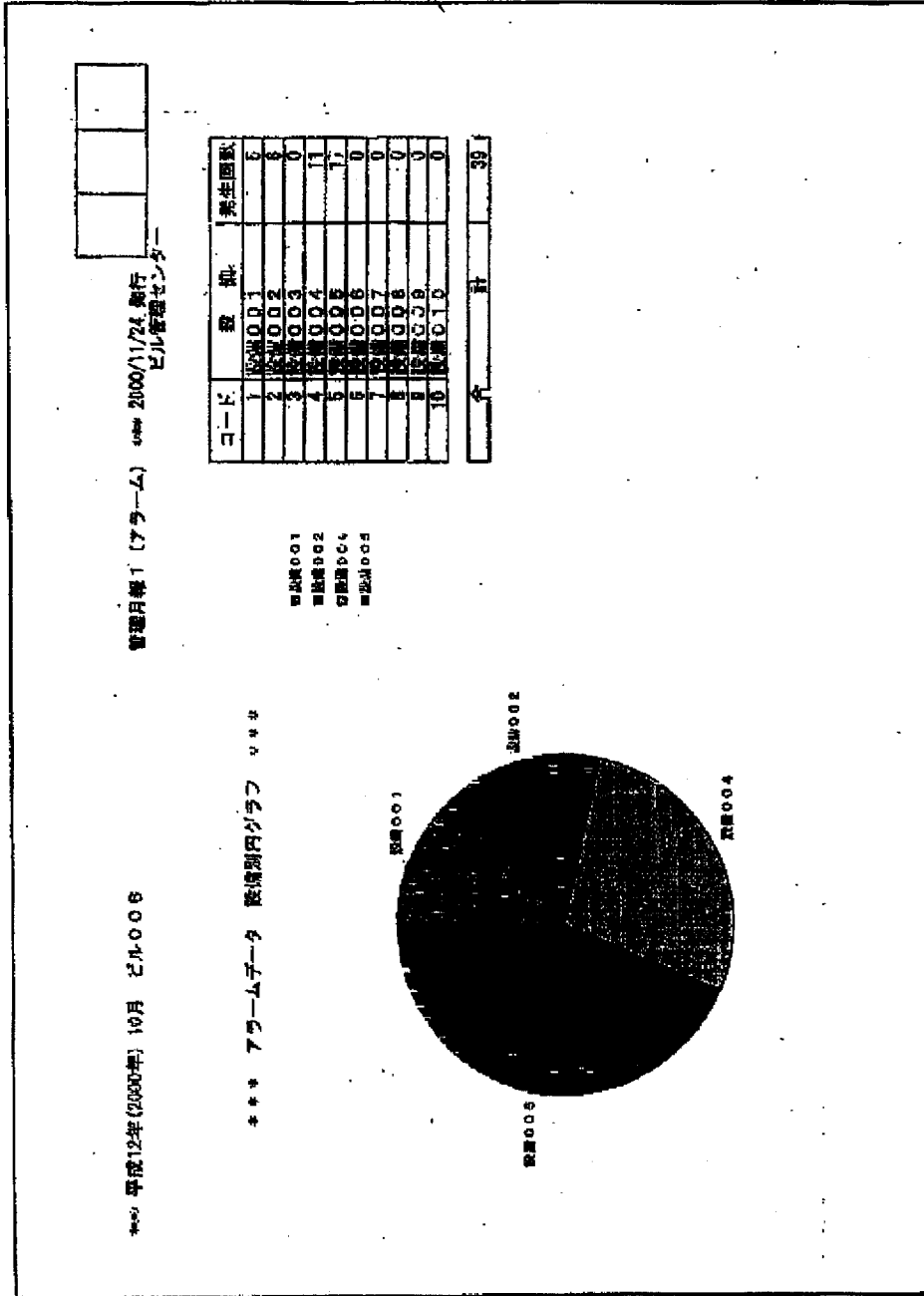






【図7】

52



【圖8】

63

2003年 12月 08日 金曜日 19:41 page. 1

**引継情報 (詳細)**

管理No. 6  
 接続番号 61001 77001

実行・事後	事前	入力型	担当001	引継社員日	2003/12/02
分取	重要度	実行型	担当010	引継終了日	2003/12/29
状況	種別				

引継内容:  
 12月29日現在 警備発生中

【図9】

64

管理員帳2 (運用時間) 2000/11/24 実行  
 管理員帳2 (運用時間) 2000/11/24 実行  
 管理員帳2 (運用時間) 2000/11/24 実行

日付	開始時間	終了時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間	経過時間
(日)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)	(H:MM)
1	0:10	1:12	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
2	0:11	1:13	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
3	0:12	1:14	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
4	0:13	1:15	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
5	0:14	1:16	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
6	0:15	1:17	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
7	0:16	1:18	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
8	0:17	1:19	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
9	0:18	1:20	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
10	0:19	1:21	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
11	0:20	1:22	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
12	0:21	1:23	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
13	0:22	1:24	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
14	0:23	1:25	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
15	0:24	1:26	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
16	0:25	1:27	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
17	0:26	1:28	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
18	0:27	1:29	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
19	0:28	1:30	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
20	0:29	1:31	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
21	0:30	1:32	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
22	0:31	1:33	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
23	0:32	1:34	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
24	0:33	1:35	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
25	0:34	1:36	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
26	0:35	1:37	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
27	0:36	1:38	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
28	0:37	1:39	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
29	0:38	1:40	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
30	0:39	1:41	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
31	0:40	1:42	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
合計	3:55	4:57	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
最大	0:40	1:42	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
最小	0:10	1:12	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24
平均	0:25	1:27	1:02	1:02	2:04	1:02	3:06	2:04	4:10	3:08	5:14	4:12	6:18	5:16	7:22	6:20	8:26	7:24

© EPODOC / EPO

- PN - JP2003141659 A 20030516  
 OPD - 2001-10-31  
 PA - YAMATAKE BUILDING SYS CO LTD  
 IN - ISEI TSUNEO  
 TI - FACILITY MANAGING DEVICE  
 AB - **PROBLEM TO BE SOLVED:** To manage a facility versatily, and to remarkably enhance operability, by linking an annunciator function to a display function of a managing screen.  
**SOLUTION:** The first screen display part 4-1 and the second screen display part 4-2 are provided in a monitor 4. An annunciator screen G1 is displayed in the first screen display part 4-1. Conditions of respective managing points are displayed in a tag BL partitioned matrix-likely in the annunciator screen G1. When the tag BL 1, for example, is touched, a managing screen G 2 (summary graph) registered to the tag BL1 is displayed in the second screen display part 4-2.
- FI - G06F3/00&652C; G06F3/14&350A; G08B23/00&510D; G08B25/04&A  
 FT - 5B069/CA03; 5B069/CA13; 5B069/CA18; 5C087/AA02; 5C087/AA03; 5C087/AA24; 5C087/AA25; 5C087/BB03; 5C087/BB74; 5C087/DD03; 5C087/DD23; 5C087/DD33; 5C087/EE06; 5C087/EE14; 5C087/FF01; 5C087/FF02; 5C087/FF04; 5C087/FF19; 5C087/FF20; 5C087/GG12; 5C087/GG23; 5C087/GG30; 5C087/GG31; 5C087/GG32; 5C087/GG51; 5C087/GG66; 5E501/AA01; 5E501/AC05; 5E501/AC32; 5E501/AC42; 5E501/BA05; 5E501/CA02; 5E501/DA15; 5E501/EA05; 5E501/FA03; 5E501/FA10; 5E501/FB28
- IC - G08B23/00; G06F3/00; G06F3/14; G08B25/04  
 ICAI - G06F3/14; G06F3/00; G06F3/048; G08B23/00; G08B25/04  
 ICCI - G06F3/14; G06F3/00; G06F3/048; G08B23/00; G08B25/01  
 AP - JP20010334064 20011031  
 PR - JP20010334064 20011031  
 FAMN - 19149252  
 PD - 2003-05-16

© WPI / Thomson

- AN - 2003-434783 [41]  
 OPD - 2001-10-31  
 PD - 2003-05-16  
 AP - JP20010334064 20011031  
 PA - (YAMA-N) YAMATAKE KEISO KK  
 CPY - YAMA-N  
 IN - ISEI T  
 TI - Facilities management apparatus for buildings, plants, has display screen which displays summary graph of management point, which is selected from points displayed in matrix form on another display screen  
 AB - **NOVELTY :**  
 The apparatus has a monitoring device (4) with a display screen (4-1) in which management points are displayed in matrix form. When a required point is selected, the management summary graph of selected point is displayed in another display screen (4-2).  
 - **USE :**  
 For management of temperature and humidity control systems installed in buildings, plants.  
 - **ADVANTAGE :**  
 Simplifies management of different facilities, thereby improving security aspect of plants.

- DESCRIPTION OF DRAWINGS :

The figure shows the display screen of monitoring device for facilities management apparatus.  
(Drawing includes non-English language text).

4 : monitoring device

4-1,4-2 : display screens

PN - JP2003141659 A 20030516 DW200341

NC - 1

IW - FACILITY MANAGEMENT APPARATUS BUILD PLANT DISPLAY SCREEN SUMMARY GRAPH  
POINT SELECT MATRIX FORM

IC - G08B23/00; G06F3/00; G06F3/14; G08B25/04

MC - T01-C T01-C04 T04-F W05-B04 W05-B05B4

DC - T01 T04 W05

\* NOTICES \*

**JPO and INPIT are not responsible for any damages caused by the use of this translation.**

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the facility management device which manages the state of the various management points in institutions, such as a building.

[0002]

[Description of the Prior Art] Conventionally, the annunciator which embedded the indicator and the final controlling element on the monitoring board main part is used as this kind of a facility management device. Annunciator is widely used, in order to perform condition monitoring, such as a plant and equipment of a building.

The state of various management points (temperature, humidity, a flow, etc.) is displayed in the partitioning region divided into matrix form for every management point.

It is possible to perform various equipment, operation/stop of apparatus, etc. by easy operation from the partitioning region which shows the state of this management point. The annunciator with such a feature is used abundantly in the minor scale system, in order to live a full-time operator in a dish.

[0003] On the other hand, in the multifunctional building management system, the state of the various management points in a building is managed with the building management device provided with the display. The outline of the conventional building management system is shown in drawing 6. In the figure, the equipment integral controller by which 1 was distributed by the various management points in a building, and 2 (2-1 - 2-n) was distributed in the building, and 3 are the building management devices formed in the central supervision room of the building.

[0004] In this building management system, the equipment integral controller 2-1 - 2-n collect periodically the data from the various management points 1 under self management, and send these collected data to the building management device 3 via communication line L. The building management device 3 stores the data from the various management points 1 through the equipment integral controller 2-1 - 2-n, and displays the state of the various management points 1 on a display to meet the demand from a user. The building management device 3 has many functions.

It is possible the display of a summary graph, the check of daily report data, the check of an alarm history, and start-and-stop operation of apparatus and equipment, and to make setting out, change, etc. of a time schedule from a screen.

[0005]

[Problem(s) to be Solved by the Invention] The building management device provided with the display is various functions as compared with the annunciator mentioned

above, and can supervise a building on many sides. In recent years, it should be considered as intelligible screen constitution, and should excel in visibility, and improvement in operativity is further aimed at so that it can be easily operated also with an operator without a know how. However, since it is various functions, in order for there to be also much number of sheets of a screen and to display a desired screen, he fully needs to understand screen constitution, functional constitution, etc. For this reason, a manual must be read carefully and the operation method according to a function must be mastered. It will not have resulted, by the time it can perform carrying out the education of an operator, etc. or arranging a full-time operator etc. by easy operation like annunciator.

[0006]There is a place which it was made in order that this invention might solve such a technical problem, and is made into the purpose in providing the facility management device which can aim at marked improvement in operativity by cooperation with an annunciator function and the display function of a management screen, while managing a many-sided institution.

[0007]

---

[Means for Solving the Problem]In order to attain such a purpose, the 1st invention (invention concerning claim 1), A management point displaying means which classifies a state of various management points in an institution into the 1st display section, and displays it for every management point, When selected designation of the desired management point is carried out among management points currently classified and shown by this management point displaying means, a registration picture displaying means which displays a management screen registered to that management point on the 2nd display section is established. According to this invention, a state of various management points in an institution is classified and displayed on the 1st display section for every management point, If selected designation of the desired management point is carried out among management points currently classified and displayed on this 1st display section, a management screen registered to that management point will be displayed on the 2nd display section. Namely, if a state of various management points is classified and displayed on the 1st display section for every management point like annunciator and selected designation of the desired management point is carried out in this 1st display section, A management screen registered in relation to the management point interlocks, and is displayed on the 2nd display section.

[0008]Inside of a management point with which the state is shown to the 1st display section by management point displaying means in the 1st invention as for the 2nd invention (invention concerning claim 2), A registration picture alteration means which enables change of a management screen registered into the management point about a management point of a request by which selected designation was carried out is established. According to this invention, selected designation of the desired management point can be carried out among management points currently classified and displayed on the 1st display section, and a management screen registered into that management point can be changed.

[0009]The 3rd invention (invention concerning claim 3) forms an authentication means which attests an operator who tries to change a management screen registered into a registration picture alteration means, and a screen list display means to display a list of screens according to an operator's attested level, in the 2nd invention. According to this invention, an operator is attested with an ID number, a password, etc. and a list of screens according to an operator's attested level is displayed.

[0010]

[Embodiment of the Invention] Hereafter, this invention is explained in detail based on a drawing. Drawing 1 is a figure showing the outline of the building management system containing the 1 embodiment of the facility management device concerning this invention. In the figure, a component that drawing 6 and identical codes are the same or equivalent is shown, and the explanation is omitted.

[0011] This building management system is provided with the monitoring instrument 4 having the function of annunciator, and the display function of the management screen. This monitoring instrument 4 is the 1 embodiment of the facility management device concerning this invention. The indicator and the final controlling element are embedded on the monitoring board main part, and the monitoring instrument 4 has the 1st display section 4-1 and 2nd display section 4-2. The touch panel with the 1st display section 4-1 and 2nd display section 4-2 transparent in the front face is provided.

[0012] The monitoring instrument 4 is provided with RAM4-4, CPU4-3, and ROM4-5 [besides the 1st display section 4-1 and the 2nd display section 4-2]-5, the interface 4-6 to 4-8, etc. as the outline of the internal configuration is shown in drawing 2. CPU4-3 operates according to the program stored in ROM4-5, acquiring the various input given via the interface 4-6 to 4-8, and accessing RAM4-4.

[0013] In this embodiment, the data from the various management points 1 is given to CPU4-3 via the equipment integral controller 2-1 shown in drawing 1 via the interface 4-8 - 2-n. CPU4-3 accesses the building management device 3 via the interface 4-8. CPU4-3 performs all processing operation mentioned later.

[0014] The example of a screen display in the 1st display section 4-1 and 2nd display section 4-2 is shown in drawing 3. The annunciator screen G1 is displayed on the 1st display section 4-1. In the annunciator screen G1, the state of each management point is displayed on the display block BL (BL1-BL18) of the rectangle divided into matrix form. Hereafter, this display block BL is called a tag.

[0015] The indicator L1 and L2 which imitated the light emitting diode (LED) are provided in the tag BL. The state of a management point is displayed by the indicator L1, lighting / putting out lights / blink of L2, etc. The character representation of the state is carried out to the name of a management point into the tag BL.

[0016] For example, the character representation of the name of a management point is carried out to "the air conditioning machine 1", and the character representation of the state is carried out to tag BL1 "under the stop." The state "under stop" of this management point is shown by the red light of the indicator L2. When this management point "is operating", the indicator L1 carries out green lighting. When this management point is an abnormal condition, the indicator L2 blinks in red.

[0017] In addition to the annunciator screen G1, run button BT1, earth-switch BT2, registration/change button BT3, and complete button BT4 are displayed on the 1st display section 4-1. For example, if run button BT1 is pushed and tag BL1 is touched, "the air conditioning machine 1" will be started. If earth-switch BT2 is pushed and tag BL2 is touched, "the fan 1" will stop. The function of registration/change button BT3 and complete button BT4 is mentioned later.

[0018] The management screen G2 registered to the tag BL is displayed on the 2nd display section 4-2. For example, if tag BL1 is touched, the management screen G2 registered to tag BL1 will interlock, and will be displayed on the 2nd display section 4-2. This screen G2 is sent from the building management device 3 by access through the interface 4-8 of CPU4-3.

[0019] Drawing 3 touches tag BL1 and shows the example which displayed the



management screen (this example summary graph of the first floor floor) G2 registered to tag BL1 on the 2nd display section 4-2. In the 2nd display section 4-2, various kinds of operations made possible by the building management device 3 side can also be performed not only using the check of the display information of the management screen G2 but using the function added to the management screen G2. For example, in this example, start-and-stop operation of the air conditioning machine shown in that top view etc. can be performed in the summary graph G2 of the first floor floor.

[0020]Thus, if the desired tag BL is touched according to this embodiment, the management screen G2 (a summary graph.) registered to the tag BL. A schedule setting screen, an alarm history screen, etc. interlock, and are displayed on the 2nd display section 4-2, and it becomes possible to manage a building on many sides by using the function which looks at the display information of this management screen G2, or is added to this management screen G2. since a management screen related only by touching the tag BL of a request of the 1st display section 4-1 appears in the 2nd display section 4-2 immediately, it is not necessary to look for a one by one related management screen, and operativity is markedly alike and improves.

[0021][Registration and change of a screen to a tag] In \*\*\*\*, although explained as that into which the management screen is already registered to the tag BL, the registration and change of a management screen to the tag BL can be made as follows. The operations of registration and change are the same.

[0022]First, registration/change button BT3 is pushed in the 1st display section 4-1 (Step 401 shown in drawing 4: refer to drawing 5 (a)). And the tag BL of the request which wants to register or change a management screen is touched (Step 402: refer to drawing 5 (b)). Then, select list LS1 as shown in drawing 5 (c) appears (Step 403).

[0023]Since the item of a "point", a "screen", and "others" appears, a "screen" is chosen as this select list LS1 from this item (Step 404). Then, as shown in drawing 5 (d), list LS2 of the management screen which can be registered appears (Step 405). A management screen to register from this screen list LS2 or a management screen to change is chosen (Step 406), and complete button BT4 is pushed (Step 407). Then, the management screen chosen from screen list LS2 is registered to the tag BL of the request which carried out selected designation by drawing 5 (b).

[0024]If the "point" is chosen from select list LS1, not screen list LS2 but a point list (not shown) will be displayed. From this point list, a desired management point can also be assigned to the tag BL which carried out selected designation like screen list LS2.

[0025]When a "screen" is chosen from select list LS1, he is trying to display the screen list LS2 [ same irrespective of an operator's levels (a post, expertise, etc.) ] in the embodiment mentioned above, but it may be made to display screen list LS2 according to the operator's level.

[0026]For example, when registration/change button BT3 is pushed in Step 401, the input of an ID number or a password is urged. And an operator is attested with the ID number and password which were entered, and screen list LS2 according to the operator's attested level is displayed. Screen list LS2 according to the operator's level is defined beforehand.

[Claim(s)]

[Claim 1]A facility management device comprising:

A management point displaying means which classifies a state of various

management points in an institution into the 1st display section, and displays it for every management point.

A registration picture displaying means which displays a management screen registered to that management point on the 2nd display section when selected designation of the desired management point is carried out among management points currently classified and shown by this management point displaying means.

[Claim 2] Inside of a management point with which the state is shown to said 1st display section by said management point displaying means in a facility management device indicated to claim 1, A facility management device provided with a registration picture alteration means which enables change of a management screen registered into the management point about a management point of a request by which selected designation was carried out.

[Claim 3] A facility management device indicated to claim 2, comprising:

An authentication means which attests an operator who tries to change a management screen where said registration picture alteration means is registered.

A screen list display means to display a list of screens according to an operator's level attested by this authentication means.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-141659

(P2003-141659A)

(43) 公開日 平成15年5月16日 (2003.5.16)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	キーワード <sup>6</sup> (参考)
G 0 8 B 23/00	5 1 0	C 0 8 B 23/00	5 1 0 D 5 B 0 6 9
G 0 6 F 3/00	6 5 2	C 0 6 F 3/00	6 5 2 C 5 C 0 8 7
	3 5 0		3 5 0 A 5 E 5 0 1
G 0 8 B 25/04		C 0 8 B 25/04	A

審査請求 未請求 請求項の数 3 O L (全 7 頁)

(21) 出願番号 特願2001-334064(P2001-334064)

(22) 出願日 平成13年10月31日 (2001.10.31)

(71) 出願人 595123535

山武ビルシステム株式会社  
東京都港区芝浦4丁目3番4号

(72) 発明者 伊世井 恒男

東京都港区芝浦4丁目3番4号 山武ビル  
システム株式会社内

(74) 代理人 100064621

弁理士 山川 政樹

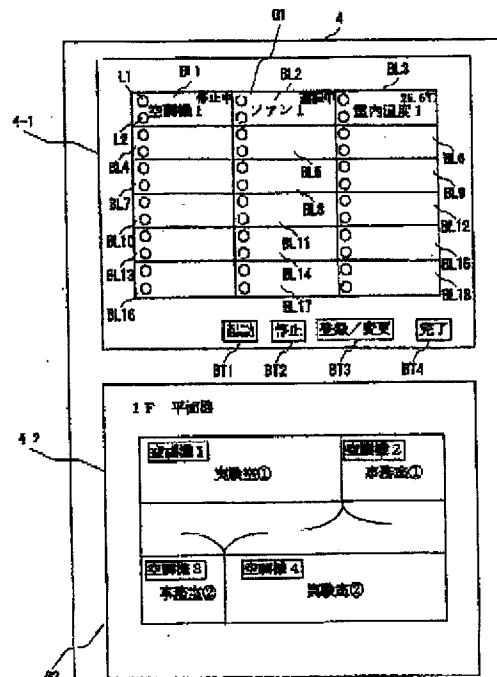
最終頁に続く

(54) 【発明の名称】 施設管理装置

(57) 【要約】

【課題】 アナンシェータ機能と管理画面の表示機能との連携により、多角的な施設の管理を行うとともに、操作性の格段の向上を図る。

【解決手段】 監視装置4に第1の画面表示部4-1と第2の画面表示部4-2とを設ける。第1の画面表示部4-1にはアナンシェータ画面G1を表示する。アナンシェータ画面G1において、各管理ポイントの状態は、マトリックス状に区切られたタグBLに表示される。第2の画面表示部4-2には、例えばタグBL1がタッチされた場合、そのタグBL1に対して登録されている管理画面G2 (サマリグラフ) を表示する。



【特許請求の範囲】

【請求項1】 施設内の各種管理ポイントの状態を各管理ポイント毎に第1の画面表示部に区分けして表示する管理ポイント表示手段と、

この管理ポイント表示手段によって区分けして表示されている管理ポイントの内、所望の管理ポイントが選択指定された場合、その管理ポイントに対して登録されている管理画面を第2の画面表示部に表示する登録画面表示手段とを備えたことを特徴とする施設管理装置。

【請求項2】 請求項1に記載された施設管理装置において、

前記管理ポイント表示手段によってその状態が前記第1の画面表示部に表示されている管理ポイントの内、選択指定された所望の管理ポイントについて、その管理ポイントに登録されている管理画面の変更を可能とする登録画面変更手段を備えたことを特徴とする施設管理装置。

【請求項3】 請求項2に記載された施設管理装置において、

前記登録画面変更手段は、登録されている管理画面の変更を行おうとする操作者を認証する認証手段と、

この認証手段によって認証された操作者のレベルに応じた画面のリストを表示する画面リスト表示手段とを備えたことを特徴とする施設管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ビルなどの施設内の各種管理ポイントの状態を管理する施設管理装置に関するものである。

【0002】

【従来の技術】従来より、この種の施設管理装置として、表示部や操作部を監視盤本体に埋め込んだアナンシェータが用いられている。アナンシェータは、プラントや建物の設備などの状態監視を行うために広く利用されており、各種管理ポイント（温度や湿度、流量など）の状態を各管理ポイント毎にマトリックス状に区切られた仕切領域にて表示する。また、この管理ポイントの状態を示す仕切領域から各種設備や機器の運転/停止などを、簡単な操作で行うことが可能である。このような特徴をもつアナンシェータは、専任のオペレータをおかずにすむために、中小規模システムにおいて多用されている。

【0003】一方、多機能のビル管理システムでは、ビル内の各種管理ポイントの状態をディスプレイを備えたビル管理装置によって管理している。図6に従来のビル管理システムの概略を示す。同図において、1はビル内の各種管理ポイント、2（2-1～2-n）はビル内に分散配置された設備統合コントローラ、3はビルの中央監視室に設けられたビル管理装置である。

【0004】このビル管理システムにおいて、設備統合

コントローラ2-1～2-nは自己の管理下の各種管理ポイント1からのデータを定期的に収集し、この収集したデータを通信ラインLを介してビル管理装置3に送る。ビル管理装置3は、設備統合コントローラ2-1～2-nを介する各種管理ポイント1からのデータを蓄積し、ユーザからの要求に応じて各種管理ポイント1の状態をディスプレイに表示する。ビル管理装置3は、多くの機能を有しており、サマリグラフの表示、日報データの確認、警報履歴の確認、機器や設備の発停操作、タイムスケジュールの設定や変更などを画面上から行うことが可能である。

【0005】

【発明が解決しようとする課題】ディスプレイを備えたビル管理装置は、前述したアナンシェータと比較して多機能であり、多角的にビルの監視を行うことができる。近年、専門知識を持っていないオペレータでも簡単に操作できるように、分かり易い画面構成とし、また視認性に優れたものとし、さらに操作性の向上を図っている。しかし、多機能であるために画面の枚数も多く、所望の画面を表示するには、画面構成、機能構成などを充分に理解しておく必要がある。このため、マニュアルを熟読し、機能に応じた操作方法を習得しなければならない。また、オペレータの教育などを実施したり、専任のオペレータを配置するなど、アナンシェータのように簡単な操作で行えるまでには至っていない。

【0006】本発明はこのような課題を解決するためになされたもので、その目的とするところは、アナンシェータ機能と管理画面の表示機能との連携により、多角的な施設の管理を行うとともに、操作性の格段の向上を図ることのできる施設管理装置を提供することにある。

【0007】

【課題を解決するための手段】このような目的を達成するために、第1発明（請求項1に係る発明）は、施設内の各種管理ポイントの状態を各管理ポイント毎に第1の画面表示部に区分けして表示する管理ポイント表示手段と、この管理ポイント表示手段によって区分けして表示されている管理ポイントの内、所望の管理ポイントが選択指定された場合、その管理ポイントに対して登録されている管理画面を第2の画面表示部に表示する登録画面表示手段とを設けたものである。この発明によれば、第1の画面表示部に施設内の各種管理ポイントの状態が各管理ポイント毎に区分けして表示され、この第1の画面表示部に区分けして表示されている管理ポイントの内、所望の管理ポイントを選択指定すると、その管理ポイントに対して登録されている管理画面が第2の画面表示部に表示される。すなわち、アナンシェータのように第1の画面表示部に各種管理ポイントの状態が各管理ポイント毎に区分けして表示され、この第1の画面表示部において所望の管理ポイントを選択指定すると、その管理ポイントと関連して登録されている管理画面が第2の画面

表示部に連動して表示される。

【0008】第2発明(請求項2に係る発明)は、第1発明において、管理ポイント表示手段によってその状態が第1の画面表示部に表示されている管理ポイントの内、選択指定された所望の管理ポイントについて、その管理ポイントに登録されている管理画面の変更を可能とする登録画面変更手段を設けたものである。この発明によれば、第1の画面表示部に区分けして表示されている管理ポイントの内、所望の管理ポイントを選択指定して、その管理ポイントに登録されている管理画面を変更することができる。

【0009】第3発明(請求項3に係る発明)は、第2発明において、登録画面変更手段に、登録されている管理画面の変更を行おうとする操作者を認証する認証手段と、認証された操作者のレベルに応じた画面のリストを表示する画面リスト表示手段とを設けたものである。この発明によれば、ID番号やパスワードなどによって操作者が認証され、認証された操作者のレベルに応じた画面のリストが表示される。

【0010】

【発明の実施の形態】以下、本発明を図面に基づいて詳細に説明する。図1は本発明に係る施設管理装置の一実施の形態を含むビル管理システムの概略を示す図である。同図において、図6と同一符号は同一或いは同等構成要素を示し、その説明は省略する。

【0011】このビル管理システムは、アナンシェータの機能と管理画面の表示機能とを合わせ持った監視装置4を備えている。この監視装置4が本発明に係る施設管理装置の一実施の形態である。監視装置4は、表示部や操作部が監視盤本体に埋め込まれており、第1の画面表示部4-1と第2の画面表示部4-2とを有している。第1の画面表示部4-1および第2の画面表示部4-2はその前面に透明のタッチパネルが設けられている。

【0012】また、監視装置4は、図2にその内部構成の概略を示すように、第1の画面表示部4-1および第2の画面表示部4-2の他、CPU4-3やRAM4-4、ROM4-5、インターフェイス4-6~4-8などを備えている。CPU4-3は、インターフェイス4-6~4-8を介して与えられる各種入力情報を得て、RAM4-4にアクセスしながら、ROM4-5に格納されたプログラムに従って動作する。

【0013】なお、この実施の形態において、CPU4-3には、インターフェイス4-8を介して、図1に示した設備統合コントローラ2-1~2-nを経由して各種管理ポイント1からのデータが与えられる。また、CPU4-3は、インターフェイス4-8を介して、ビル管理装置3にアクセスする。また、後述する処理動作は、全てCPU4-3が行う。

【0014】図3に第1の画面表示部4-1および第2の画面表示部4-2における画面表示例を示す。第1の

画面表示部4-1にはアナンシェータ画面G1が表示される。アナンシェータ画面G1において、各管理ポイントの状態は、マトリックス状に区切られた矩形的表示ブロックBL(BL1~BL18)に表示される。以下、この表示ブロックBLをタグと呼ぶ。

【0015】タグBLには発光ダイオード(LED)を模した表示部L1、L2が設けられている。表示部L1、L2の点灯/消灯/点滅などで管理ポイントの状態が表示される。また、タグBL中に、管理ポイントの名称とその状態が文字表示される。

【0016】例えば、タグBL1には、管理ポイントの名称が「空調機1」と文字表示され、その状態が「停止中」と文字表示されている。また、この管理ポイントの「停止中」の状態は、表示部L2の赤色点灯によっても表示されている。なお、この管理ポイントが「運転中」である場合には、表示部L1が緑色点灯する。また、この管理ポイントが異常状態である場合には、表示部L2が赤色で点滅する。

【0017】第1の画面表示部4-1には、アナンシェータ画面G1に加えて、起動ボタンBT1、停止ボタンBT2、登録/変更ボタンBT3、完了ボタンBT4が表示される。例えば、起動ボタンBT1を押し、タグBL1をタッチすると、「空調機1」が起動される。停止ボタンBT2を押し、タグBL2をタッチすると、「ファン1」が停止する。登録/変更ボタンBT3、完了ボタンBT4の機能については後述する。

【0018】第2の画面表示部4-2にはタグBLに対して登録されている管理画面G2が表示される。例えば、タグBL1をタッチすると、タグBL1に対して登録されている管理画面G2が第2の画面表示部4-2に連動して表示される。この画面G2は、CPU4-3のインターフェイス4-8を介するアクセスにより、ビル管理装置3より送られてくる。

【0019】図3は、タグBL1をタッチし、タグBL1に対して登録されている管理画面(この例では、1階フロアのサマリグラフ)G2を第2の画面表示部4-2に表示した例を示している。第2の画面表示部4-2では、管理画面G2の表示内容の確認のみならず、その管理画面G2に付加されている機能を利用して、ビル管理装置3側で可能とされている各種の操作を行うこともできる。例えば、この例では、1階フロアのサマリグラフG2において、その平面図中に示された空調機の発停操作などを行うことができる。

【0020】このように、本実施の形態によれば、所望のタグBLをタッチすると、そのタグBLに対して登録されている管理画面G2(サマリグラフ、スケジュール設定画面、警報履歴画面など)が第2の画面表示部4-2に連動して表示され、この管理画面G2の表示内容を見たり、この管理画面G2に付加されている機能を利用して、多角的にビル管理を行うことが可能

となる。また、第1の画面表示部4-1の所望のタグBLをタッチするのみで、関連する管理画面が即座に第2の画面表示部4-2に現れるので、一々関連する管理画面を探さなくてもよく、操作性が格段に向上する。

【0021】〔タグに対する画面の登録および変更〕上述においては、タグBLに対してすでに管理画面が登録されているものとして説明したが、タグBLに対する管理画面の登録や変更は次のようにして行うことができる。登録も変更も操作は同じである。

【0022】まず、第1の画面表示部4-1において、登録/変更ボタンBT3を押す(図4に示すステップ401;図5(a)参照)。そして、管理画面を登録あるいは変更したい所望のタグBLにタッチする(ステップ402;図5(b)参照)。すると、図5(c)に示すような選択リストLS1が現れる(ステップ403)。

【0023】この選択リストLS1には、「ポイント」、「画面」、「その他」という項目が現れるので、この項目から「画面」を選択する(ステップ404)。すると、図5(d)に示すように、登録可能な管理画面のリストLS2が出現する(ステップ405)。この画面リストLS2から登録したい管理画面、あるいは変更したい管理画面を選択し(ステップ406)、完了ボタンBT4を押す(ステップ407)。すると、画面リストLS2より選択した管理画面が、図5(b)で選択指定した所望のタグBLに対して登録される。

【0024】なお、選択リストLS1から「ポイント」を選択すると、画面リストLS2ではなく、ポイントリスト(図示せず)が表示される。このポイントリストから、画面リストLS2と同様にして、選択指定したタグBLに所望の管理ポイントを割り付けることもできる。

【0025】上述した実施の形態では、選択リストLS1から「画面」が選択された場合、操作者のレベル(役職や専門技術など)に拘わらず同じ画面リストLS2を表示するようにしているが、操作者のレベルに応じた画面リストLS2を表示するようにしてもよい。

【0026】例えば、ステップ401において登録/変更ボタンBT3が押された場合、ID番号やパスワードの入力を促すようにする。そして、入力されたID番号やパスワードで操作者を認証し、認証した操作者のレベルに応じた画面リストLS2を表示する。操作者のレベルに応じた画面リストLS2は予め定義しておく。

【0027】

【発明の効果】以上説明したことから明らかなように本発明によれば、第1の画面表示部に施設内の各種管理ポ

イントの状態が各管理ポイント毎に区分けして表示され、この第1の画面表示部に区分けして表示されている管理ポイントの内、所望の管理ポイントを選択指定すると、その管理ポイントに対して登録されている管理画面が第2の画面表示部に表示されるものとなり、第2の画面表示部に表示される管理画面の表示内容を見たり、この管理画面に付加されている機能を利用することにより、多角的に施設の管理を行うことが可能となるとともに、一々関連する管理画面を探さなくてもよく、操作性が格段に向上するものとなる。また、第1の画面表示部に区分けして表示されている管理ポイントの内、所望の管理ポイントを選択指定して、その管理ポイントに登録されている管理画面を変更することができるようにすることにより、操作者が頻繁に利用する管理画面を第2の画面表示部に表示させることが可能となり、操作性がさらに向上する。また、ID番号やパスワードで操作者を認証するようにし、認証された操作者のレベルに応じた画面のリストを表示することにより、操作者の役職や専門技術に適した画面のみを表示させることが可能となり、施設におけるセキュリティ性を確保することができるようになる。

【図面の簡単な説明】

【図1】 本発明に係る施設管理装置の一実施の形態(監視装置)を含むビル管理システムの概略を示す図である。

【図2】 このビル管理システムにおける監視装置の内部構成の概略を示すブロック図である。

【図3】 この監視装置の第1の画面表示部および第2の画面表示部における画面表示例を示す図である。

【図4】 所望のタグに対して管理画面の登録および変更を行う場合の操作過程を示すフローチャートである。

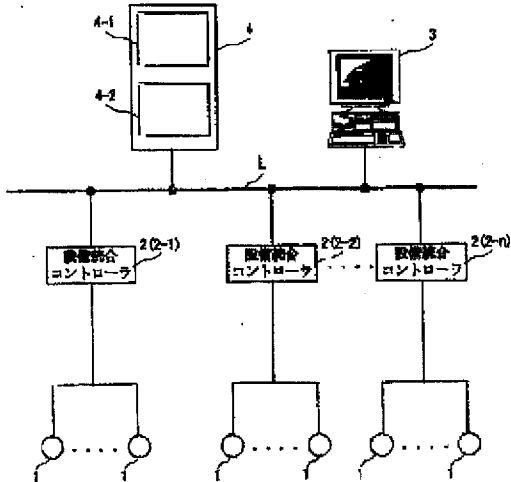
【図5】 所望のタグに対して管理画面の登録および変更を行う場合の操作過程を説明する図である。

【図6】 従来のビル管理システムの概略を示す図である。

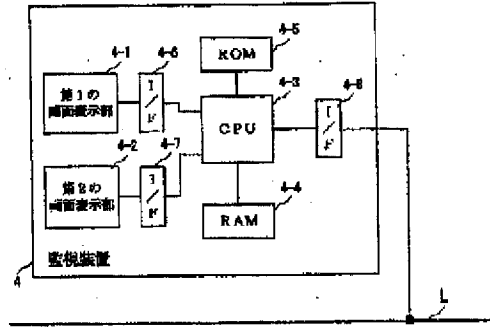
【符号の説明】

4…監視装置、4-1…第1の画面表示部、4-2…第2の画面表示部、4-3…CPU、4-4…RAM、4-5…ROM、4-6~4-8…インターフェイス、BL(BL1~BL18)…表示ブロック(タグ)、L1、L2…表示部、BT1…起動ボタン、BT2…停止ボタン、BT3…登録/変更ボタン、BT4…完了ボタン、G1…アナンシェータ画面、G2…管理画面、LS1…選択リスト、LS2…画面リスト。

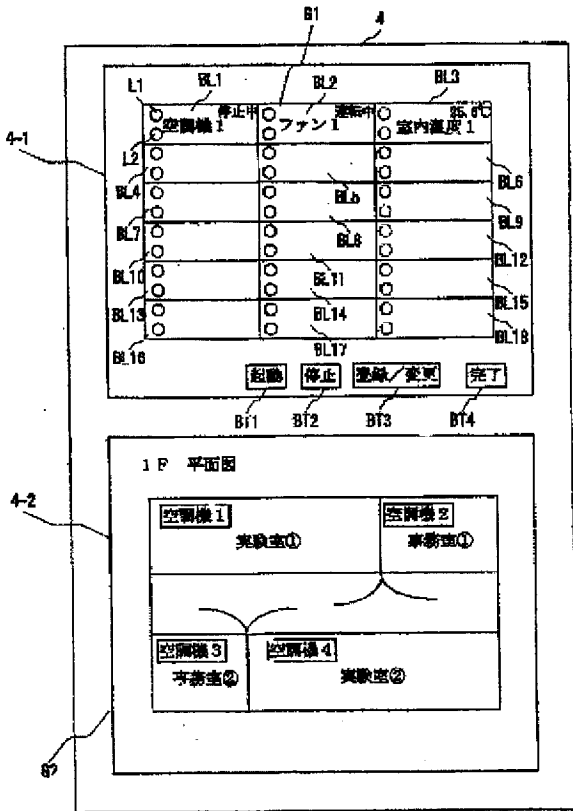
【図1】



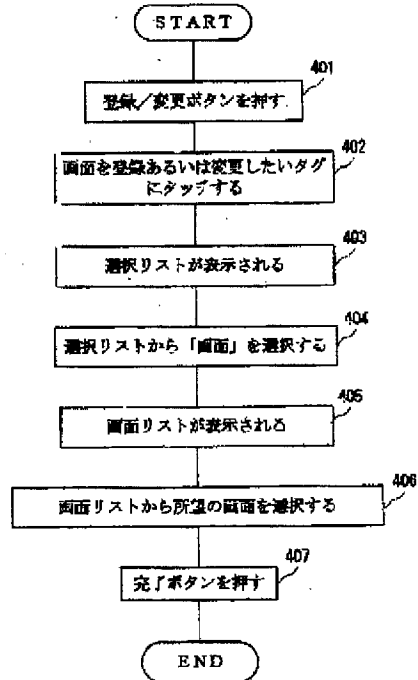
【図2】



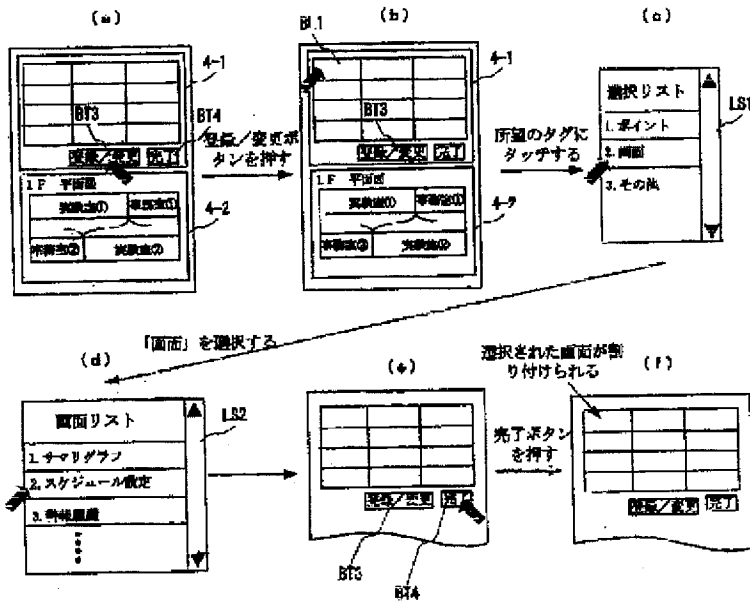
【図3】



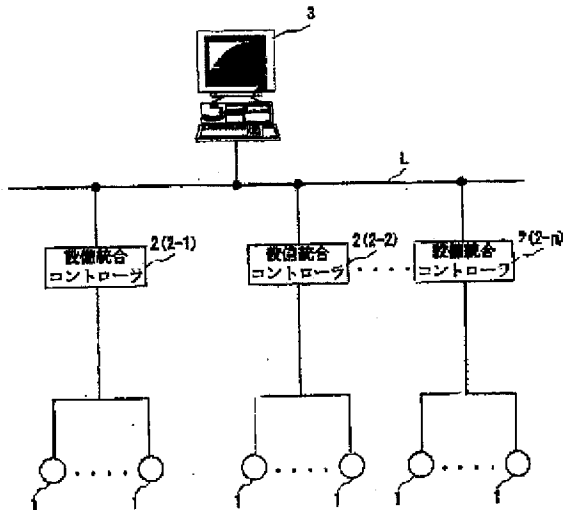
【図4】



【図5】



【図6】





フロントページの続き

Fターム(参考) 5B069 CA03 CA13 CA18  
5C087 AA02 AA03 AA24 AA25 BB03  
BU74 DD03 DD23 DD33 EE06  
EE14 FF01 FF02 FF04 FF19  
FF20 GG12 GG23 GG30 GG31  
GG32 GG51 GG66  
5E501 AA01 AC05 AC32 AC42 BA05  
CA02 DA15 EA05 FA03 FA10  
FB28

© EPODOC / EPO

PN - JP2004192659 A 20040708  
 OPD - 2004-02-27  
 PA - SONY CORP  
 IN - CHIHARA SHUICHI  
 TI - DATA PROCESSING METHOD, AND DATA PROCESSOR  
 AB - PROBLEM TO BE SOLVED: To convert a format of data into a reproducible format in regard to a data processing method and a data processor.  
 - SOLUTION: A home gateway 1 judges whether or not output data is a format which can be reproduced by an output target apparatus on the basis of a reproduction request by a user. If the output data is not a format which can be reproduced by the output target apparatus, the home gateway 1 converts the output data into a format which can be reproduced by the output target apparatus, and supplies it to the output target apparatus. The present invention can be applied in a home gateway for example.  
 - COPYRIGHT: (C)2004,JPO&NCIP  
 FI - G06F12/00&511C; G06F12/00&520E  
 FT - 5B082/AA13; 5B082/EA09; 5B082/HA05  
 IC - G06F12/00  
 ICAI - G06F12/00  
 ICCI - G06F12/00  
 AP - JP20040053432 20040227  
 PR - JP20040053432 20040227  
 FAMN - 32768237  
 PD - 2004-07-08

© WPI / Thomson

AN - 2004-536817 [52]  
 OPD - 1997-03-28  
 PD - 2004-07-08  
 AP - [Div Ex] JP19970077283 19970328; JP20040053432 20040227  
 PA - {SONY } SONY CORP  
 CPY - SONY  
 IN - CHIHARA S  
 TI - Data processing method in data management system in home, involves converting data to format compatible for reproduction at destination apparatus  
 AB - NOVELTY :  
 The data is converted into a format compatible for reproduction at the destination apparatus e.g. TV (3), prior to transmission to destination apparatus, if the format of the output data is judged to be incompatible for reproduction at destination apparatus.  
 - DETAILED DESCRIPTION :  
 An INDEPENDENT CLAIM is also included for data processor.  
 - USE :  
 For processing data e.g. music data, moving image data, still image data and audio data in platform gateway for storing or reproducing data using TV, digital video tape recorder (DVTR), cassette tape recorder, mini disk recorder, digital versatile disk (DVD)-RAM recorder, magnetic tape recorder, hard disk and personal computer in data management system at home or office.  
 - ADVANTAGE :

Enables efficient format conversion data prior to display in TV.

- DESCRIPTION OF DRAWINGS :

The figure shows a block diagram of the data management system. (Drawing includes non-English language text).

1 : home gateway

2 : digital video tape recorder

3 : TV

4 : cassette tape recorders

5 : mini disk recorder

6 : DVD-RAM recorder

7 : personal computer

8 : network

PN - JP2004192659 A 20040708 DW200452

NC - 1

IW - DATA PROCESS METHOD MANAGEMENT SYSTEM HOME CONVERT FORMAT COMPATIBLE  
REPRODUCE DESTINATION APPARATUS

IC - G06F12/00

MC - T01-D02 W04-P01A W04-V10

DC - T01 W04

- NOTICES \*

**JPO and INPIT are not responsible for any damages caused by the use of this translation.**

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

[Detailed Description of the Invention]

[Field of the Invention]

[0001]

Especially this invention relates to the data processing method and data processing device which transform the form of data into a refreshable form about a data processing method and a data processing device.

[Background of the Invention]

[0002]

The variety of information is provided via various media as predetermined data and signal of form with progress of semiconductor technology. For example, transmission and reception of various digital data are performed via the computer network. Such digital data is saved at the hard disk connected or built in the computer in many cases.

[0003]

On the other hand, when supplying music data etc., the portable recording medium of MD (trademark) (mini disc) etc. is used in many cases, for example.

[0004]

What is called some electrical household appliances and electrical equipment record predetermined data and signal of form on a predetermined medium like the MD recorder which records data, for example on MD.

[0005]

Since management of data is performed for every apparatus while the portability and flexibility of data are missing, since the management gestalt of different data for every apparatus is adopted, such electrical household appliances and electrical equipment (and recording medium corresponding to it) are difficult to visualize the management state of all the data.

[Description of the Invention]

[Problem(s) to be Solved by the Invention]

[0006]

By the way, in the home gate way where the television receiver (TV) was connected, for example, It is convenient if data can judge whether it is a refreshable form by TV, it can change into a refreshable form by TV when it is not a refreshable form by TV, and the data after the conversion can be supplied to TV.

[0007]

This invention was made in view of such a situation, and transforms the form of data into a refreshable form.

[Means for Solving the Problem]

[0008]

This invention is characterized by a data processing method comprising the following. A judgment step output data judges it to be whether it is a refreshable form by apparatus of an output destination change based on a reproduction request by a user.

A converting step which changes output data into a refreshable form by apparatus of an output destination change when output data is not a refreshable form by apparatus of an output destination change.

A supply step which supplies output data changed into a refreshable form by apparatus of an output destination change to apparatus of an output destination change.

[0009]

A data processing method can be performed in a home gate way.

[0010]

In a home gate way, management data of output data described with a markup language can be memorized.

[0011]

A request step which requires output data memorized by apparatus other than apparatus of an output destination change of a data processing method based on a user's reproduction request and management data, From another apparatus, a receiving step which receives output data can be provided further, and output data received in a receiving step can make a judgment step judge whether it is a refreshable form by apparatus of an output destination change.

[0012]

Another apparatus can be connected to a home gate way via a wide area network.

[0013]

This invention is characterized by a data processing device comprising the following.

A decision means output data judges it to be whether it is a refreshable form by apparatus of an output destination change based on a reproduction request by a user.

A conversion method which changes output data into a refreshable form by apparatus of an output destination change when output data is not a refreshable form by apparatus of an output destination change.

A feeding means which supplies output data changed into a refreshable form by apparatus of an output destination change to apparatus of an output destination change.

[0014]

A data processing device can be made into a home gate way.

[0015]

In a home gate way, management data of output data described with a markup language can be memorized.

[0016]

A request means which requires output data memorized by apparatus other than apparatus of an output destination change of a data processing device based on a user's reproduction request and management data, From another apparatus, a reception means which receives output data can be established further, and output data received in a reception means can make a decision means judge whether it is a refreshable form by apparatus of an output destination change.

[0017]

Another apparatus can be connected to a home gate way via a wide area network.

[0018]

In a data processing method and a data processing device of this invention, Based on a reproduction request by a user, it is judged whether output data is a refreshable form with apparatus of an output destination change, and when output data is not a

refreshable form by apparatus of an output destination change, output data is changed into a refreshable form by apparatus of an output destination change. Output data changed into a refreshable form by apparatus of an output destination change is supplied to apparatus of an output destination change.

[Effect of the Invention]

[0019]

According to the data processing method and data processing device of this invention, the form of data is convertible for a refreshable form.

[Best Mode of Carrying Out the Invention]

[0020]

Although the best gestalt of this invention is explained below, it is as follows when the correspondence relation between constituent features given in a claim and the example in an embodiment of the invention is illustrated. This statement is for the example which supports the invention indicated to the claim to check what is indicated to the embodiment of the invention. therefore, an embodiment of the invention -- although indicated in inside, even if the example which is not indicated is here as a thing corresponding to constituent features, that does not mean that the example is not a thing corresponding to the constituent features. On the contrary, though the example was indicated as a thing corresponding to constituent features here, that does not mean that the example is what does not correspond to any constituent features other than the constituent features, either.

[0021]

This statement does not mean that the invention corresponding to the example indicated to the embodiment of the invention is altogether indicated to the claim. If it puts in another way, this statement is the invention corresponding to the example indicated to the embodiment of the invention, it will be divided, or it will appear by amendment, and existence of the invention which is not indicated to the claim of this application, i.e., in the future, will not deny existence of the invention added.

[0022]

The data processing method according to claim 1,

In the data processing method which processes the output data outputted to the apparatus of an output destination change,

The judgment step (for example, processing of Step S106 of drawing 11) said output data judges it to be whether it is a refreshable form by the apparatus of said output destination change based on the reproduction request by a user,

The converting step (for example, processing of Step S107 of drawing 11) which changes said output data into a refreshable form by the apparatus of said output destination change when said output data is not a refreshable form by the apparatus of said output destination change,

The supply step (for example, processing of Step S108 of drawing 11) which supplies the output data changed into a refreshable form by the apparatus of said output destination change to the apparatus of said output destination change

\*\*\*\*\* -- it is characterized by things.

[0023]

The data processing method according to claim 4,

The request step (for example, processing of Step S103 of drawing 11) which requires said output data memorized by apparatus other than the apparatus of said output destination change based on said user's reproduction request and said management data,

The receiving step (for example, processing of Step S105 of drawing 11) which

receives said output data from said another apparatus

It contains in a pan,

Said judgment step judges whether it is form with said output data refreshable by the apparatus of said output destination change received in said receiving step.

It is characterized by things.

[0024]

The data processing device according to claim 6,

In the data processing device which processes the output data outputted to the apparatus of an output destination change,

The decision means (for example, CPU21 which performs processing of Step S106 of drawing 11) said output data judges it to be whether it is a refreshable form by the apparatus of said output destination change based on the reproduction request by a user,

The conversion method (for example, CPU21 which performs processing of Step S107 of drawing 11) which changes said output data into a refreshable form by the apparatus of said output destination change when said output data is not a refreshable form by the apparatus of said output destination change,

The feeding means (for example, CPU21 which performs processing of Step S108 of drawing 11) which supplies the output data changed into a refreshable form by the apparatus of said output destination change to the apparatus of said output destination change

\*\*\*\*\* -- it is characterized by things.

[0025]

The data processing device according to claim 9,

The request means (for example, CPU21 which performs processing of Step S103 of drawing 11) which requires said output data memorized by apparatus other than the apparatus of said output destination change based on said user's reproduction request and said management data,

The reception means (for example, network interface 27 of drawing 2) which receives said output data from said another apparatus

It contains in a pan,

Said decision means judges whether it is form with said output data refreshable by the apparatus of said output destination change received in said reception means.

It is characterized by things.

[0026]

Drawing 1 shows the example of 1 composition of the data management system adapting this invention. This data management system is arranged in a home or an office, for example, and the information supplied via public lines, such as a telephone line, is received in the home gate way 1, The data is managed while saving the data (text data, dynamic image data, still picture information, voice data, etc.) corresponding to the information at what is called electrical household appliances and electrical equipment that have the Records Department.

[0027]

In this data management system, to the network 8 of a predetermined standard (for example, an IEEE1394 High Performance Serial Bus standard and Ethernet (R)). As the home gate way 1 and regenerating section which perform reception and management of data. As the \*\* television receiver (TV) 3 and the Records Department. The personal computer 7 having the \*\* digital video recorder (DVTR) 2, the cassette tape recorder 4, MD recorder 5, the DVD(Digital Versatile Disc)-RAM recorder 6, and the hard disk 11, etc. are connected.

[0028]

Drawing 2 shows the example of composition of the home gate way 1. In the home gate way 1, CPU(Central Processing Unit) 21 is made as [ perform / according to the program currently recorded on ROM(Read Only Memory) 22 / various processing ].

[0029]

ROM22 holds the program compatible with reception and management of data.

[0030]

RAM(Random Access Memory) 23 is temporarily made as [ memorize / data or a program ], while various processing is performed by CPU21.

[0031]

The hard disk 24 is made as [ hold / the management data generated by CPU21 corresponding to the received signal / suitably ]. Management data is described by the hypertext markup language (HTML:Hyper-Text Markup Language).

[0032]

The communication circuit 25 is connected to the transmission medium of the public, such as a telephone line, for example, The signal corresponding to various data is received via the transmission medium, when the received signal is an analog signal after getting over, the signal is outputted to the A/D conversion circuit 26, and when it is a digital signal, it is made as [ output / to CPU21 / the signal (data) ].

[0033]

The A/D conversion circuit 26 changes into a digital signal the analog signal supplied from the communication circuit 25, and is made as [ output / to CPU21 / the signal (data) ].

[0034]

It is connected to the network 8 and the network interface 27 is made as [ receive / data / according to a predetermined standard / transmit and ].

[0035]

Drawing 3 shows the example of composition of DVTR2. The network control section 31 receives the data supplied via the network 8 from the home gate way 1, It outputs to the recording reproduction section 32, and also is made as [ supply / the signal corresponding to the directions inputted by the user in the final controlling element 33 / to the home gate way 1 / via the network 8 ].

[0036]

In the network control section 31, CPU41 is made as [ perform / according to the program currently recorded on ROM42 / various processing ]. The program compatible with above-mentioned processing is held ROM42. And RAM43 is temporarily made as [ memorize / data or a program ], while various processing is performed by CPU41. It is connected to the network 8 and the network interface 44 is made as [ receive / data / according to a predetermined standard / transmit and ].

[0037]

The recording reproduction section 32 is made as [ read / corresponding to the signal from the final controlling element 33, or the signal from CPU41 / the data which records data on the videotape (not shown) which is a recording medium, or is recorded on videotape ].

[0038]

Drawing 4 shows the example of composition of TV3. The network control section 31 receives the data supplied via the network 8 from the home gate way 1 like the thing of drawing 2, and outputs it to the drive circuit 52, and also. It is made as [ supply / the signal corresponding to the directions inputted by the user in the final controlling element 55 / to the home gate way 1 / via the network 8 ].



[0039]

it is setting out corresponding to the signal supplied from the final controlling element 55 (channel etc.), and the tuner 51 is not illustrated -- a television broadcasting signal is received via an antenna and it is made as [ output / to the drive circuit 52 / the picture signal and audio signal corresponding to the signal ].

[0040]

The drive circuit 52 the image data and voice data which are supplied from the network control section 31, While changing into an analog picture signal or an analog voice signal in the D/A conversion part 61 to build in and displaying the picture corresponding to an analog picture signal on CRT53, While making the sound corresponding to an analog voice signal output to the loudspeaker 54 and also displaying on CRT53 the picture corresponding to the picture signal supplied from the tuner 51, it is made as [ make / the sound corresponding to the audio signal supplied from the tuner 51 / output to the loudspeaker 54 ].

[0041]

the cassette tape recorder 4, MD recorder 5, and the DVD-RAM recorder 6 of drawing 1 -- a recording medium (a cassette tape (magnetic tape) and MD.) Or it has the network control section 31 like DVTR2 and TV3 besides the recording reproduction section which performs record or reproduction of data to DVD-RAM.

[0042]

Build in the network interface (not shown) corresponding to the network 8, and various processing is performed, and also the personal computer 7 is made as [ receive / data / via the network 8 / transmit and ].

[0043]

Next, operation of the home gate way 1 is explained with reference to the flow chart of drawing 5 thru/or drawing 8.

[0044]

In Step S1 (setting at the time of starting), CPU21 of the home gate way 1 performs initialization processing of each circuit of the home gate way 1 first.

[0045]

Next, in Step S2, when it is judged whether the communication circuit 25 received the signal and it is judged that the communication circuit 25 has not received the signal, in Step S3, other processings, for example, processing of the various demands supplied via the network 8, are performed, and it returns to Step S2 after that.

[0046]

Thus, other processings are performed when the communication circuit 25 has not received the signal.

[0047]

And in Step S2, when it is judged that the communication circuit 25 received the signal, it progresses to step S4 and CPU21 chooses the apparatus which becomes a preservation destination of data from the apparatus connected to the network 8 corresponding to the kind and quantity of a signal which were received (after-mentioned).

[0048]

Next, in Step S5 CPU21, In [ judge whether the data which accessed selected apparatus via the network 8 and was received can be saved, and / when it can save ] Step S7, After creating the management data corresponding to the data in HTML, the received data is outputted to the network interface 27. And the network interface 27 makes the data supply and save to selected apparatus via the network 8 (after-mentioned). Thus, after data is saved, it returns to Step S2. Management data is saved

at the hard disk 24 of the home gate way 1.

[0049]

When it is judged that the received data cannot be saved to selected apparatus in Step S5 on the other hand, in Step S6 CPU21, The information, including for example, a title, the receipt time, etc. of data, about the data (signal) which cannot be saved is saved as a predetermined file at the hard disk 24. After performing processing such at the time of preservation impossible, it returns to Step S2.

[0050]

Thus, while the received data is saved to apparatus selected corresponding to the size and kind of the data, the management data corresponding to the data is saved at the hard disk 24 of the home gate way 1. Since the saved data is put in block by the home gate way 1 and it is managed, reproduction and reuse of the saved data become easy.

[0051]

Next, with reference to the flow chart of drawing 6, the details of the processing which chooses the apparatus which saves data in step S4 of drawing 5 are explained.

[0052]

CPU21 [ first, ] of the home gate way 1, In [ in Step S21, control the network interface 27, count the kind and number of the apparatus connected to the network 8, and ] Step S22, Usable apparatus (namely, thing which has the Records Department or a recording medium and from which the power supply is turned on) is investigated among the apparatus.

[0053]

Next, in Step S23, CPU21 investigates the size of the data to save and chooses from usable apparatus the candidate of apparatus who saves the data in Step S24 corresponding to the size and kind of data to save.

[0054]

CPU21 chooses the candidate of the optimal apparatus corresponding to the cost of the recording medium to the transfer rate of the data at the time of reproduction, and predetermined storage capacity.

[0055]

And CPU21 controls the network interface 27, In [ make it investigated whether the residue and the writing to apparatus (recording medium) of the storage capacity of the apparatus chosen as the network control section 31 of selected apparatus are permitted via the network 8, and ] Step S25, When it judges whether the residue of the storage capacity of selected apparatus is more than the size of the data to save and it is judged that the residue of storage capacity is smaller than the size of the data to save, it progresses to Step S26 and it is judged whether there is other usable apparatus.

[0056]

In Step S26, when it is judged that there is other usable apparatus, after one apparatus is chosen from those apparatus, in Step S28, it returns to Step S25.

[0057]

On the other hand, in Step S26, when it is judged that other usable apparatus cannot be found, it is judged that preservation of data is impossible and it progresses to Step S5 (drawing 5).

[0058]

In Step S25, when the residue of the storage capacity of selected apparatus is judged to be more than the size of the data to save, it progresses to Step S29. And it progresses to Step S26 and CPU21 performs processing in Step S26 thru/or Step S28 as mentioned above, when it is judged that it judges whether the writing to selected apparatus (recording medium) is permitted, and the writing to selected apparatus

(recording medium) is not permitted.

[0059]

On the other hand, in Step S29, when it is judged that the writing to selected apparatus (recording medium) is permitted, it progresses to Step S30 and the apparatus is specified as the preservation destination of data.

[0060]

Thus, the apparatus which saves the data is chosen corresponding to a kind, a size, etc. of data.

[0061]

Next, with reference to the flow chart of drawing 7, the details of the processing which saves data in Step S7 of drawing 5 are explained.

[0062]

First, in [ when it is judged whether the signal received by the communication circuit 25 is a digital signal and it is judged that the received signal is not a digital signal (it is an analog signal) in Step S41 ] Step S42, The analog signal is changed into a digital signal by the A/D conversion circuit 26. When the received signal is judged to be a digital signal, Step S42 is skipped.

[0063]

And in Step S43 CPU21, It is judged whether the file name is added to the digital signal (data), That is, when it judges whether the file name is contained in the received data and it is judged that the file name is not added to the data, in Step S44, a file name is added to the data by a prescribed method (for example, method using the date which received). For example, the file name "1996\_0901\_02.xxx" is added to the 2nd data received on September 1, 1996. At this time, the extension ".xxx" is set up corresponding to the kind of data.

[0064]

When the file name is added to data, Step S44 is skipped.

[0065]

Next, in Step S45, CPU21 are a predetermined header of HTML which has a title (file name) of data, a file name of data, and a link of HTML corresponding to the memory location, and generate the management data shown, for example in drawing 8.

[0066]

The management data (what was described in HTML) shown in drawing 8, A title (file name) by the image data compressed by the JPEG (Joint Photographic Experts Group) method which is "1997\_0101\_01\_switzerland.jpg." A recording place is management data to what is "VTR1." The extension ".jpg" expresses that the data is JPEG image data. Namely, in the management data shown in drawing 8 with a link "<A HREF='http://VTR1/1997\_0101\_01\_switzerland.jpg'>." The preservation place of JPEG image data "1997\_0101\_01\_switzerland.jpg" is saved. "VTR1" is set up beforehand point out DVTR2, for example.

[0067]

In Step S45, CPU21 manages collectively the data saved under each date, for example, creates the management data according to date shown in drawing 9. In the management data according to date of drawing 9, six data saved on January 1, 1997 is registered. "md1" points out MD recorder 5, "dvd1" points out the DVD-RAM recorder 6, "cas1" points out the cassette tape recorder 4, and "vtr2" is set up beforehand point out the 2nd DVTR that is connected to the network 8 and that is not illustrated.

[0068]

And in Step S46, CPU21 of the home gate way 1 saves the management data

generated at Step S45, and the management data according to date at the hard disk 24.  
[0069]

Next, in Step S47, CPU21 supplies the signal which requires preservation of data of apparatus selected by step S4 (drawing 5) via the network interface 27 and the network 8.

[0070]

And in Step S48, CPU21 stands by until the signal which notifies completion of preservation preparation from the apparatus is supplied via the network 8.

[0071]

When the signal which notifies completion of preservation preparation is supplied, progress to Step S49 and CPU21 of the home gate way 1, Transmission of the data to selected apparatus is started via the network interface 27 and the network 8, and in Step S50, data is communicated one by one until it receives the signal which reports that all the data was received from the apparatus.

[0072]

And in Step S50, when the signal which reports that all the data was received is received, CPU21 ends processing of data storage and returns to Step S2 (drawing 5).

[0073]

Thus, when saving the received data, after the management data corresponding to the data is generated and being saved at the hard disk 24 of the home gate way 1, the received data is transmitted to selected apparatus from the home gate way 1.

[0074]

Next, operation of DVTR2 is explained with reference to the flow chart of drawing 10.

[0075]

In Step S81 (setting at the time of starting), CPU41 of DVTR2 performs initialization processing of each circuit of DVTR2 first.

[0076]

Next, in Step S82 CPU41 of the network control section 31, When it is judged that it judges whether the signal corresponding to the data storage demand from the home gate way (HGW) 1 was received, and has not received, in Step S83, other processings, for example, the processing to a user's operation in the final controlling element 33, are performed, and it returns to Step S82 after that.

[0077]

Thus, other processings are performed when not having received the signal corresponding to a data storage demand from the home gate way 1.

[0078]

And when it is judged in Step S82 that the signal corresponding to a data storage demand was received, progress to Step S84 and CPU41 of the network control section 31, When it judges whether it is possible to save data at a recording medium (videotape) and it is judged that preservation of data is not possible, in Step S85, the signal showing preservation of data not being possible for is outputted to the home gate way 1 via the network 8. And it returns to Step S82.

[0079]

The information on the size of the data to save is included in the signal corresponding to a data storage demand, and CPU41 compares the residue of the record section of a recording medium with the size of data at this time.

[0080]

On the other hand, in Step S84, when it is judged that preservation of data is possible, it progresses to Step S86 and preparations of preservation of data are made. For

example, the recording reproduction section 32 moves a recording position to the field to which record is permitted among all the record sections of videotape by performing rapid traverse and rewinding.

[0081]

And after preparation of preservation of data is completed, in Step S87, the network control section 31 outputs the signal which notifies completion of preservation preparation to the home gate way 1 via the network 8.

[0082]

And in Step S88 the network control section 31, In [ the network interface 44 receives the data transmitted via the network 8, and ] Step S89, When it judges whether all the data was received and it is judged that no data is received, it returns to Step S88 and the data transmitted to the next is received.

[0083]

On the other hand, when it is judged that all the data was received, it progresses to Step S90 and the network control section 31 makes the data which controlled the recording reproduction section 32 and was received, and its title write in videotape in Step S89.

[0084]

And after the writing of data is completed, in Step S91, the network control section 31 outputs the signal which reports that the writing of data was completed to the home gate way 1, and returns to Step S82.

[0085]

If the signal corresponding to a data storage demand as mentioned above is supplied from the home gate way 1, it is judged whether preservation of data is possible, and when preservation of data is possible, data will be transmitted and it will be written in a recording medium (videotape). And other processings are performed when the signal corresponding to a data storage demand is not supplied from the home gate way 1.

[0086]

It operates like [ the cassette tape recorder 4, MD recorder 5, and the DVD-RAM recorder 6 ] DVTR2.

[0087]

Next, with reference to the flow chart of drawing 11, operation of each device when reproducing the data saved DVTR2 by TV3 is explained in the data management system of drawing 1.

[0088]

First, in Step S101, the final controlling element 55 of TV3 is operated by the user, the program of the browser currently beforehand recorded on ROM42 of TV3 is started, and a browser picture is displayed on CRT53. And corresponding to operation by the user in the final controlling element 55 of TV3, a list of the data saved under the predetermined date is displayed on CRT53, as shown, for example in drawing 12.

[0089]

It may be made to use general-purpose browsers, such as "Internet Explorer" by Microsoft Corp., and Netscape Communications "Netscape Navigator", as a browser.

[0090]

At this time, according to the program of a browser, CPU41 of the network control section 31 of TV3, The home gate way 1 is accessed via the network 8, the management data according to date of the date selected among the management data according to date saved at the hard disk 24 of the home gate way 1 is read, and the picture corresponding to it is displayed on CRT53.

[0091]

For example, if the management data according to date on January 1, 1997 shown in drawing 9 is read, the picture shown in drawing 12 will be displayed on CRT53.

[0092]

And when the data to reproduce is chosen from the title of the data currently displayed on CRT53 by the user in Step S102, the network control section 31 of TV3, The signal corresponding to the reproduction request of selected data is outputted to the home gate way 1 via the network 8.

[0093]

In Step S103, CPU21 of the home gate way 1, The signal of this reproduction request is received via the network 8 and the network interface 27, With reference to the management data according to date saved at the hard disk 24, the apparatus holding selected data (for example, "Switzerland.jpg" of drawing 12) is investigated, and the signal which requires read-out of the data chosen as the apparatus (in the case of now DVTR2) is outputted.

[0094]

When that apparatus is in the state which cannot be operated at this time, the home gate way 1 supplies a predetermined signal to TV3, and it may be made to make it warn to a user.

[0095]

In Step S104, the network control section 31 of DVTR2 receives the signal, controls the recording reproduction section 32, makes selected data read from videotape, and is supplied to the home gate way 1 via the network 8.

[0096]

In Step S105, CPU21 of the home gate way 1, In [ receive the data transmitted via the network 8 via the network 8 and the network interface 27, and ] Step S106, When it judges whether the form of the data is a form refreshable at TV3 and it is judged that the form of the data is not a form refreshable at TV3, in Step S107, data is changed into a refreshable form by TV3.

[0097]

At this time, CPU21 judges the form of that data with reference to the extension of the saved data. For example, when an extension is ".bmp", it is judged that the data is bit map data (still picture information), When an extension is ".tif", it is judged that the data is the still picture information of TIFF (Tag Image File Format) form, When an extension is ".gif", it is judged that the data is the still picture information of GIF (Graphics Interchange Format) form.

[0098]

For example, in TV3, only the still picture information of JPEG form or GIF form changes the still picture information of other forms into the still picture information of JPEG form or GIF form CPU21, when it can display.

[0099]

On the other hand, when the form of the data is judged to be a refreshable form by TV3, Step S107 is skipped.

[0100]

And in Step S108, the home gate way 1 transmits selected data to TV3 via the network 8, and TV3 receives the data in Step S109.

[0101]

In Step S110, the network control section 31 of TV3 outputs the data to the drive circuit 52, and displays the picture corresponding to the data on CRT53.

[0102]

Data is chosen from a list of the data saved as mentioned above, and selected data is read from the apparatus which saves the data, and is reproduced.

[0103]

As mentioned above, in the data management system of drawing 1. While outputting the data (electrical household appliances and electrical equipment etc.) corresponding to a signal to the Records Department which distinguished the kind of signal supplied via the predetermined medium, and chose corresponding to the kind of signal, Since the management data showing the recording place of a signal is generated and management data was saved, while managing the data of various gestalten collectively and making the portability and flexibility of data good, the management state of data can be visualized.

[0104]

The apparatus of a remote place connected to the network can be chosen as a preservation place of data by connecting the home gate way 1 to a wide area network (for example, Internet). In that case, an above-mentioned link for example, by using "<A HREF="http://VTR1.xxx.co.jp/1996\_0902\_01.txt">", The data "1996\_0902\_01.txt" saved "VTR1" of xxx in Japan is manageable.

[0105]

It is not limited to the above-mentioned embodiment and this invention can be applied to other devices.

[Brief Description of the Drawings]

[0106]

[Drawing 1]It is a block diagram showing the example of composition of the data management system adapting this invention.

[Drawing 2]It is a block diagram showing the example of composition of the home gate way of drawing 1.

[Drawing 3]It is a block diagram showing the example of composition of the digital video recorder of drawing 1.

[Drawing 4]It is a block diagram showing the example of composition of the television receiver of drawing 1.

[Drawing 5]It is a flow chart explaining operation of a home gate way.

[Drawing 6]It is a flow chart explaining the details of processing of selection of the preservation destination of the data of drawing 5.

[Drawing 7]It is a flow chart explaining the details of processing of preservation of the data of drawing 5.

[Drawing 8]It is a figure showing an example of management data.

[Drawing 9]It is a figure showing an example of the management data according to date.

[Drawing 10]It is a flow chart explaining operation of a digital video recorder.

[Drawing 11]In the data management system of drawing 1, it is a flow chart explaining operation of each device when reproducing the data saved at the digital video recorder with a television receiver.

[Drawing 12]It is a figure showing an example of the list display of the title of the data saved.

[Description of Notations]

[0107]

1 A home gate way and 2 Digital video recorder (DVTR), 3 A television receiver (TV), Four cassette tape recorders and five MD recorders, 6 A DVD-RAM recorder and seven personal computers, Eight networks, 21 CPU, and 22. ROM, 23 RAM, and 24 [ Network interface ] A hard disk and 25 A communication circuit, 26 A/D

conversion circuits, and 27 A network interface, 31 network control sections, 41 CPU, 42 ROM, 43 RAM, and 44

[Claim(s)]

[Claim 1]

In a data processing method which processes output data outputted to apparatus of an output destination change,

A judgment step said output data judges it to be whether it is a refreshable form by apparatus of said output destination change based on a reproduction request by a user,

A converting step which changes said output data into a refreshable form by apparatus of said output destination change when said output data is not a refreshable form by apparatus of said output destination change,

A supply step which supplies output data changed into a refreshable form by apparatus of said output destination change to apparatus of said output destination change

\*\*\*\*\* -- a data processing method characterized by things.

[Claim 2]

It performs in a home gate way.

The data processing method according to claim 1 characterized by things.

[Claim 3]

Said home gate way has memorized management data of said output data described with a markup language.

The data processing method according to claim 2 characterized by things.

[Claim 4]

A request step which requires said output data memorized by apparatus other than apparatus of said output destination change based on said user's reproduction request and said management data,

A receiving step which receives said output data from said another apparatus

It contains in a pan,

Said judgment step judges whether it is form with said output data refreshable by apparatus of said output destination change received in said receiving step.

The data processing method according to claim 3 characterized by things.

[Claim 5]

Said another apparatus is connected to said home gate way via a wide area network.

The data processing method according to claim 4 characterized by things.

[Claim 6]

In a data processing device which processes output data outputted to apparatus of an output destination change,

A decision means said output data judges it to be whether it is a refreshable form by apparatus of said output destination change based on a reproduction request by a user,

A conversion method which changes said output data into a refreshable form by apparatus of said output destination change when said output data is not a refreshable form by apparatus of said output destination change,

A feeding means which supplies output data changed into a refreshable form by apparatus of said output destination change to apparatus of said output destination change

\*\*\*\*\* -- a data processing device characterized by things.

[Claim 7]

It is a home gate way.

The data processing device according to claim 6 characterized by things.

[Claim 8]



Said home gate way has memorized management data of said output data described with a markup language.

The data processing device according to claim 7 characterized by things.

[Claim 9]

A request means which requires said output data memorized by apparatus other than apparatus of said output destination change based on said user's reproduction request and said management data,

A reception means which receives said output data from said another apparatus

It contains in a pan,

Said decision means judges whether it is form with said output data refreshable by apparatus of said output destination change received in said reception means.

The data processing device according to claim 8 characterized by things.

[Claim 10]

Said another apparatus is connected to said home gate way via a wide area network.

The data processing device according to claim 9 characterized by things.

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-192659

(P2004-192659A)

(43) 公開日 平成16年7月8日(2004.7.8)

(51) Int. Cl.<sup>7</sup>  
G06F 12/00

F I  
G06F 12/00 511C  
G06F 12/00 520E

テーマコード(参考)  
5B082

審査請求 有 請求項の数 10 ○ L (全 16 頁)

(21) 出願番号 特願2004-53432 (P2004-53432)  
(22) 出願日 平成16年2月27日(2004.2.27)  
(62) 分割の表示 特願平9-77283の分割  
原出願日 平成9年3月28日(1997.3.28)

(71) 出願人 000002185  
ソニー株式会社  
東京都品川区北品川6丁目7番35号  
(74) 代理人 100082131  
弁理士 楠本 義雄  
(72) 発明者 千原 秀一  
東京都品川区北品川6丁目7番35号 ソ  
ニー株式会社内  
Fターム(参考) 5B082 AA13 EA09 HA05

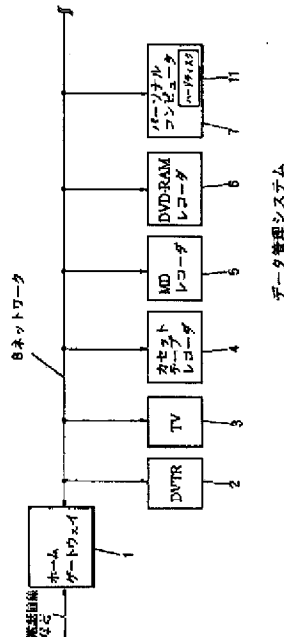
(54) 【発明の名称】 データ処理方法およびデータ処理装置

(57) 【要約】

【課題】 データの形式を、再生可能な形式に変換する

【解決手段】 ホームゲートウェイは、ユーザによる再生要求に基づいて、出力データが、出力先の機器で再生可能な形式か否かを判断する。また、ホームゲートウェイは、出力データが、出力先の機器で再生可能な形式でない場合、その出力データを、出力先の機器で再生可能な形式に変換し、出力先の機器に供給する。本発明は、例えば、ホームゲートウェイに適用することができる。

【選択図】 図1



## 【特許請求の範囲】

## 【請求項1】

出力先の機器に出力する出力データを処理するデータ処理方法において、  
 ユーザによる再生要求に基づき、前記出力データが、前記出力先の機器で再生可能な形式か否かを判断する判断ステップと、  
 前記出力データが、前記出力先の機器で再生可能な形式でない場合、前記出力データを、前記出力先の機器で再生可能な形式に変換する変換ステップと、  
 前記出力先の機器で再生可能な形式に変換された出力データを、前記出力先の機器に供給する供給ステップと  
 を含むことを特徴とするデータ処理方法。

10

## 【請求項2】

ホームゲートウェイにおいて実行される  
 ことを特徴とする請求項1に記載のデータ処理方法。

## 【請求項3】

前記ホームゲートウェイは、マークアップランゲージで記述された、前記出力データの管理データを記憶している  
 ことを特徴とする請求項2に記載のデータ処理方法。

## 【請求項4】

前記出力先の機器とは別の機器に記憶された前記出力データを、前記ユーザの再生要求および前記管理データに基づき要求する要求ステップと、  
 前記別の機器から、前記出力データを受信する受信ステップと  
 をさらに含み、

20

前記判断ステップは、前記受信ステップにおいて受信された前記出力データが、前記出力先の機器で再生可能な形式か否かを判断する  
 ことを特徴とする請求項3に記載のデータ処理方法。

## 【請求項5】

前記別の機器は、広域ネットワークを介して、前記ホームゲートウェイに接続されている  
 ことを特徴とする請求項4に記載のデータ処理方法。

## 【請求項6】

出力先の機器に出力する出力データを処理するデータ処理装置において、  
 ユーザによる再生要求に基づき、前記出力データが、前記出力先の機器で再生可能な形式か否かを判断する判断手段と、  
 前記出力データが、前記出力先の機器で再生可能な形式でない場合、前記出力データを、前記出力先の機器で再生可能な形式に変換する変換手段と、  
 前記出力先の機器で再生可能な形式に変換された出力データを、前記出力先の機器に供給する供給手段と  
 を含むことを特徴とするデータ処理装置。

30

## 【請求項7】

ホームゲートウェイである  
 ことを特徴とする請求項6に記載のデータ処理装置。

40

## 【請求項8】

前記ホームゲートウェイは、マークアップランゲージで記述された、前記出力データの管理データを記憶している  
 ことを特徴とする請求項7に記載のデータ処理装置。

## 【請求項9】

前記出力先の機器とは別の機器に記憶された前記出力データを、前記ユーザの再生要求および前記管理データに基づき要求する要求手段と、  
 前記別の機器から、前記出力データを受信する受信手段と  
 をさらに含み、

50

前記判断手段は、前記受信手段において受信された前記出力データが、前記出力先の機器で再生可能な形式か否かを判断する

ことを特徴とする請求項8に記載のデータ処理装置。

【請求項10】

前記別の機器は、広域ネットワークを介して、前記ホームゲートウェイに接続されている

ことを特徴とする請求項9に記載のデータ処理装置。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、データ処理方法およびデータ処理装置に関し、特に、データの形式を、再生可能な形式に変換するデータ処理方法およびデータ処理装置に関する。

【背景技術】

【0002】

半導体技術の進歩に伴い、各種情報が、所定の形式のデータや信号として、各種媒体を介して提供されている。例えば、コンピュータネットワークを介して、様々なデジタルデータの送受信が行われている。また、このようなデジタルデータは、コンピュータに接続または内蔵されているハードディスクに保存されることが多い。

【0003】

その一方で、音楽データなどを供給する場合、例えばMD（商標）（ミニディスク）などの携帯可能な記録媒体が利用されることが多い。

【0004】

なお、所謂家電機器の中には、例えばMDにデータを記録するMDレコーダのように、所定の形式のデータや信号を所定の媒体に記録するものがある。

【0005】

そのような家電機器（および、それに対応する記録媒体）は、機器ごとに異なるデータの管理形態を採用しているため、データの可搬性や汎用性に欠けるとともに、データの管理が機器ごとに行われているため、すべてのデータの管理状況を可視化することが困難である。

【発明の開示】

【発明が解決しようとする課題】

【0006】

ところで、例えば、テレビジョン受像機（TV）が接続されたホームゲートウェイにおいて、データが、TVで再生可能な形式か否かを判断し、TVで再生可能な形式でない場合には、TVで再生可能な形式に変換し、その変換後のデータをTVに供給することができれば便利である。

【0007】

本発明は、そのような状況に鑑みてなされたもので、データの形式を、再生可能な形式に変換するものである。

【課題を解決するための手段】

【0008】

本発明のデータ処理方法は、ユーザによる再生要求に基づき、出力データが、出力先の機器で再生可能な形式か否かを判断する判断ステップと、出力データが、出力先の機器で再生可能な形式でない場合、出力データを、出力先の機器で再生可能な形式に変換する変換ステップと、出力先の機器で再生可能な形式に変換された出力データを、出力先の機器に供給する供給ステップとを含むことを特徴とする。

【0009】

データ処理方法は、ホームゲートウェイにおいて実行されるようにすることができる。

【0010】

ホームゲートウェイには、マークアップランゲージで記述された、出力データの管理デ

10

20

30

40

50

ータが記憶されるようにすることができる。

【0011】

データ処理方法には、出力先の機器とは別の機器に記憶された出力データを、ユーザの再生要求および管理データに基づき要求する要求ステップと、別の機器から、出力データを受信する受信ステップとをさらに設けるようにすることができ、判断ステップには、受信ステップにおいて受信された出力データが、出力先の機器で再生可能な形式か否かを判断させるようにすることができる。

【0012】

別の機器は、広域ネットワークを介して、ホームゲートウェイに接続されるようにすることができる。

10

【0013】

本発明のデータ処理装置は、ユーザによる再生要求に基づき、出力データが、出力先の機器で再生可能な形式か否かを判断する判断手段と、出力データが、出力先の機器で再生可能な形式でない場合、出力データを、出力先の機器で再生可能な形式に変換する変換手段と、出力先の機器で再生可能な形式に変換された出力データを、出力先の機器に供給する供給手段とを含むことを特徴とする。

【0014】

データ処理装置は、ホームゲートウェイとすることができる。

【0015】

ホームゲートウェイには、マークアップランゲージで記述された、出力データの管理データが記憶されるようにすることができる。

20

【0016】

データ処理装置には、出力先の機器とは別の機器に記憶された出力データを、ユーザの再生要求および管理データに基づき要求する要求手段と、別の機器から、出力データを受信する受信手段とをさらに設けるようにすることができ、判断手段には、受信手段において受信された出力データが、出力先の機器で再生可能な形式か否かを判断させるようにすることができる。

【0017】

別の機器は、広域ネットワークを介して、ホームゲートウェイに接続されるようにすることができる。

30

【0018】

本発明のデータ処理方法およびデータ処理装置においては、ユーザによる再生要求に基づき、出力データが、出力先の機器で再生可能な形式か否かが判断され、出力データが、出力先の機器で再生可能な形式でない場合、出力データが、出力先の機器で再生可能な形式に変換される。また、出力先の機器で再生可能な形式に変換された出力データが、出力先の機器に供給される。

【発明の効果】

【0019】

本発明のデータ処理方法およびデータ処理装置によれば、データの形式を、再生可能な形式に変換することができる。

40

【発明を実施するための最良の形態】

【0020】

以下に本発明の最良の形態を説明するが、請求項に記載の構成要件と、発明の実施の形態における具体例との対応関係を例示すると次のようになる。この記載は、請求項に記載されている発明をサポートする具体例が、発明の実施の形態に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、構成要件に対応するものとして、ここには記載されていない具体例があったとしても、そのことは、その具体例が、その構成要件に対応するものではないことを意味するものではない。逆に、具体例が構成要件に対応するものとしてここに記載されていたとしても、そのことは、その具体例が、その構成要件以外の構成要件には対応しないものであることを意味するも

50

のみもない。

【0021】

さらに、この記載は、発明の実施の形態に記載されている具体例に対応する発明が、請求項にすべて記載されていることを意味するものではない。換言すれば、この記載は、発明の実施の形態に記載されている具体例に対応する発明であって、この出願の請求項には記載されていない発明の存在、すなわち、将来、分割されたり、補正により出現し、追加される発明の存在を否定するものではない。

【0022】

請求項1に記載のデータ処理方法は、

出力先の機器に出力する出力データを処理するデータ処理方法において、

ユーザによる再生要求に基づき、前記出力データが、前記出力先の機器で再生可能な形式か否かを判断する判断ステップ（例えば、図11のステップS106の処理）と、

前記出力データが、前記出力先の機器で再生可能な形式でない場合、前記出力データを、前記出力先の機器で再生可能な形式に変換する変換ステップ（例えば、図11のステップS107の処理）と、

前記出力先の機器で再生可能な形式に変換された出力データを、前記出力先の機器に供給する供給ステップ（例えば、図11のステップS108の処理）と

を含むことを特徴とする。

10

【0023】

請求項4に記載のデータ処理方法は、

前記出力先の機器とは別の機器に記憶された前記出力データを、前記ユーザの再生要求および前記管理データに基づき要求する要求ステップ（例えば、図11のステップS103の処理）と、

前記別の機器から、前記出力データを受信する受信ステップ（例えば、図11のステップS105の処理）と

をさらに含み、

前記判断ステップは、前記受信ステップにおいて受信された前記出力データが、前記出力先の機器で再生可能な形式か否かを判断すること

を特徴とする。

20

【0024】

請求項6に記載のデータ処理装置は、

出力先の機器に出力する出力データを処理するデータ処理装置において、

ユーザによる再生要求に基づき、前記出力データが、前記出力先の機器で再生可能な形式か否かを判断する判断手段（例えば、図11のステップS106の処理を実行するCPU21）と、

前記出力データが、前記出力先の機器で再生可能な形式でない場合、前記出力データを、前記出力先の機器で再生可能な形式に変換する変換手段（例えば、図11のステップS107の処理を実行するCPU21）と、

前記出力先の機器で再生可能な形式に変換された出力データを、前記出力先の機器に供給する供給手段（例えば、図11のステップS108の処理を実行するCPU21）と

を含むことを特徴とする。

30

40

【0025】

請求項9に記載のデータ処理装置は、

前記出力先の機器とは別の機器に記憶された前記出力データを、前記ユーザの再生要求および前記管理データに基づき要求する要求手段（例えば、図11のステップS103の処理を実行するCPU21）と、

前記別の機器から、前記出力データを受信する受信手段（例えば、図2のネットワークインタフェース27）と

をさらに含み、

前記判断手段は、前記受信手段において受信された前記出力データが、前記出力先の機

50

器で再生可能な形式が否かを判断すること  
ことを特徴とする。

【0026】

図1は、本発明を応用したデータ管理システムの一構成例を示している。このデータ管理システムは、例えば家庭やオフィスに配置され、電話回線などの公衆回線を介して供給される情報をホームゲートウェイ1で受け取り、その情報に対応するデータ（テキストデータ、動画データ、静止画像データ、音声データなど）を、記録部を有する所謂家電機器に保存するとともに、そのデータを管理する。

【0027】

このデータ管理システムにおいては、所定の規格（例えば、IEEE1394 High Performance Serial Bus規格やイーサネット(R)）のネットワーク8に、データの受信および管理を行うホームゲートウェイ1、再生部としてのテレビジョン受像機(TV)3、記録部としてのデジタルビデオテープレコーダ(DVTR)2、カセットテープレコーダ4、MDレコーダ5、DVD(Digital Versatile Disc)-RAMレコーダ6、ハードディスク11を内蔵するパーソナルコンピュータ7などが接続されている。

【0028】

図2は、ホームゲートウェイ1の構成例を示している。ホームゲートウェイ1においては、CPU(Central Processing Unit)21は、ROM(Read Only Memory)22に記録されているプログラムに従って各種処理を行うようになされている。

【0029】

ROM22は、データの受信や管理に対応するプログラムを保持している。

【0030】

RAM(Random Access Memory)23は、CPU21により各種処理が行われている間、一時的に、データやプログラムを記憶するようになされている。

【0031】

ハードディスク24は、受信した信号に対応してCPU21により生成された管理データを適宜保持するようになされている。なお、管理データは、ハイパーテキストマークアップランゲージ(HTML:Hyper Text Markup Language)で記述されている。

【0032】

通信回路25は、例えば電話回線などの公衆の伝送媒体に接続されており、その伝送媒体を介して各種データに対応する信号を受信し、復調した後、受信した信号がアナログ信号である場合、その信号をA/D変換回路26に出力し、デジタル信号である場合、その信号(データ)をCPU21に出力するようになされている。

【0033】

A/D変換回路26は、通信回路25より供給されたアナログ信号をデジタル信号に変換し、その信号(データ)をCPU21に出力するようになされている。

【0034】

ネットワークインタフェース27は、ネットワーク8に接続され、所定の規格に従ってデータの送受信を行うようになされている。

【0035】

図3は、DVTR2の構成例を示している。ネットワーク制御部31は、ホームゲートウェイ1からネットワーク8を介して供給されたデータを受信して、記録再生部32に出力する他、操作部33においてユーザにより入力された指示に対応する信号を、ネットワーク8を介してホームゲートウェイ1に供給するようになされている。

【0036】

ネットワーク制御部31においては、CPU41は、ROM42に記録されているプログラムに従って各種処理を行うようになされている。なお、ROM42には、上述の処理に対応するプログラムが保持されている。そして、RAM43は、CPU41により各種処理が行われている間、一時的に、データやプログラムを記憶するようになされている。さらに、ネットワークインタフェース44は、ネットワーク8に接続され、所定の規格に

従ってデータの送受信を行うようになされている。

【0037】

記録再生部32は、操作部38からの信号またはCPU41からの信号に対応して、記録媒体であるビデオテープ（図示せず）にデータを記録するか、あるいは、ビデオテープに記録されているデータを読み出すようになされている。

【0038】

図4は、TV3の構成例を示している。ネットワーク制御部31は、図2のものと同様に、ホームゲートウェイ1よりネットワーク8を介して供給されたデータを受信して駆動回路52に出力する他、操作部55においてユーザにより入力された指示に対応する信号を、ネットワーク8を介してホームゲートウェイ1に供給するようになされている。

10

【0039】

チューナ51は、操作部55より供給される信号に対応する設定（チャンネルなど）で、図示せぬアンテナを介して例えばテレビジョン放送信号を受信し、その信号に対応する画像信号と音声信号を駆動回路52に出力するようになされている。

【0040】

駆動回路52は、ネットワーク制御部31より供給される画像データと音声データを、内蔵するD/A変換部61でアナログ画像信号またはアナログ音声信号に変換し、アナログ画像信号に対応する画像をCRT58に表示させるとともに、アナログ音声信号に対応する音声をスピーカ54に出力させる他、チューナ51より供給された画像信号に対応する画像をCRT58に表示させるとともに、チューナ51より供給された音声信号に対応する音声をスピーカ54に出力させるようになされている。

20

【0041】

図1のカセットテープレコーダ4、MDレコーダ5、および、DVD-RAMレコーダ6は、記録媒体（カセットテープ（磁気テープ）、MD、または、DVD-RAM）に対してデータの記録または再生を行う記録再生部の他、DVTR2、TV3と同様にネットワーク制御部31を有している。

【0042】

パーソナルコンピュータ7は、ネットワーク8に対応するネットワークインタフェース（図示せず）を内蔵し、各種処理を行う他、ネットワーク8を介してデータの送受信を行うようになされている。

30

【0043】

次に、図5乃至図8のフローチャートを参照して、ホームゲートウェイ1の動作について説明する。

【0044】

最初にステップS1において（起動時において）、ホームゲートウェイ1のCPU21は、ホームゲートウェイ1の各回路の初期化処理を行う。

【0045】

次に、ステップS2において、通信回路25が信号を受信したか否かが判断され、通信回路25が信号を受信していないと判断された場合、ステップS3において、他の処理、例えばネットワーク8を介して供給される各種要求の処理が行われ、その後、ステップS2に戻る。

40

【0046】

このように、通信回路25が信号を受信していないときには、他の処理が行われている。

【0047】

そして、ステップS2において、通信回路25が信号を受信したと判断された場合、ステップS4に進み、CPU21は、受信した信号の種類や量に対応して、ネットワーク8に接続されている機器から、データの保存先になる機器を選択する（後述）。

【0048】

次に、ステップS5において、CPU21は、選択した機器にネットワーク8を介して

50



アクセスして、受信したデータを保存することができると判断し、保存可能である場合、ステップS7において、そのデータに対応する管理データをHTMLで作成した後、受信したデータをネットワークインタフェース27に出力する。そして、ネットワークインタフェース27は、そのデータを、ネットワーク8を介して、選択された機器に供給し、保存させる(後述)。このようにデータが保存された後、ステップS2に戻る。なお、管理データは、ホームゲートウェイ1のハードディスク24に保存される。

【0049】

一方、ステップS5において、選択した機器に、受信したデータを保存することができないと判断された場合、ステップS6において、CPU21は、保存することができないデータ(信号)に関する情報(例えば、データのタイトルや受信時刻など)を所定のファイルとしてハードディスク24に保存しておく。このような保存不可能時の処理を行った後、ステップS2に戻る。

【0050】

このようにして、受信したデータが、そのデータの大きさと種類に対応して選択された機器に保存されるとともに、そのデータに対応する管理データが、ホームゲートウェイ1のハードディスク24に保存される。保存したデータは、ホームゲートウェイ1により一括して管理されるので、保存したデータの再生や再利用が簡単になる。

【0051】

次に、図6のフローチャートを参照して、図5のステップS4における、データを保存する機器を選択する処理の詳細について説明する。

【0052】

まず、ホームゲートウェイ1のCPU21は、ステップS21において、ネットワークインタフェース27を制御して、ネットワーク8に接続されている機器の種類と数を調べ、ステップS22において、その機器のうち、使用可能な機器(即ち、記録部または記録媒体を有するものであり、電源がオンになっているもの)を調べる。

【0053】

次に、CPU21は、ステップS23において、保存するデータの大きさを調べ、ステップS24において、保存するデータの大きさと種類に対応して、使用可能な機器から、そのデータを保存する機器の候補を選択する。

【0054】

さらに、CPU21は、再生時におけるデータの転送速度や、所定の記録容量に対する記録媒体のコストに対応して、最適な機器の候補を選択する。

【0055】

そして、CPU21は、ネットワークインタフェース27を制御して、ネットワーク8を介して、選択した機器のネットワーク制御部81に、選択した機器の記録容量の残量と、その機器(記録媒体)への書き込みが許可されているかを調べさせ、ステップS25において、選択した機器の記録容量の残量が、保存するデータの大きさ以上であるかを判断し、記録容量の残量が、保存するデータの大きさより小さいと判断した場合、ステップS26に進み、使用可能な他の機器があるかを判断する。

【0056】

ステップS26において、使用可能な他の機器があると判断された場合、ステップS28において、それらの機器から1つの機器が選択された後、ステップS25に戻る。

【0057】

一方、ステップS26において、使用可能な他の機器がないと判断された場合、データの保存が不可能であると判断され、ステップS5(図5)に進む。

【0058】

また、ステップS25において、選択した機器の記録容量の残量が、保存するデータの大きさ以上であると判断された場合、ステップS29に進む。そして、CPU21は、選択した機器(記録媒体)への書き込みが許可されているかを判断し、選択した機器(記録媒体)への書き込みが許可されていないと判断した場合、ステップS26に進み、上

述のように、ステップ826乃至ステップ828における処理を行う。

【0059】

一方、ステップ829において、選択した機器（記録媒体）への書き込みが許可されていると判断された場合、ステップ830に進み、その機器が、データの保存先に指定される。

【0060】

このようにして、データの種類や大きさなどに対応して、そのデータを保存する機器が選択される。

【0061】

次に、図7のフローチャートを参照して、図5のステップ87における、データを保存する処理の詳細について説明する。

【0062】

まず、ステップ841において、通信回路25により受信された信号がデジタル信号であるか否かが判断され、受信された信号がデジタル信号ではない（アナログ信号である）と判断された場合、ステップ842において、A/D変換回路26により、そのアナログ信号はデジタル信号に変換される。なお、受信された信号がデジタル信号であると判断された場合、ステップ842はスキップされる。

【0063】

そして、ステップ843において、CPU21は、そのデジタル信号（データ）にファイル名が付加されているか否かを判断し、即ち、受信したデータにファイル名が含まれているか否かを判断し、そのデータにファイル名が付加されていないと判断した場合、ステップ844において、所定の方式（例えば、受信した日付を利用した方式）でファイル名をそのデータに付加する。例えば1996年9月1日に受信した第2番目のデータには、「1996\*0901\*02.xxx」というファイル名が付加される。このとき、拡張子「.xxx」は、データの種類に対応して設定される。

【0064】

なお、データにファイル名が付加されている場合、ステップ844はスキップされる。

【0065】

次に、ステップ845において、CPU21は、データのタイトル（ファイル名）を有するHTMLの所定のヘッダと、データのファイル名と記録場所に対応するHTMLのリンクで、例えば図8に示す管理データを生成する。

【0066】

なお、図8に示す管理データ（HTMLで記述されたもの）は、タイトル（ファイル名）が「1997\*0101\*01\*switzerland.jp9」であるJPEG（Joint Photographic Experts Group）方式で圧縮された画像データで、記録場所が「VTR1」であるものに対する管理データである。拡張子「.jp9」は、そのデータがJPEG画像データであることを表している。即ち、図8に示す管理データにおいては、リンク「<A HREF="http://VTR1/1997\*0101\*01\*switzerland.jp9">」により、JPEG画像データ「1997\*0101\*01\*switzerland.jp9」の保存場所が保存される。なお、「VTR1」は、例えばDVT R 2を指すように予め設定される。

【0067】

さらに、ステップ845において、CPU21は、各日付で保存したデータを一括して管理する例えば図9に示す日付別管理データを作成する。図9の日付別管理データにおいては、1997年1月1日に保存された6つのデータが登録されている。なお、「md1」はMDレコーダ5を指し、「dvd1」はDVD-RAMレコーダ6を指し、「cas1」は、カセットテープレコーダ4を指し、「vtr2」はネットワーク8に接続されている図示せぬ第2のDVT Rを指すように予め設定されている。

【0068】

そして、ステップ846において、ホームゲートウェイ1のCPU21は、ステップ845で生成した管理データおよび日付別管理データをハードディスク24に保存する。

## 【0069】

次に、ステップ847において、CPU21は、ネットワークインタフェース27およびネットワーク8を介して、ステップ84（図5）で選択した機器に、データの保存を要求する信号を供給する。

## 【0070】

そして、ステップ848において、CPU21は、その機器から保存準備の完了を通知する信号がネットワーク8を介して供給されるまで待機する。

## 【0071】

保存準備の完了を通知する信号が供給されると、ステップ849に進み、ホームゲートウェイ1のCPU21は、ネットワークインタフェース27およびネットワーク8を介して、選択した機器へのデータの送信を開始し、ステップ850において、すべてのデータを受信したことを通知する信号をその機器から受け取るまで、データの通信を順次行う。

10

## 【0072】

そして、ステップ850において、すべてのデータを受信したことを通知する信号が受信された場合、CPU21は、データ保存の処理を終了し、ステップ82（図5）に戻る。

## 【0073】

このようにして、受信したデータを保存するときにおいては、そのデータに対応する管理データが生成され、ホームゲートウェイ1のハードディスク24に保存された後、受信したデータが、ホームゲートウェイ1から、選択された機器に転送される。

20

## 【0074】

次に、図10のフローチャートを参照して、DVTR2の動作について説明する。

## 【0075】

最初にステップ881において（起動時において）、DVTR2のCPU41は、DVTR2の各回路の初期化処理を行う。

## 【0076】

次に、ステップ882において、ネットワーク制御部81のCPU41は、ホームゲートウェイ（HGW）1からの、データ保存要求に対応する信号を受信したか否かを判断し、受信していないと判断した場合、ステップ883において、他の処理、例えば操作部88におけるユーザの操作に対する処理を行い、その後、ステップ882に戻る。

30

## 【0077】

このように、ホームゲートウェイ1からデータ保存要求に対応する信号を受信していないときには、他の処理が行われている。

## 【0078】

そして、ステップ882において、データ保存要求に対応する信号を受信したと判断された場合、ステップ884に進み、ネットワーク制御部81のCPU41は、記録媒体（ビデオテープ）にデータを保存することが可能であるか否かを判断し、データの保存が可能ではないと判断した場合、ステップ885において、データの保存が可能ではないことを表す信号を、ネットワーク8を介してホームゲートウェイ1に出力する。そして、ステップ882に戻る。

40

## 【0079】

データ保存要求に対応する信号には、保存するデータの大きさの情報が含まれており、このとき、CPU41は、記録媒体の記録領域の残量とデータの大きさを比較する。

## 【0080】

一方、ステップ884において、データの保存が可能であると判断された場合、ステップ886に進み、データの保存の準備が行われる。例えば、記録再生部82は、早送りや巻き戻しを行うことにより、ビデオテープの全記録領域のうち、記録が許可されている領域に、記録位置を移動させる。

## 【0081】

そして、データの保存の準備が完了した後、ステップ887において、ネットワーク制

50

制御部 31 は、保存準備の完了を通知する信号を、ネットワーク 8 を介してホームゲートウェイ 1 に出力する。

【0082】

そして、ステップ 888 において、ネットワーク制御部 31 は、ネットワーク 8 を介して伝送されてくるデータをネットワークインタフェース 44 で受信し、ステップ 889 において、すべてのデータを受信したか否かを判断し、すべてのデータを受信していないと判断した場合、ステップ 888 に戻り、次に伝送されてくるデータを受信する。

【0083】

一方、ステップ 889 において、すべてのデータを受信したと判断された場合、ステップ 890 に進み、ネットワーク制御部 31 は、記録再生部 82 を制御して、受信したデータおよびそのタイトルをビデオテープに書き込ませる。 10

【0084】

そして、データの書き込みが完了した後、ステップ 891 において、ネットワーク制御部 31 は、データの書き込みが完了したことを通知する信号を、ホームゲートウェイ 1 に出力し、ステップ 882 に戻る。

【0085】

以上のようにして、ホームゲートウェイ 1 からデータ保存要求に対応する信号が供給されると、データの保存が可能であるか否かが判断され、データの保存が可能である場合、データが転送され、記録媒体（ビデオテープ）に書き込まれる。そして、ホームゲートウェイ 1 からデータ保存要求に対応する信号が供給されていない場合においては、その他の 20 処理が行われる。

【0086】

なお、カセットテープレコーダ 4、MDレコーダ 5、および、DVD-RAMレコーダ 6 も、DVT R 2 と同様に動作する。

【0087】

次に、図 11 のフローチャートを参照して、図 1 のデータ管理システムにおいて、DVT R 2 に保存されているデータを TV 3 で再生するときの各装置の動作について説明する。

【0088】

最初に、ステップ 8101 において、ユーザにより TV 3 の操作部 55 が操作され、予め TV 3 の ROM 42 に記録されているブラウザのプログラムが起動され、ブラウザ画面が CRT 53 に表示される。そして、TV 3 の操作部 55 におけるユーザによる操作に対応して、所定の日付で保存されているデータの一覧が、例えば図 12 に示すように CRT 53 に表示される。 30

【0089】

なお、ブラウザとして、マイクロソフト社製の「Internet Explorer」やネットスケープ社製の「Netscape Navigator」などの汎用のブラウザを使用するようにしてもよい。

【0090】

このとき、ブラウザのプログラムに従って、TV 3 のネットワーク制御部 31 の CPU 41 が、ネットワーク 8 を介してホームゲートウェイ 1 にアクセスし、ホームゲートウェイ 1 のハードディスク 24 に保存されている日付別管理データのうち、選択された日付の日付別管理データを読み出し、それに対応する画像を CRT 53 に表示させる。 40

【0091】

例えば、図 9 に示す 1997 年 1 月 1 日の日付別管理データが読み出されると、CRT 53 には、図 12 に示す画像が表示される。

【0092】

そして、ステップ 8102 において、ユーザにより、CRT 53 に表示されているデータのタイトルから、再生するデータが選択されると、TV 3 のネットワーク制御部 31 は、選択されたデータの再生要求に対応する信号をホームゲートウェイ 1 に、ネットワーク 8 を介して出力する。 50

## 【0093】

ステップS108において、ホームゲートウェイ1のCPU21は、この再生要求の信号を、ネットワーク8およびネットワークインタフェース27を介して受け取り、ハードディスク24に保存されている日付別管理データを参照し、選択されたデータ（例えば、図12の「Switzerland.jpg」）を保持している機器を調べ、その機器（今の場合、DVT R2）に、選択されたデータの読み出しを要求する信号を出力する。

## 【0094】

なお、このとき、その機器が動作不能の状態である場合、ホームゲートウェイ1が、TV8に所定の信号を供給し、ユーザに対して警告させるようにしてもよい。

## 【0095】

ステップS104において、DVT R2のネットワーク制御部31は、その信号を受け取り、記録再生部32を制御して、選択されたデータをビデオテープから読み出させ、ネットワーク8を介してホームゲートウェイ1に供給する。

## 【0096】

ステップS105において、ホームゲートウェイ1のCPU21は、ネットワーク8を介して伝送されてくるデータを、ネットワーク8およびネットワークインタフェース27を介して受け取り、ステップS106において、そのデータの形式が、TV8で再生可能な形式であるか否かを判断し、そのデータの形式が、TV8で再生可能な形式ではないと判断した場合、ステップS107において、データを、TV8で再生可能な形式に変換する。

## 【0097】

このとき、CPU21は、保存されたデータの拡張子を参照して、そのデータの形式を判断する。例えば、拡張子が「.bmp」である場合、そのデータはビットマップデータ（静止画像データ）であると判断され、拡張子が「.tif」である場合、そのデータはTIFF（Tag Image File Format）形式の静止画像データであると判断され、拡張子が「.gif」である場合、そのデータはGIF（Graphics Interchange Format）形式の静止画像データであると判断される。

## 【0098】

例えば、JPEG形式またはGIF形式の静止画像データだけが、TV8において表示可能である場合、CPU21は、他の形式の静止画像データを、JPEG形式またはGIF形式の静止画像データに変換する。

## 【0099】

一方、そのデータの形式が、TV8で再生可能な形式であると判断された場合、ステップS107はスキップされる。

## 【0100】

そして、ステップS108において、ホームゲートウェイ1は、選択されたデータを、ネットワーク8を介してTV8に転送し、ステップS109において、TV8は、そのデータを受信する。

## 【0101】

TV8のネットワーク制御部31は、ステップS110において、そのデータを駆動回路52に出力し、そのデータに対応する画像をCRT53に表示させる。

## 【0102】

以上のようにして、保存されているデータの一覧からデータが選択され、選択されたデータが、そのデータを保存している機器から読み出され、再生される。

## 【0103】

以上のように、図1のデータ管理システムでは、所定の媒体を介して供給された信号の種類を判別し、信号の種類に対応して選択した記録部（家電機器など）に、信号に対応するデータを出力するとともに、信号の記録場所を表す管理データを生成し、管理データを保存するようにしたので、様々な形態のデータを一括して管理し、データの可搬性や汎用性を良好にするとともに、データの管理状況を可視化することができる。

10

20

30

40

50

## 【0104】

なお、ホームゲートウェイを広域ネットワーク（例えばインターネット）に接続することにより、そのネットワークに接続されている遠隔地の機器をデータの保存場所として選択することができる。その場合、上述のリンクを例えば「<A HREF="http://VTR1.xxx.co.jp/1996\*0902\*01.txt">」にすることにより、日本国内の×××社の「VTR1」に保存しているデータ「1996\*0902\*01.txt」を管理することができる。

## 【0105】

なお、本発明は、上記実施の形態に限定されるものではなく、他の装置にも応用することが可能である。

## 【図面の簡単な説明】

10

## 【0106】

【図1】本発明を応用したデータ管理システムの構成例を示すブロック図である。

【図2】図1のホームゲートウェイの構成例を示すブロック図である。

【図3】図1のデジタルビデオテープレコーダの構成例を示すブロック図である。

【図4】図1のテレビジョン受像機の構成例を示すブロック図である。

【図5】ホームゲートウェイの動作を説明するフローチャートである。

【図6】図5のデータの保存先の選択の処理の詳細を説明するフローチャートである。

【図7】図5のデータの保存の処理の詳細を説明するフローチャートである。

【図8】管理データの一例を示す図である。

【図9】日付別管理データの一例を示す図である。

20

【図10】デジタルビデオテープレコーダの動作を説明するフローチャートである。

【図11】図1のデータ管理システムにおいて、デジタルビデオテープレコーダに保存されているデータをテレビジョン受像機で再生するときの各装置の動作を説明するフローチャートである。

【図12】保存されているデータのタイトルの一覧表示の一例を示す図である。

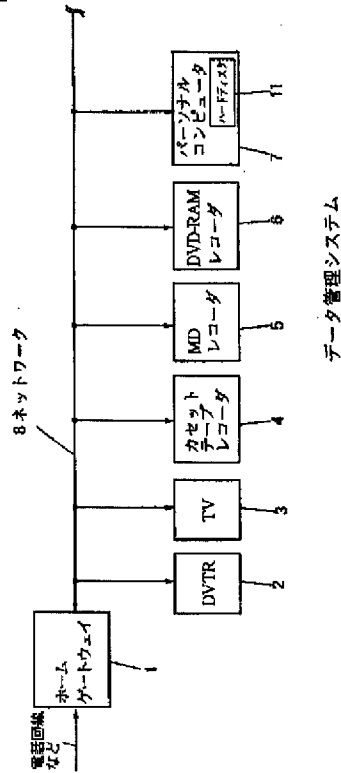
## 【符号の説明】

## 【0107】

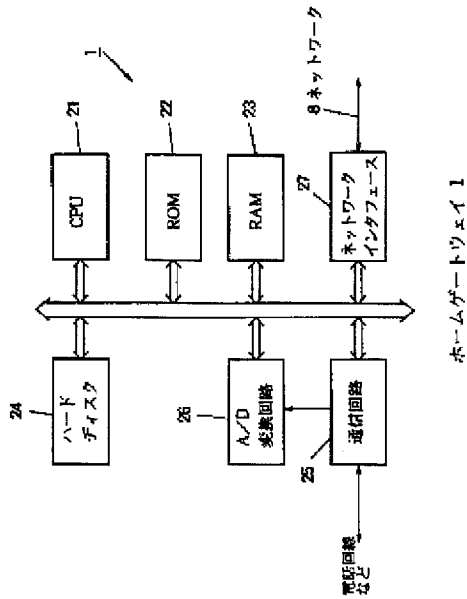
1 ホームゲートウェイ、 2 デジタルビデオテープレコーダ（DVTR）、 3  
テレビジョン受像機（TV）、 4 カセットテープレコーダ、 5 ミニディスクレ  
コーダ、 6 DVD-RAMレコーダ、 7 パーソナルコンピュータ、 8 ネットワ  
ーク、 21 CPU、 22 ROM、 23 RAM、 24 ハードディスク、  
25 通信回路、 26 A/D変換回路、 27 ネットワークインタフェース、 3  
1 ネットワーク制御部、 41 CPU、 42 ROM、 43 RAM、 44  
ネットワークインタフェース

80

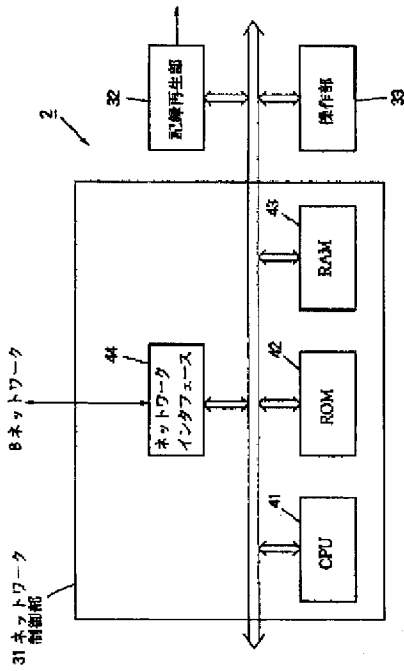
【図1】



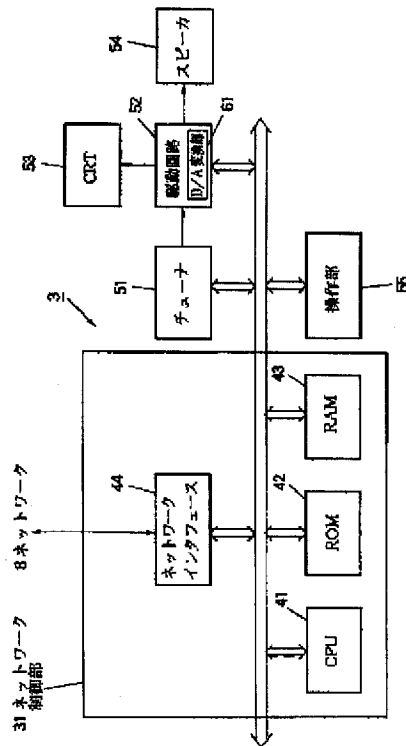
【図2】



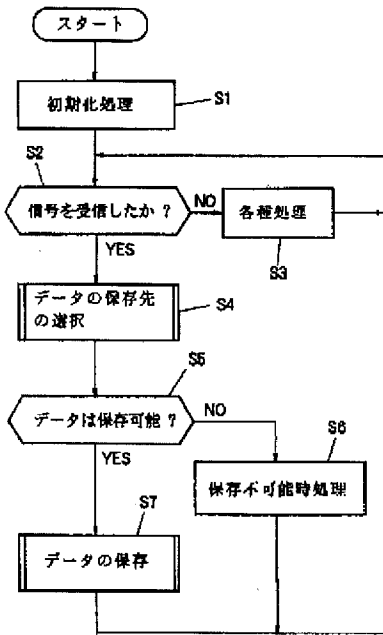
【図3】



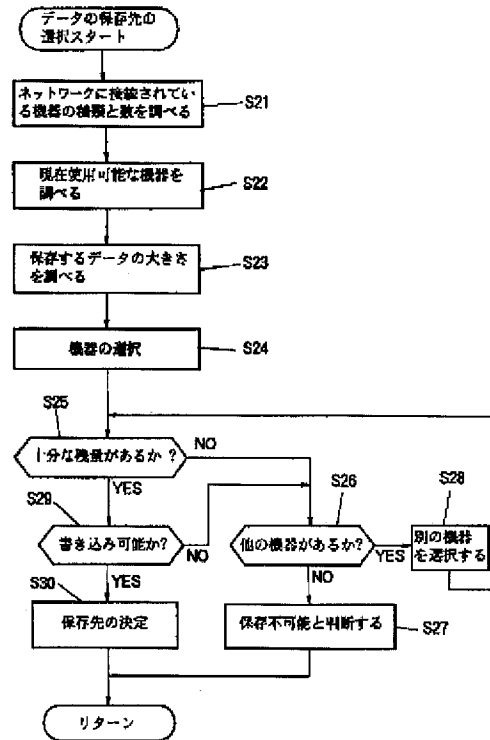
【図4】



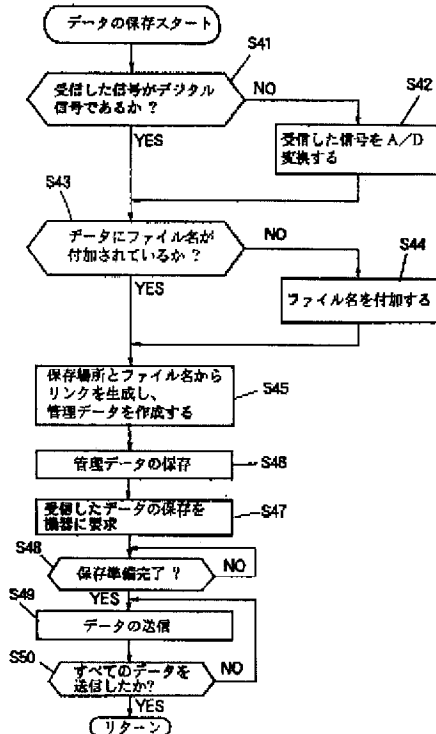
【図5】



【図6】



【図7】



【図8】

```

</HTML>
</HEAD>
<TITLE>
1997_0101_01_switzerland.jpg
</TITLE>
</HEAD>
<BODY>
<A HREF="http://VTR1/1997_0101_01_switzerland.jpg">Switzerland.jpg</A>
</BODY>
</HTML>
  
```

管理データの一例



【図9】

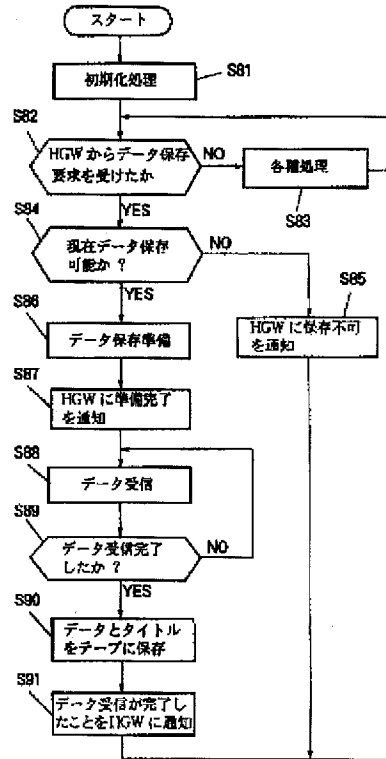
```

<HTML>
<TITLE>
1997年1月1日のデータ
</TITLE>
<BODY BGCOLOR="#FFFFFF">
<H3>1997年1月1日の保存データ</H3>
<HR>
<P>
<A HREF="http://vtr/1997_0101_01_switzerland.jpg">Switzerland.jpg</A><P>
<A HREF="http://vtr/1997_0101_02_arabia.avi">Arabia.avi</A><P>
<A HREF="http://vtr/1997_0101_03_alps.mid">Alps.mid</A><P>
<A HREF="http://vtr/1997_0101_04_china.tif">China.tif</A><P>
<A HREF="http://vtr/1997_0101_05_thai.mpk">Thai.mpk</A><P>
<A HREF="http://vtr/1997_0101_06_france.txt">France.txt</A><P>
<HR>
</BODY>
</HTML>

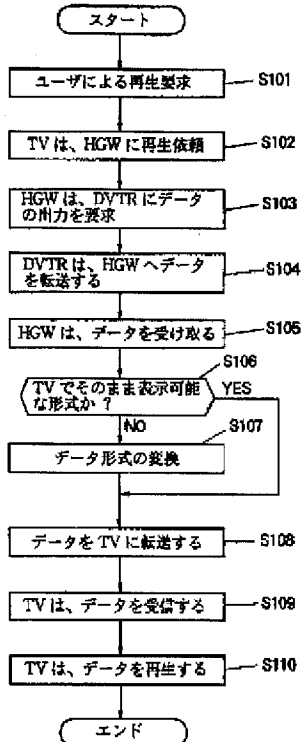
```

日付別管理データの一例

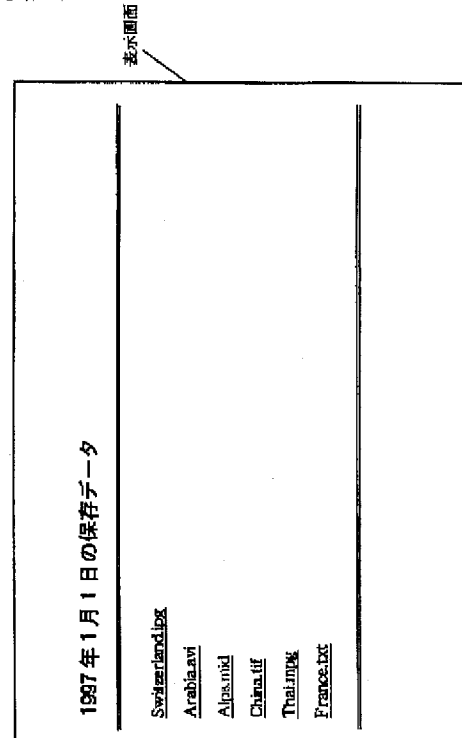
【図10】



【図11】



【図12】



© EPODOC / EPO

PN - KR20060021605 A 20060308  
 OPD - 2004-09-03  
 PA - DAEWOO ELECTRONICS CORP [KR]  
 IN - KIM SEONG UK [KR]  
 TI - SYSTEM AND METHOD FOR BRIDGING A PROTOCOL IN A MULTI HOME NETWORK  
 ICAI - H04L12/66; H04L29/06  
 ICCI - H04L12/66; H04L29/06  
 AP - KR20040070406 20040903  
 PR - KR20040070406 20040903  
 FAMN - 37128402  
 PD - 2006-03-08

© WPI / Thomson

AN - 2006-808861 [82]  
 OPD - 2004-09-03  
 PD - 2006-03-08  
 AP - KR20040070406 20040903  
 PA - (DAEW-N) DAEWOO ELECTRONICS CORP  
 CPY - DAEW-N  
 IN - KIM S U  
 TI - System and a method for bridging protocols in a multi-home network, communication between devices of different networks by converting communication request data into a protocol of a network  
 AB - NOVELTY :  
 A system and method for bridging protocols in a multi-home network are provided to allow devices of different networks to communicate with each other in an integrated home network consisting of networks using a plurality of protocols.  
 - DETAILED DESCRIPTION :  
 A memory (135) stores information on every protocol of a home network and information about lower devices of each network. A network processing unit (132) includes modules corresponding to protocols used by each network and performs communication between devices of each network. A bridge unit (134) is connected with one module of the network processing unit (132), receives communication request data from an arbitrary device, and is connected with other modules of the network processing unit (132) based on a control signal. A central controller (138) receives the communication request data through the bridge unit (134), fetches protocol information of a receiving side device desired for communication, and generates the control signal for connecting the bridge unit (134) to the module corresponding to the fetched protocol information. A data conversion unit (136) converts the communication request data based on the protocol information and transmits it to the receiving side device through the module connected with the bridge unit (134).  
 PN - KR20060021605 A 20060308 DW200682  
 NC - 1  
 IW - SYSTEM METHOD BRIDGE MULTI HOME NETWORK COMMUNICATE DEVICE CONVERT REQUEST DATA PROTOCOL  
 MC - T01-N02A1 W01-A06F7A W01-A06G2 W01-A06G5C  
 DC - T01 W01



(19)대한민국특허청(KR)  
(12) 공개특허공보(A)

(51) Int. Cl. (11) 공개번호 10-2006-0021605.  
H04L 12/66 (2006.01) (43) 공개일자 2006년03월08일  
H04L 29/06 (2006.01)

(21) 출원번호 10-2004-0070406  
(22) 출원일자 2004년09월03일

(71) 출원인 주식회사 대우일렉트로닉스  
서울특별시 마포구 아현동 686

(72) 발명자 김성욱  
서울특별시 마포구 망원동 374-1호

(74) 대리인 장성구  
김원준

심사청구 : 있음

(54) 다중 홈 네트워크에서 프로토콜을 브리지하는 시스템 및방법

요약

본 발명은 다중 프로토콜을 지원하는 홈 네트워크에서 프로토콜을 브리지하는 것으로서, 이를 위해 임의의 망에 포함된 디바이스로부터 망간 통신 요청 데이터를 수신한 후 통신 요청 데이터에 포함된 수신측 디바이스가 포함된 망의 프로토콜을 검색하고, 통신 요청 데이터를 검색된 프로토콜로 변환한 후 이를 이용하여 통신을 수행한다.

이와 같이, 본 발명은 망 구성에 사용된 프로토콜 정보 및 각 망의 하위 디바이스 정보들을 토대로 통신 요청 데이터를 수신측 디바이스가 포함된 망의 프로토콜로 변환시켜 상이한 망의 디바이스들간 통신을 수행함으로써, 다수의 프로토콜들을 이용하는 망들로 구성된 통합 홈 네트워크에서 상이한 망들의 디바이스들간 통신을 가능하게 할 수 있다.

대표도

도 1

명세서

도면의 간단한 설명

도 1은 본 발명의 바람직한 실시 예에 따른 프로토콜을 브리지하는 홈 게이트웨이를 포함한 홈 네트워크 구성도이고,

도 2는 본 발명의 바람직한 실시 예에 따른 홈 게이트웨이가 망간 통신을 수행하는 과정을 도시한 흐름도이다.

<도면의 주요부분에 대한 부호의 설명>

100 : 전력선망 110 : IP망

120 : 무선망 130 : 홈 게이트웨이

132 : 망 처리부 134 : 브리지부

135 : 메모리 136 : 데이터 변환부

138 : 중앙 제어부

### 발명의 상세한 설명

#### 발명의 목적

#### 발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 홈 네트워크에 관한 것으로, 특히 다중 홈 네트워크의 프로토콜을 브릿지시킬 수 있는 장치 및 방법에 관한 것이다.

홈 네트워크에 대한 관심이 높아지면서 PLC, IEEE 1394 및 홈 PNA(Home Phone Network Alliance) 등의 기반 기술을 바탕으로 한 홈 네트워킹 프로토콜의 표준화에 대한 많은 연구와 노력이 이어지고 있다. 이와 더불어 홈 네트워킹의 기능을 탑재한 인텔리전트한 디지털 가전기기들에 대한 소비자의 관심이 높아지면서, 다양한 홈 네트워킹용 디지털 가전기기들이 출시되고 있다.

디지털 텔레비전 수상기 및 셋 탑 박스 등의 디지털 가전기기들과 노트북형 컴퓨터, 데스크탑형 컴퓨터, PDA(Personal Digital Assistant), 태블릿 퍼스널 컴퓨터(Tablet PC) 등의 정보기술 기기들뿐만 아니라 에어컨디셔너, 세탁기, 전자 레인지 및 냉장고 등과 같은 백색 가전기기들, 그리고 조명기기에 이르기까지 홈 네트워킹 기기의 범위는 지속적으로 확대되고 있으며, 따라서 이들을 하나로 통합 관리할 수 있는 중심기기인 홈 서버(Media Center)와 같은 디지털 가전기기와 같은 홈 게이트웨이에 대한 관심도 증가하고 있다.

이러한 홈 네트워크는 각 노드가 되는 디지털 가전기기들의 특성에 따라 여러 가지 프로토콜들을 운영하고 있는데, 그 예로서 전력선을 기반으로 데이터를 송수신하는 전력선 통신을 기반으로 하는 HNCP(홈 네트워크 제어 프로토콜(Home Network Control Protocol)), IP를 기반으로 데이터를 송수신하는 인터넷 기반 프로토콜, 무선으로 데이터를 송수신하는 무선 프로토콜, 프로토콜에 관계없이 네트워크에서 주변장치들의 식별을 가능하게 해주는 자반기반의 네트워크 분산 기술인 JINI 등이 있다.

전력선 통신을 사용하는 홈 네트워크는 통신을 위한 별도 케이블 설치없이 기존 전력선을 통신망으로 활용하며, 집안으로 50~60Hz 주파수의 교류전기를 공급하는 전력선에 수백kHz에서 수십MHz의 고주파 통신 신호를 함께 보낸 접속 장비로 이 통신 신호만을 수신해 통신한다. 이 기술은 많은 비용이 드는 전용이나 기간망을 설치할 필요 없이 콘센트에 접속함으로써 인터넷 접속 등의 외부망이나 홈 랜 등 근거리 통신망을 이용할 수 있다는 점에서 편리하고 경제적이지만, 제한된 전송 전력, 높은 부하간섭과 잡음 및 짧은 거리와 1Mbps에 불과한 전송 속도의 한계로 인해 간단한 데이터 전송이나 기본적인 통신만을 제공하게 될 백색가전에 사용된다.

IP망으로 구현된 홈 네트워크는 IP를 처리할 수 있는 디바이스들만을 인식하여 디바이스들간에 데이터 송수신과 같은 네트워킹을 수행한다.

무선랜 환경에서 구현된 홈 네트워크는 AP(Access Point)가 필요하며 IEEE 802.11a, IEEE 802.11b, ZigBee 와 같은 프로토콜을 구현한 프로그램이 장착된 디바이스들만을 인식하여 디바이스들간에 데이터 송수신과 같은 네트워킹을 수행한다.

이러한 프로토콜들 중 어느 하나만 사용해도 홈 네트워크를 구성할 수 있지만, 모든 가정에서 단일 프로토콜을 사용하는 가전제품을 구입하지 않는 것이 현실이다. 오히려 각 프로토콜에는 각각의 장단점이 있으므로 가전제품에 가장 적합한 프로토콜을 사용하는 기기들을 구입하는 것이 일반적이며, 하나의 프로토콜로는 모든 가전제품들을 효율적으로 네트워킹하지 못한다.

즉, 통합 홈 네트워크의 모든 프로토콜간의 연동을 지원하는 브릿지는 구현된 바 없기 때문에 상이한 망들에 연결된 디바이스들간의 자유로운 통신은 아직 실현되지 않고 있다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은 이와 같은 종래 기술의 문제점을 해결하기 위한 것으로, 망 구성에 사용된 프로토콜 정보 및 각 망의 하위 디바이스 정보들을 토대로 통신 요청 데이터를 수신측 디바이스가 포함된 망의 프로토콜로 변환시켜 상이한 망의 디바이스들간 통신을 수행함으로써, 다수의 프로토콜들을 이용하는 망들로 구성된 통합 홈 네트워크에서 상이한 망들의 디바이스들간 통신을 가능하게 하는 다중 홈 네트워크에서 프로토콜을 브리지하는 시스템 및 방법을 제공하고자 한다.

상기와 같은 목적을 달성하기 위하여 본 발명은, 적어도 두개 이상의 상이한 프로토콜을 이용하는 망들로 구성된 홈 네트워크에서 프로토콜을 브리지하는 시스템으로서, 상기 홈 네트워크에 구성된 모든 프로토콜들과 각 망의 하위 디바이스들에 대한 정보가 저장된 메모리와, 상기 각각의 망에서 사용하는 프로토콜에 대응되는 모듈들로 구성되며, 상기 각 망의 디바이스들간 통신을 수행하는 망 처리부와, 상기 망 처리부의 어느 한 모듈과 연결되어 임의의 디바이스로부터 통신 요청 데이터를 수신하고, 제어 신호에 의거하여 상기 망 처리부의 다른 모듈과 연결되는 브리지부와, 상기 브리지부를 통해 통신 요청 데이터를 수신하고, 상기 메모리 검색을 통해 통신하고자 하는 수신측 디바이스의 프로토콜 정보를 인출한 후 상기 인출된 프로토콜 정보에 대응되는 모듈에 상기 브리지부를 연결시키기 위한 상기 제어 신호를 발생시키는 중앙 제어부와, 상기 중앙 제어부에서 인출된 프로토콜 정보에 의거하여 상기 통신 요청 데이터를 변환한 후 이를 상기 브리지부와 연결된 모듈을 통해 수신측 디바이스로 전송하는 데이터 변환부를 포함한다.

또한, 본 발명은, 적어도 두개 이상의 상이한 프로토콜을 이용하는 망들로 구성된 홈 네트워크에서 프로토콜을 브리지하는 방법으로서, 임의의 망에 포함된 디바이스로부터 망간 통신 요청 데이터를 수신하는 단계와, 상기 통신 요청 데이터에 포함된 수신측 디바이스가 포함된 망의 프로토콜을 검색하는 단계와, 상기 통신 요청 데이터를 상기 검색된 프로토콜로 변환하는 단계와, 상기 변환된 데이터를 이용하여 통신을 수행하는 단계를 포함한다.

발명의 구성 및 작용

이하에서 첨부한 도면을 참조하여 바람직한 실시 예에 대하여 상세히 설명하기로 한다.

도 1은 본 발명의 바람직한 실시 예에 따른 프로토콜을 브리지하는 홈 게이트웨이를 포함한 홈 네트워크 구성도이다.

도 1을 참조하면, 각 망들(100, 110, 120)이 홈 게이트웨이(130)에 연결되어 있으며, 홈 게이트웨이(130)에 연결되는 각 망들은 n 개의 전력선 디바이스들(104/1 ~ 104/n)과 PLC 모듈(102/1 ~ 102/n)으로 구성된 전력선망(100), m 개의 IP 기반의 디바이스들(112/1 ~ 112/n)로 구성된 IP 망(110), 1 개의 무선 프로토콜 기반의 디바이스들(122/1 ~ 122/l)로 구성된 무선망(120)으로 이루어져있다. 이때 홈 게이트웨이(130)에는 상이한 프로토콜을 사용하는 다른 망들이 추가 구성되어 연결될 수 있다.

홈 게이트웨이(130)는 적어도 두개 이상의 상이한 프로토콜을 이용하는 망들(100, 110, 120)로 구성된 홈 네트워크에서 프로토콜을 브리지하는 장치로서, 망 처리부(132), 브리지부(134), 메모리(135), 데이터 변환부(136) 및 중앙 제어부(138)로 구성된다.

메모리(135)에는 홈 네트워크를 구성하고 있는 망들(100, 110, 120)의 모든 프로토콜들, 그 예로서 전력선을 기반으로 한 HNCIP, IP, 무선 프로토콜과 각 망(100, 110, 120)의 하위 디바이스들에 대한 정보가 저장되어 있다. 이와 같이 메모리(135)에 저장된 정보는 디바이스가 플러그인 또는 플러그아웃됨에 따라서 중앙 제어부(138)에 의해서 업 데이트된다.

망 처리부(132)는 각각의 망(100, 110, 120)에서 사용하는 프로토콜에 대응되는 모듈인 전력선 모듈(132a), IP 모듈(132b) 및 무선 모듈(132c)로 구성되며, 각 망(100, 110, 120)의 디바이스들간 통신을 수행한다. 즉, 전력선 모듈(132a)은 전력선망(100)에 연결되고, IP 모듈(132b)은 IP 망(110)에 연결되고, 무선 모듈(132c)은 무선망(120)에 연결된다.

브리지부(134)는 망 처리부(132)의 어느 한 모듈, 즉 통신 요청 데이터를 송신한 디바이스가 포함된 망에 대응되는 모듈 또는 통신 요청 데이터를 수신할 디바이스가 포함된 망에 대응되는 모듈과 연결되어 임의의 디바이스로부터 통신 요청 데이터를 수신하고, 제어 신호에 의거하여 망 처리부(132)의 다른 모듈과 연결된다. 즉 전력선망(100)에 포함된 디바이스가 IP망(110)에 포함된 디바이스와 통신하기 위해 통신 요청 데이터를 송신한 경우 브리지부(134)는 망 처리부(132)의 전력선 모듈(132a)과 연결되어 통신 요청 데이터를 수신한 후 통신 요청 데이터를 IP망(110)에 포함된 디바이스에 송신하고자 할 경우 브리지부(134)는 망 처리부(132)의 IP 모듈(132b)과 연결된다.

중앙 제어부(138)는 브리지부(134)를 통해 통신 요청 데이터를 수신하고, 메모리(135) 검색을 통해 통신하고자 하는 수신측 디바이스의 프로토콜 정보를 인출한 후 인출된 프로토콜 정보에 대응되는 모듈에 브리지부(134)를 연결시키기 위한 제어 신호를 발생시킨다. 이러한 제어 신호에 따라 브리지부(134)는 수신측 디바이스가 포함된 망에 대응되는 모듈과 연결된다.

데이터 변환부(136)는 중앙 제어부(138)에서 인출된 프로토콜 정보에 의거하여 통신 요청 데이터를 프로토콜 변환한 후 이를 브리지부(134)와 연결된 모듈을 통해 수신측 디바이스로 전송한다.

상기와 같은 구성을 갖는 홈 게이트웨이가 망간 통신을 위해 프로토콜을 브리지하는 과정은 도 2를 참조하여 설명한다. 도 2는 본 발명의 바람직한 실시 예에 따른 홈 게이트웨이가 망간 통신을 수행하는 과정을 도시한 흐름도이다.

도 2에 도시된 바와 같이, 먼저 망간 통신 요청이 시작되면(S200), 홈 게이트웨이(130)는 임의의 망에 포함된 디바이스로부터 통신 요청 데이터를 수신한다(S202). 이때, 통신 요청 데이터는 망간 통신을 요청한 디바이스 포함된 망에 대응되는 모듈과 브리지부(134)를 통해 중앙 제어부(138)에 제공된다.

중앙 제어부(138)는 통신 요청 데이터를 토대로 수신측 디바이스를 추출하고, 메모리(135)의 검색을 통해 수신측 디바이스의 프로토콜 정보를 인출한 후 인출된 프로토콜 정보와 통신 요청 데이터를 데이터 변환부(136)에 제공함과 더불어 인출된 프로토콜 정보를 토대로 브리지부(134)에 제어 신호를 발생시켜 브리지부(134)를 프로토콜 정보에 대응되는 모듈로 연결시킨다(S204).

데이터 변환부(136)는 중앙 제어부(138)에서 제공받은 프로토콜 정보를 토대로 통신 요청 데이터를 변환한 후 브리지부(134)에 연결된 모듈을 통해 수신측 디바이스에 변환된 통신 요청 데이터를 전송한다(S206, S208).

전술한바와 같이, 프로토콜들을 브리지하는 홈 게이트웨이를 통해 상이한 망간 통신을 유연하게 수행할 수 있기 때문에 통합 홈 네트워크의 한 디바이스와 다른 망의 디바이스간의 통신을 가능하게 해준다.

본 발명에 대한 앞의 설명에서는 일 실시예에 국한하여 설명하였으나 본 발명의 기술이 당업자에 의하여 용이하게 변형 실시될 가능성이 자명하다. 이러한 변형된 실시예들은 본 발명의 특허청구범위에 기재된 기술사상에 포함된다고 하여야 할 것이다.

#### 발명의 효과

이상 설명한 바와 같이, 본 발명은 망 구성에 사용된 프로토콜 정보 및 각 망의 하위 디바이스 정보들을 토대로 통신 요청 데이터를 수신측 디바이스가 포함된 망의 프로토콜로 변환시켜 상이한 망의 디바이스들간 통신을 수행함으로써, 다수의 프로토콜들을 이용하는 망들로 구성된 통합 홈 네트워크에서 상이한 망들의 디바이스들간 통신을 가능하게 할 수 있다.

#### (57) 청구의 범위

##### 청구항 1.

적어도 두개 이상의 상이한 프로토콜을 이용하는 망들로 구성된 홈 네트워크에서 프로토콜을 브리지하는 시스템으로서,

상기 홈 네트워크에 구성된 모든 프로토콜들과 각 망의 하위 디바이스들에 대한 정보가 저장된 메모리와,

상기 각각의 망에서 사용하는 프로토콜에 대응되는 모듈들로 구성되며, 상기 각 망의 디바이스들간 통신을 수행하는 망 처리부와,

상기 망 처리부의 어느 한 모듈과 연결되어 임의의 디바이스로부터 통신 요청 데이터를 수신하고, 제어 신호에 의거하여 상기 망 처리부의 다른 모듈과 연결되는 브리지부와,

상기 브리지부를 통해 통신 요청 데이터를 수신하고, 상기 메모리 검색을 통해 통신하고자 하는 수신측 디바이스의 프로토콜 정보를 인출한 후 상기 인출된 프로토콜 정보에 대응되는 모듈에 상기 브리지부를 연결시키기 위한 상기 제어 신호를 발생시키는 중앙 제어부와,

상기 중앙 제어부에서 인출된 프로토콜 정보에 의거하여 상기 통신 요청 데이터를 변환한 후 이를 상기 브리지부와 연결된 모듈을 통해 수신측 다비아스로 전송하는 데이터 변환부

를 포함하는 다중 홈 네트워크에서 프로토콜을 브리지하는 시스템.

청구항 2.

제 1 항에 있어서,

상기 메모리는, 상기 각 망에 디바이스들이 추가됨에 따라 업데이트되는 것을 특징으로 하는 다중 홈 네트워크에서 프로토콜을 브리지하는 시스템.

청구항 3.

적어도 두개 이상의 상이한 프로토콜을 이용하는 망들로 구성된 홈 네트워크에서 프로토콜을 브리지하는 방법으로서,

임의의 망에 포함된 디바이스로부터 망간 통신 요청 데이터를 수신하는 단계와,

상기 통신 요청 데이터에 포함된 수신측 디바이스가 포함된 망의 프로토콜을 검색하는 단계와,

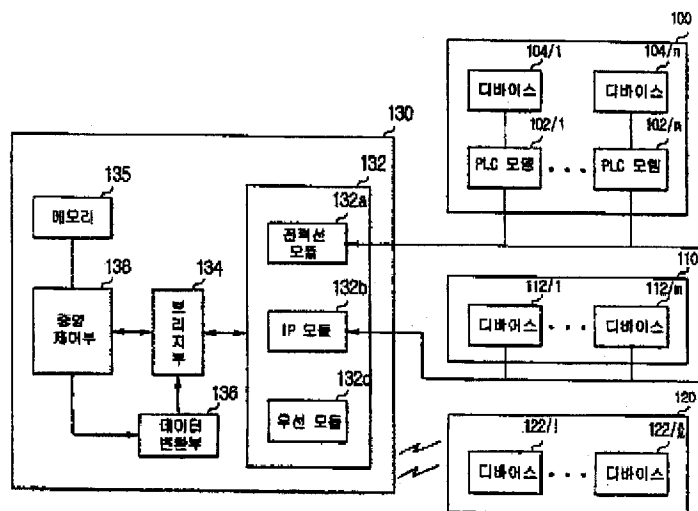
상기 통신 요청 데이터를 상기 검색된 프로토콜로 변환하는 단계와,

상기 변환된 데이터를 이용하여 통신을 수행하는 단계

를 포함하는 다중 홈 네트워크에서 프로토콜을 브리지하는 방법.

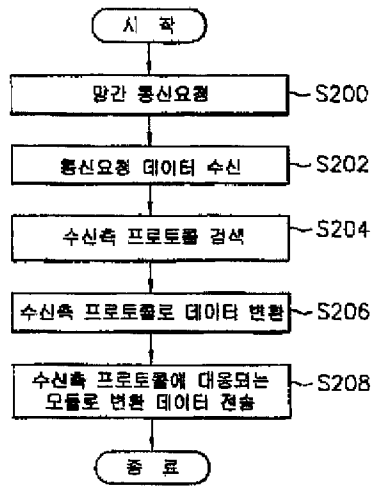
도면

도면 1





도면2



(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
19 July 2001 (19.07.2001)

PCT

(10) International Publication Number  
WO 01/52478 A2

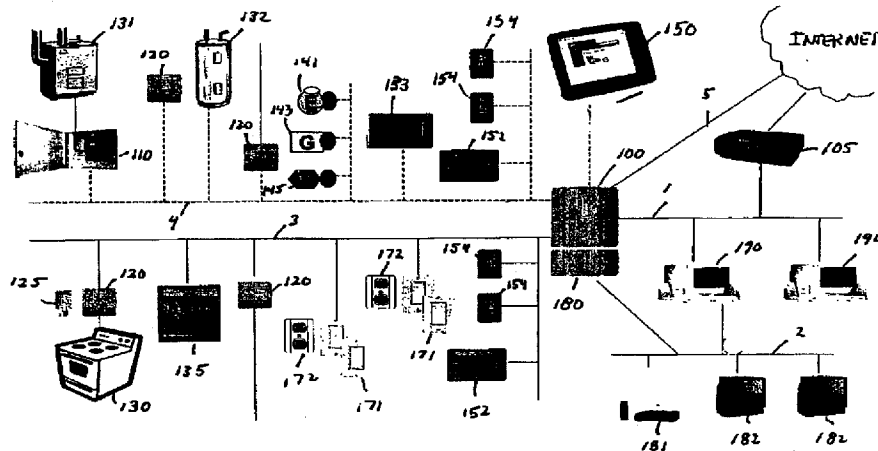
- (51) International Patent Classification<sup>7</sup>: **H04L 12/00**
- (21) International Application Number: PCT/US01/00428
- (22) International Filing Date: 8 January 2001 (08.01.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
 

60/174,829	7 January 2000 (07.01.2000)	US
60/176,005	14 January 2000 (14.01.2000)	US
60/180,281	4 February 2000 (04.02.2000)	US
09/755,203	8 January 2001 (08.01.2001)	US
09/755,202	8 January 2001 (08.01.2001)	US
09/755,194	8 January 2001 (08.01.2001)	US
- (63) Related by continuation (CON) or continuation-in-part (CIP) to earlier applications:
 

US	60/174,829 (CON)
Filed on	7 January 2000 (07.01.2000)
US	60/176,005 (CON)
Filed on	14 January 2000 (14.01.2000)
US	60/180,281 (CON)
Filed on	4 February 2000 (04.02.2000)
- (71) Applicant (for all designated States except US): **INVEN-SYS CONTROLS PLC** [US/US]; 33 Commercial Street, Foxboro, MA 02035 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **SHAROOD, John**, N. [US/US]; Invensys Controls, Suite 400, 2809 Emerywood Parkwood, Richmond, VA 23294 (US). **TURNER, James, H.** [US/US]; Invensys Controls, 1701 Byrd Avenue, Richmond, VA 23230-3011 (US). **BAILEY, Graham** [DE/DE]; Am Neuen Rheinhafen 4, 67346 Speyer (DE). **HENDERSON, Bruce, H.** [US/US]; Invensys Controls, Suite 400, 2809 Emerywood Parkwood, Richmond, VA 23294 (US). **CARR, D., Mitchell** [—/US]; 20755 Quiet Brook Place, Potomac Falls, VA 20165 (US). **JOHNSON, Terri** [US/US]; 15 Dorchester Court, Hawthorn Woods, IL 6007 (US). **PEACHEY, David** [US/US]; Invensys Controls, Suite 203, 2141 E. Broadway Road, Tempe, AZ 85282-1895 (US).
- (74) Agents: **BODENDORF, Andrew, F.**; Fish & Richardson P.C., 601 Thirteenth Street, N.W., Washington, DC 20005 et al. (US).

[Continued on next page]

(54) Title: BUILDING CONTROL



(57) Abstract: In one general aspect, a complete home and commercial automation system may accommodate existing appliances at a cost that is affordable to the average homeowner or small business. In addition, the automation system can be installed in a home or a building without substantial rewiring, expense, or invasiveness. The automation system allows control of all associated systems from a remote location using virtual controls that resemble the actual controls of the appliances. In addition, the virtual controls have a consistent appearance between most interfaces. As a result, a user can operate and monitor systems without having to be present on site and without having to learn how to operate new controls. The automation system also can monitor the use of all home appliances and provide this information to a monitoring facility or a service provider. As a result, the monitoring facility or the service provider can provide services to the user at a time when the service would be most beneficial to the user. In addition, by monitoring specific use of home appliances and user activities, companies can offer the user better service through the use of interactive coupons, warranties, improved maintenance, repair information, and interactive messaging.

WO 01/52478 A2



(81) **Designated States (national):** AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— without international search report and to be republished upon receipt of that report

(84) **Designated States (regional):** ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

## BUILDING CONTROL

### TECHNICAL FIELD

This invention relates generally to building automation, and more particularly to a  
5 retrofit monitoring device for use in building automation.

### BACKGROUND

Building automation concepts have been known for some time. However, in  
general, these concepts have been limited to large industrial settings or to custom-  
10 designed systems for luxury homes because of the prohibitive cost associated with  
conventional automation systems. In addition, automation systems generally have been  
placed in new structures because of the substantial wiring necessary to implement these  
systems. Retrofitting automation systems in existing structures has been unpopular  
because, in general, the procedure is invasive and may require destruction of interior  
15 surfaces, substantial rewiring, significant expense, and inconvenience to the homeowner  
or tenant.

### SUMMARY

In one general aspect, a complete home and commercial automation system may  
20 accommodate existing appliances at a cost that is affordable to the average homeowner or  
small business. In addition, the automation system can be installed in a home or a  
building without substantial rewiring, expense, or invasiveness. The automation system  
allows control of all associated systems from a remote location using virtual controls that  
resemble the actual controls of the appliances. In addition, the virtual controls have a  
25 consistent appearance between most interfaces. As a result, a user can operate and  
monitor systems without having to be present on site and without having to learn how to  
operate new controls. The automation system also can monitor the use of all home  
appliances and provide this information to a monitoring facility or a service provider. As  
a result, the monitoring facility or the service provider can provide services to the user at  
30 a time when the service would be most beneficial to the user. In addition, by monitoring  
specific use of home appliances and user activities, companies can offer the user better  
service through the use of interactive coupons, warranties, improved maintenance, repair  
information, and interactive messaging.

In one general aspect, a device monitors an appliance that receives power from a source. The device includes a first coupler that couples the device to the power source. A second coupler couples the device to the appliance. A monitoring circuit is connected between the first coupler and the second coupler to monitor power supplied by the source to the appliance. A communications circuit also is provided. The monitoring circuit provides data based on the monitored power to the communications circuit, and the communications circuit outputs these data through the first coupler.

The communications circuit may include a receiver that receives a signal from the first coupler to control the monitoring circuit. The communications circuit also may include a transceiver that receives a signal from the first coupler to control the monitoring circuit and to transmit monitored power data. For example, the communications circuit may include a power line carrier transceiver and a power line driver.

The monitoring circuit may measure current drawn by the appliance, and may include a processor that determines an operating state of the appliance based on the measured current. The monitoring circuit also may include a memory for storing the measured current and periodically sending measured current data to the first coupler. The memory may store an electronic signature, and the processor may determine an operating state of the appliance based on the electronic signature.

A modem may be connected to the monitoring circuit and may transmit data based on the measured current. A radio frequency transmitter also may be connected to the monitoring circuit for transmitting data based on the measured current. A serial port connected to the monitoring circuit may be used to receive data about the appliance.

A battery may be included to supply power to the monitoring circuit when power is not received by the first coupler.

A switch may be connected to the first coupler. The switch can be opened in response to the control signal. When opened, power from the source may be inhibited from being supplied to the appliance.

The first coupler may include a pin for connection to a live line and a pin for connection to a neutral line. First and second power lines may connect the first and second couplers. The second coupler may include a first slot connected to the live pin through the first power line and a neutral slot connected to the second pin through the second power line.

In another general aspect, a system for monitoring an appliance that receives power from a source may include a power line connected to the source, a circuit

connected to the power line and the appliance, a circuit that monitors power supplied to the appliance, and a processor connected to the power line. The circuit sends signals to the processor through the power line. The signals are based on the power supplied to the appliance.

5           The circuit may include a first coupler coupling the circuit to the power line, a second coupler coupling the circuit to the appliance, a monitoring circuit connected between the first coupler and the second coupler to monitor power supplied by the source to the appliance, and a communications circuit connected to the monitoring circuit. The monitoring circuit may provide data based on the monitored power to the  
10           communications circuit.

The circuit may be a plug having a live pin and a neutral pin and slots for receiving a live pin and a neutral pin from the appliance's plug. The live pin connects to a live line and the neutral pin connects to a neutral line.

The system may include a connection to a service provider that monitors the  
15           appliance. The processor may be a control server that sends signals to the service provider about the operation of the appliance. The processor also may be a gateway.

The processor may diagnose the signals to determine if an appliance needs servicing.

The system may include a display. The processor may send a message to the display  
20           alerting a user when the appliance needs servicing.

In another general aspect, a retrofit plug is adapted to be that receives by an appliance receiving power from a source. The retrofit plug includes a live pin, a neutral pin, a first line connected to the live pin, and a second line connected to the neutral pin. A first slot is connected the first line for receiving a live pin connected to the appliance. A  
25           second slot is connected to the second line for receiving a neutral pin connected to the appliance. A transformer monitors the first and second lines. A measurement circuit connected to the transformer measures current supplied to the appliance. A power line carrier transceiver encodes a power line carrier signal based on the measured current.

In one general aspect, a wireless damper includes a register, a controller regulating  
30           the amount of air flow provided by the register, and a radio frequency communications circuit. The radio frequency communications circuit provides a signal to the controller to adjust the amount of air flow. A register regulation mechanism opens and closes the register in response to a signal from the controller to regulate air flow through the

damper. The register regulation mechanism can be a variable switch, which variably adjusts the amount of air flow through the damper and a magnetic latch.

5 A battery supplies power to the damper, the controller, the register regulation mechanism, and the radio frequency communications circuit. The controller may monitor a power level of the battery. To do so the controller may send a signal for transmission by the radio frequency communications circuit when the power level reaches a predetermined amount. The controller may open the register if the power level of the battery reaches the predetermined amount.

10 The damper may include a sensor for determining a condition at the damper. The controller may adjust the register regulation mechanism in response to the condition determined by the sensor. The controller receives the determined condition from the sensor and may send a signal with the determined condition to the radio frequency communications device for transmission of the determined condition signal. The condition sensed may be temperature.

15 The radio frequency communications circuit may be a radio frequency transceiver.

The controller may include a processor. The processor may send a signal to the radio frequency communications circuit identifying the damper. The processor also may determine if a signal received by the radio frequency communications circuit is addressed to the damper. The controller may include a memory for storing damper identification. 20 The processor may determine if a signal is addressed to the damper using the stored damper identification.

In another general aspect, a wireless air flow control system may include a wireless damper including a battery, and a zone controller. The zone controller sends a signal to the wireless damper to control the amount of air flow through the damper.

25 The wireless air flow control system may include a display on which the zone controller displays a message identifying that the damper's battery power level is low or needs replacing.

The wireless air flow control system may include a user interface. The user interface generates a signal and the zone controller controls the damper in response to the user interface generated signal. The user interface can be a thermostat or a computer. 30

The wireless air flow control system also may include a control server. The control server controls the zone controller in coordination with other building functions under control of the control server.

The wireless air flow control system may include a building air flow generation mechanism. The zone controller opens and closes the damper in response to activation and deactivation of the air flow generation mechanism.

The wireless air flow control system may include a processor that sends a signal to a zone controller to identify the damper. The processor can determine if a signal received by the radio frequency communications circuit is addressed to the damper.

Other features and advantages will be apparent from the description, the drawings, and the claims.

10

## DESCRIPTION OF DRAWINGS

Fig. 1 is a block diagram of an exemplary automation system.

Figs. 2 and 3 are block diagrams of a control server of the system of Fig. 1.

Fig. 4 is a diagram of a universal controller of the system of Fig. 1.

15

Fig. 5 is a perspective view of an exemplary communications module of the system of Fig. 1.

Fig. 6 is a perspective view of an exemplary retrofit plug.

Figs. 6B-6D are block diagrams of a retrofit plug of the system of Fig. 1.

Figs. 7A-7C are exemplary screen shots of touchpad user interfaces of the system of Fig. 1.

20

Fig. 8 is a block diagram of a distributed video network.

Fig. 9 is a block diagram of a retrofit damper system.

Fig. 10 is a block diagram of a retrofit damper of the system of Fig. 9.

Fig. 11 is a block diagram of a zone controller of the system of Fig. 9.

Fig. 12 is a block diagram of function blocks for home manager software.

25

Fig. 13 is a screen shot of the home manager temperature control of the software of Fig. 12.

Fig. 14 is a screen shot of the home manager kitchen assistant of the software of Fig. 12.

Fig. 15 is a block diagram of a metering network.

30

Fig. 16 is a screen shot of a remote monitoring service.

Fig. 17 is a screen shot of a temperature monitoring interface.

Fig. 18 is a block diagram of a central locking network.

Fig. 19 is a block diagram of a security network.

Fig. 20 is a block diagram of a lighting network.



Fig. 21 is a block diagram of a heating network.

Fig. 22 is a block diagram of a zone controller and a heating network.

Fig. 23 is a screen shot of a home manager heating control interface.

Fig. 24 is a block diagram of an appliance control system.

5 Fig. 25 is a screen shot of an exemplary virtual control panel of the system of Fig.  
24.

Figs. 26A and 26B are block diagrams of a refrigeration monitoring unit.

Figs. 27A and 27B are block diagrams of a refrigeration monitoring unit.

Like reference symbols in the various drawings indicate like elements

10

## DETAILED DESCRIPTION

### ***SYSTEM OVERVIEW***

15 An automation system, which may also be referred to as a building control (BC)  
system, may be used to automate a home, an office, or another type of commercial or  
residential building. In the residential context, the BC system establishes a home network  
that controls, coordinates, facilitates, and monitors user-designated activities within the  
home. The BC system provides compatibility between external and internal networks,  
systems, and appliances, and is modular in construction to allow easy expansion and  
20 customization. The BC system can be retrofitted for use in existing structures and legacy  
appliances without the need for drastic remodeling, added wiring, or complicated  
installation/customization, and can be installed by a homeowner with minimal instruction.  
Professional installation and maintenance also are simplified, so as to avoid the high costs  
typically associated with custom home automation.

25 The modularity of the BC system provides for easy customization for either  
commercial or residential use. For residential applications, system elements may be  
sealed for easy installation, configuration, and aesthetic appearance. Expansion within  
the residential applications can be accomplished by adding new modules to the system.  
On the other hand, for commercial or advanced residential applications, the system can be  
30 custom configured and expanded through the additional use of expansion boards,  
PCMCIA cards, or plug in solutions. Although the following examples are primarily  
described with reference to home applications, the described devices and concepts also  
are applicable for commercial use.

### The BC System

Referring to Fig. 1, an exemplary BC system is based around a control server 100 that manages a number of primary networks including: an internal home network 1 (e.g., a USB or Ethernet network), a video distribution network 2 (e.g., Peracom AvCast System), a power line carrier (PLC) network 3, a wireless radio frequency (RF) communications network 4, and an Internet portal 5 (e.g., a DSL modem). BC system devices attach to the control server 100 through one of these networks, and each network services a different aspect of home automation.

The home network 1 can include a residential broadband gateway 105 for high-speed interaction with the Internet and service providers. In addition, a number of computer systems 190 can be connected to provide access to the control server 100 and between the computer systems 190. The home network 1 can be implemented using any LAN system, such as, for example, an Ethernet system. The computer system 190 can be used as an interface for controlling home automation and running home automation software.

The video distribution network 2 can include an AvCast subcomponent 180 that plugs into the control server 100 to coordinate multimedia activity between, for example, video monitors 182 and a satellite TV system 181. The video distribution system 2 also can act as an interface to the control server 100.

The PLC network 3 provides control of switches 171, power outlets 172, and smart appliances 135. In addition, a number of communications modules 120 can be used to communicate with legacy devices, such as a range 130. Retrofit plugs 125 also can be used within the PLC network to provide communication with legacy devices. A number of different interfaces, such as, for example, touch pads 152, 154 and portable tablet 150, can be used to provide for user interaction with the control server.

The RF network 4 includes communications modules 120, legacy appliances 132, and interfaces 152 and 154. In addition, a universal controller 110 can be used to control appliances, such as a furnace 131. The RF network 4 can be connected with sensors 141, 143, and 145 to monitor home utilities such as electricity, gas, and water, respectively. A smart thermostat 133 and a damper system can be used to control and optimize home heating and cooling.

The Internet portal 5 allows access and control of the BC system from a remote location. In addition, service providers may remotely monitor appliances, usage, and

security within the home. New applications and upgrades of existing software can be obtained through the Internet.

### **BC Controller/Server**

5           The control server 100 is the core of the BC system. The control server 100 provides multi-protocol routing and supervisory control for communicating appliances and general purpose device controllers. The control server 100 is responsible for communicating with subordinate system devices while making data available to other supervising devices. The supervising devices include local user interfaces or Internet-  
10 based remote interfaces.

          The control server 100 features pre-configured control function blocks or objects, in addition to user defined control strategies, that run on a real time control engine capable of executing combinational and sequential logic control. The control engine may be application specific or generic depending on the size and the intended purpose of the  
15 BC system in which the control engine is implemented. The control function blocks executed by the control server 100 are designed to operate in a number of modes, such as, for example, an away mode, a sleep mode, and a vacation mode, among others. The control server 100 operates appliances and subsystems based on the BC system's current operating mode. For example, when entering the away mode, the control server 100 can  
20 activate the security system and turn down the heat or the air conditioning. In addition to modes that can be selected and transitioned, "hard-wired" functions are provided to initiate actions based on recognition of certain external conditions. One example of such an action is the flashing of red screens on all televisions and displays in a home when a fire alarm is tripped.

25           The control server 100 also provides for protocol conversion. For example, if an attached appliance has a stripped-down protocol, the control server 100 adds the missing elements to make the appliance appear to be compliant with a desired industry standard protocol. Where the physical layer necessary for communication with a device is not available in the control server 100, add-on units may be used to attach the control server  
30 to the device. The control server 100 accommodates multiple protocols and physical layers through communications modules 120 attached between devices using foreign protocols or physical layers and the control server 100. Similarly, smart modules, retrofit plugs, and universal controllers may be used to provide the function of protocol conversion. The control server 100 interfaces with any of the system graphic user

interfaces (GUIs), PC networks, Internet, and all other portions of the BC system as described in greater detail below.

The control server 100 is modular in design and can be scaled with regard to size, functions, and hardware desired for a specific implementation. One example of a control server 100 is shown in Fig. 2. As shown in Fig. 2, the control server 100 includes a processor 200. The processor 200 is connected to a board with a communications bus 202, an I/O port 203, and interfaces including a RF digital signal processor 207, a 10 BASE-T interface 206, a modem 205, and a serial interface 204. The interfaces provide communication between the control server 100 and the primary BC system networks 1-5.

The processor 200 also is connected to a flash memory 224, a RAM 222, and an EEPROM 220. An optional power source (RTC xtal and Battery) 230 can be used to power the control server 100 in the event of loss of power. A number of communication ports are connected with the various interfaces. The communication ports can include a 10 BASE-T port 212, a TELCO DAA 214, a RS-232 port 216, a RS-485 port 218, and a S-BUS port (or USB port) 219.

In addition, a PLC controller 280 and an EmWare Adapter 260 are connected to the communications input/output port 203. These devices may be configured on the board or as add-on modules. The EmWare adapter 260 can be used to communicate with and control appliances or systems that use an EmWare communications protocol. Other adapters for other communications protocol or systems can be provided in an original device or as add-on, plug-in applications. A VGA controller 240 is provided for connection with a PC raster port 242.

As shown in Fig. 3, the control server 100 also can be implemented as a main board 300 with optional add on boards and PCMCIA slots. The main board 300 includes an Ethernet connection 301, a serial I/O port 315, and an optional slot for a PC card 305. Daughter boards are connected to the main board using a system bus connector. A daughter board typically includes an eight-way serial interface card and a four-way Ethernet card, with an optional slot for a PC card. The main board 300 can be implemented using a Motorola MPC860 PowerPC core 304, a memory (including flash 306, DRAM 308, NVRAM 307), and I/O including: Dual SCC channels with HDLC interface, two status LEDs, two Tx/Rx pair communication status LED indicators, a debug RS-232 serial port, a PCMCIA slot, 10/100 Base T physical interface connector, an EIA-232 serial port, an EIA-485 serial port, and an EIA-485 serial port with 24V PSU input.

External connections from the main board 300 include a single RJ-45 connector 301 for an Ethernet connection and a number of RJ-11 connectors for serial communications. The first RJ-11 connector 303 can support two connections for 24V DC serial communication for PLC 310 and a second connector 302 for an EIA-485 serial interface. The serial interfaces on the main board 300 can use RJ-11 connectors. PLC interfaces to the main board, as well as other boards, are made through a serial interface to, for example, external communications modules. The primary PLC interface 310 is enclosed inside the external transformer housing that provides 24V DC to the control server.

Functionally, the Ethernet interface 360 to the main board 300 is the primary WAN or broadband interface. Typically, the interface 360 can be connected to a cable modem or a DSL modem and can provide a firewall to secure data access. The EIA-232 interface 350 is provided for programming and debugging of the control server 100 in the field. The free EIA-485 interface allows flexible customization of the control server 100 or connection to an external POTS modem, a serial interface (third party device), or a second PLC.

The control server 100 main board 300 can accommodate a number of additional EIA-485 interfaces (e.g., eight interfaces). The additional interfaces can provide connection to third party devices, such as security panels, lighting control systems, HVAC zoning systems, and others. The additional interfaces also can be used for connection to external bridges, such as additional PLC interfaces, RF subsystems, communications modules, and retrofit plugs.

The Ethernet board (not shown) on the main board 300 includes four 10/100 base T Ethernet interfaces. The four interfaces provide connections for two secure LAN connections, one unsecure LAN connection, and one unsecure WAN connection.

The control server video board (not shown) can include the following interfaces: video out/VGA out, video in, dual USB – printer, keyboard/mouse interface, IR interface, and PCMCIA slot (optional). The video board provides video I/O as well as IR command transmission. A keyboard and mouse combination can be used with the video board through a USB or USB-to-RF interface (in the case of a wireless keyboard or mouse). A second USB connector can interface with printers, digital cameras, and other peripheral equipment. Functionally, the board accepts video input and digitizes the video for use by the rest of the BC system using the MPEG4 standard. The video board also provides video output as a TV channel for broadcast on connected televisions within the home.

### **Universal Controller**

The universal controller 110 is an optimized form of the control server 100. The universal controller 110 performs a single dedicated task, such as HVAC control. As a result, the universal controller 110 includes only the input and output features that are necessary for the dedicated task. The universal controller 110 can be used in a stand-alone configuration with access through remote dial-up, Internet access, and/or a touchpad interface. The universal controller 110 also can be controlled and monitored by the control server 100. The universal controller 110 communicates with the control server through the RF or PLC networks or by directly wired serial communication. The universal controller 110 can be used to handle applications that are pre-packaged for physical distribution, that have outgrown the capability of the control server 100, or that have special features not handled by a standard control server 100. In addition, the universal controller 110 can be implemented as a daughter board to the control server 100.

According to the example shown in Fig. 4, the universal controller 110 includes a processor 400 to which a memory 420 is connected. The memory includes communications software for the remote uploading and downloading of data and software for control of specific attached subsystems, such as, for example, HVAC control. The universal controller 110 also includes 16 analog/digital switches for receipt of signals from sensors. An RS-232 communication interface 430 is provided for PC, modem, and other communication with serial communication ports of other devices. Twenty four relays configured in pairs of twelve are provided as output 440. Each relay in a pair can be configured for an individual device that is powered from a common source.

25

### **Control Modules**

Referring again to Fig. 1, control modules (e.g., 120 and 125) allow legacy appliances that have already been purchased by a homeowner or commercial operator to be integrated into a home automation system. This is important because appliances are expensive and have relatively long operational lives. As a result, appliances typically are not replaced until failure. Therefore, for existing appliances to be incorporated in a total home or commercial automation system, an interface is needed to allow communication with the automation system so that a user is not forced to buy a network ready appliance.

30

The control modules provide such an interface in a form that can be installed easily by the homeowner or business operator.

In addition, manufacturers may not wish to sell devices that are network/system compliant due to the added cost associated with outfitting the appliance with the necessary software and control circuitry. Therefore, a control module can be inserted into an appliance aftermarket, or by the manufacturer, to provide network protocol compliance.

Two examples of control modules are the appliance communications module and the retrofit plug. The appliance communication module acts a bridge between the control server (or remote monitoring service provider) and an appliance by providing protocol conversion that is specific to the appliance. The communication module also allows the control server to control the appliance. The retrofit plug provides for remote monitoring and diagnosis of an appliance, and is easily installed with any appliance.

#### Appliance Communications Module

The appliance communications module 120 is adapted to be received by an appliance having an appliance controller. The communications module 120 includes a communications protocol translator. The communications protocol translator translates signals received from a communications media into appliance controller signals. The translator also translates appliance control signals received from the appliance controller into a communications protocol to be output to an appliance communications network. The communications module 120 also can include a power line transceiver connected to the communications protocol translator and a power line driver connected to the transceiver and the connector. The communications module's connector is electrically coupled to the appliance controller. Alternatively, the communications module 120 can include a radio frequency (RF) transceiver or modem for connection to an appliance network. An example of the communications module 120 is shown in Fig. 5.

The protocol translator translates signals received from the network into appliance controller signals. The translator also translates received appliance control signals according to a communications protocol to be output to the network through the modem or transceiver.

A network ready appliance is also provided. The network ready appliance includes an appliance controller having a communications port. The appliance also includes a cavity, defined by walls, that is adapted to receive the communications module

120. An opening in a wall of the appliance allows access to the cavity. A connector is attached to one of the cavity walls. A communications line connecting the communications port and the connector also is provided. The connector is electrically coupled to the appliance controller or to the main power supply. The network ready  
5 appliance further includes a detachable cover provided over the opening to protect a user from electric shock. Alternatively, the appliance connector can be recessed in a cavity to protect the user against shock.

The communications module is described in detail in U.S. Patent Application 09/511,313 title "COMMUNICATION MODULE" which was filed February 23, 2000,  
10 and is incorporated by reference in its entirety.

#### Retrofit Plug

The retrofit plug 125, shown in Figs. 6A-6D, is a plug-through device that is either attached in line with the main appliance electrical supply or internally in line with a  
15 main control board interface connector of an appliance 130. As shown in Fig. 6A, the retrofit plug can be installed on legacy equipment by simply connecting the retrofit plug 125 to the pins of the appliance that are used to supply power to the appliance. As a result, a legacy appliance can be easily incorporated into a network to allow monitoring and control of the appliance by a homeowner without the need for custom or professional  
20 installation.

As one example of an internal connection, control signals inside certain refrigerators pass through a marshalling connector connected to the main control board. By connecting a retrofit plug to this connector, all signals within the refrigerator can be tapped for diagnostic data. The diagnostic data may be sent to the control server 100 that  
25 monitors the appliance 130, for example, through the PLC network 3. The data gathered from the appliance 130 can be stored by the control server 100 or downloaded to a remote database maintained by a service provider.

In a standalone application, the control server 100 can be replaced by a gateway connected to a PLC network. Data from the retrofit plug can be sent through the PLC  
30 network to the gateway. The gateway transmits the data to a service provider monitoring the appliance 130. The plug may operate as a stand-alone unit by equipping the plug with a modem to communicate with an external computer (e.g., as provided by a monitoring service). The retrofit plug 125 also can be equipped with an RF transceiver so that the



plug may be incorporated in a wireless network 4 for monitoring and control of an associated appliance.

Fig. 6B shows an exemplary retrofit plug 125 that provides an interface between an appliance's electronic control system and the control server 100. The retrofit plug 125 has an outer housing 600 made of, for example, an electrically-insulating plastic (class II) or (class I). The retrofit plug can include a number of couplers. For example, the housing 600 includes slots 601 and 602 for connection with pins from the appliance 130, for example, on a power cord, that are used to supply power to the appliance 130. Pins 603 and 604 extend from the housing for connection with the mains that supply power to the appliance 130. Although only two pins and two slots are shown in the example of Fig. 6B-D, additional pins and slots may be included as needed to be compatible with any particular appliance's power supply. For example, a retrofit plug could attach to a three pin connector by adding an additional slot and pin for an earth connection or to a four pin connector having two live pins, a neutral pin, and a ground pin by adding slots and pins for the second live pin and the earth pin.

The retrofit plug 125 includes a power supply 650 for supplying power to a measure and transmit circuit 620, a power line communication (PLC) transceiver 630, and a line driver 640. The power supply 620 powers the retrofit plug's components (620, 630, and 640) by converting the appliance AC voltage (e.g., 100V to 264V and 50/60 Hz) to a 5/10V DC voltage. The power supply 650 receives power from pins 603 and 604 through lines 641 and 643.

The retrofit plug includes monitoring circuitry. For example, a measure and transmit circuit 620 is connected to a current transformer 610 to measure the current being drawn by the appliance attached to the retrofit plug 125. Other circuitry that could be used to monitor the current drawn by the attached appliance includes a Rogowski coil or a shunt.

The measure and transmit circuitry 620 may include a processor (e.g., an ASIC, a DSP, a microprocessor, or a microcontroller) and memory (such as an integrated circuit (IC) memory or a flash memory). The measure and transmit circuit 620 can simply monitor and report the current drawn by the attached appliance 130. Specifically, the measure and transmit circuit 620 may monitor current draw timing, duration, and amount. In more sophisticated applications, the measure and transmit circuit can be upgraded to perform bi-directional communication by translating between a communications media protocol used by the control server 100 and the appliance's control protocol. In addition,

if the appliance's load current is measured, an indication of power can be derived from the square of the load current. Line voltage may be measured and multiplied by the load current to measure true power consumption.

The current draw data or power data can be stored by the measure and transmit  
5 circuit 620. The measure and transmit circuit 620 can be programmed to periodically send the measured data to the control server 100 as part of a general monitoring function, such as, for example, energy management and logging functions. In addition, the measure and transmit circuit 620 can be programmed to compare measurement data to specific electronic signatures stored in a table in the memory of the retrofit plug 125. The  
10 measure and transmit circuitry can send messages to the control server 100 in response to events which indicate a state of the appliance 130 requiring some further action (e.g., shut off power).

The retrofit plug 125 also includes a communications circuit. The communications circuit sends data from the measure and transmit circuit to a remote  
15 processor, such as, for example, the control server 100. The communications circuit may also receive signals from a remote processor, such as, for example, the control server 100. The communications circuit may include a transmitter and a receiver or a transceiver, a power line communication (PLC) transceiver 630, and a line driver 640. Measurement data is supplied to the PLC transceiver 630 and are coded for PLC transmission on the  
20 PLC network 3. The PLC transceiver 630 operates a line driver 640. The line driver 640 places the measurement data as PLC coded signals on lines 641 and 643 according to a network protocol.

The PLC coded signals are supplied by the retrofit plug to the external power circuit that supplies power to the appliance. The control server 100 monitors the external  
25 power circuit to receive the PLC coded signals. In this way, the control server 100 can monitor appliances connected to the external power circuit and the appliances can exchange data with the control server 100 or other appliances connected to the network.

The control server 100 or a remote monitoring service is able to perform diagnostic interpretation about the appliance 130. In this manner, the BC system can  
30 determine the health of the appliance, the appliance's current function (e.g., how many burners are on, oven capacity, temperature monitoring in a refrigerator, and washer and drier cycles including length), and device failure (including cause). For example, if a current signature or power usage for the light bulb in a refrigerator is detected as being active over an extended period of time, the control server 100 can determine that an open

door condition exists and can generate a message for display on an interface 150 to alert the user to shut the door.

The retrofit plug 125 also can include a power-switching device under control of the measure and transmit circuit 620. The power-switching device enables remote shutdown of the attached appliance, for example, through the retrofit plug 125, if a situation occurs that may damage the appliance if operation is continued or if a hazardous condition may result from continued operation. The power-switching device also can permit dimming and variable current flow regulation for remote control of the appliance.

The retrofit plug 125 can be designed specifically for a particular appliance. As a result, the retrofit plug 125 can perform sophisticated diagnosis, monitoring, and control specific to the appliance. Alternatively, the retrofit plug 125 can contain sufficient memory that control data or programs can be downloaded to the plug from the control server 100 through the PLC network. The software and data may be provided directly by the service provider. Software also may be installed in the field using a flash memory chip that is inserted into the retrofit plug 125.

As shown in Fig. 6C, an optional battery 655 can be connected with the power supply 650 to provide power to components of the retrofit plug in the event that power is lost. The battery may be a rechargeable battery that charges while the retrofit plug is supplied with power, if the battery is not in a fully charged state.

A serial port or other communications interface also can be provided in the retrofit plug to provide additional communication capabilities. The serial interface may be used for connection with another sensor to provide additional data about the device connected to the retrofit plug 125. The additional data can be transmitted to a remote monitoring device using the PLC network.

Other types of communications media also can be supported by the retrofit plug. As shown in Fig. 6C a modem 670 is provided within the retrofit plug 125 to provide communication to a network through a phone line. Alternatively, a wireless modem could be used for remotely located appliances where a phone line may not be available. The processor in the measure and transmit circuit 620 handles modem dial-up to an external network and provides buffering for the two-way data transfer on line 671. A phone line can be attached to the data transfer line 671 by adding a RJ connector in the housing of the retrofit plug 125. The modem 670 does not have to be included within the retrofit plug 125, instead, the modem can be a snap-on attachment to the retrofit plug 125.

As an example, the modified retrofit plug with serial port and modem can be used to monitor a commercial freezer. A retrofit plug 125 is installed on the main power supply to the freezer. In addition, a temperature sensor is fitted inside the freezer compartment to measure the freezer's interior temperature. The temperature sensor is attached to the retrofit plug 125 using the serial port. The battery provides power capability to the retrofit plug 125 and its components. In addition, the retrofit plug 125 has a telephone modem. In this case, if the main power supplied to the freezer fails and the freezer temperature approaches 32 degrees, the retrofit plug 125 can sense the rise in temperature using the remote temperature sensor and dial the operator or monitoring service to alert that food spoilage is possible.

### **Operator Interfaces**

Operator interfaces that can be used with the BC system include, for example, single room touch pad, small touchpad, standard touchpad, portable tablet, PC, and web enabled phones. In general, the look and feel of the operator interfaces is consistent between each interface where possible, and may look as is shown in Figs. 7A-7C.

#### Single Room Touchpad

The single room touchpad is basic in design and is intended for installation into a standard light switch box. The touch pad is capable of controlling at least two functions such as temperature and lighting. The single room touchpad also can accommodate an intercom for communication between rooms in the home. Through use of RF or PLC communications, the touchpad may be sized to fit in a standard switch box for ease of installation and integration.

#### Small Touchpad

The basic functionality of the small touchpad is that of a home automation system controller or room controller. Where appropriate, colors and sounds can be used to catch a person's attention or to signal an alarm. An exemplary small touchpad 154 is shown in Fig. 7A.

The small touchpad 154 includes a display, such as, for example, a 2.6" color TFT display. The display 701 shows the controls for lighting in a room. A room selection bar 702 displays the area that the small touchpad is being used to control. An arrow button 703 allows the user to switch between multiple areas. Control bars are used to control

appliances within the area, such as, for example, a control bar 705 for overhead lighting and a control bar 708 for a table light. The amount of overhead lighting can be adjusted by selecting the + or – buttons 706 and 707 on the display. The side table light 1 can be turned on or off using the buttons 709 and 710 on control bar 708. Additional control bars, if any, can be accessed by using the down arrow 711. A back button 712 navigates the user to the previous display. Selections can be made by touching the screen using a stylus, a finger, or the like. Three buttons are provided for controlling the display of the small touchpad 154.

### 10        Standard Touchpad

The standard touchpad 152 is a sophisticated operator interface designed for more enhanced presentation of information. The standard touchpad includes a 4 inch, 320 x 240 pixel personal data assistant (PDA)-style display and is capable of displaying video images as well as textual or icon based images. It is also capable of presenting web content in the manner of alerts or breaking news items. The standard touchpad 152 provides alarm and alert notification by means of color and sound, examples of which are:

Red-Flashing with buzzer – extreme alarm such as fire or intrusion detection;

Red with beeper – alarm such as system fault or pre-defined alarm condition (the two year old has entered the pool area);

Yellow with beeper – general alert such as hurricane warning or other weather or news advisory; and

Green with low level beeper – general information, such as clothes are ready from the dryer.

Being more sophisticated, the standard touchpad 152, which may be the only operator interface available, is not bound to controlling a single portion or subset of the BC system, and, instead, is capable of looking at the whole environment controlled by the BC system. It also is capable of configuring the system. An option for video display allows the standard touchpad 152 to present low-grade camera images such as, for example, from a camera positioned at the front door. A speaker and microphone can be included to provide an intercom with the video feature.

The standard touchpad 152 builds on the display of the small touchpad 154. The standard touchpad includes a display 731. A room selection bar 732 appears at the top of the display. The user may switch between rooms using the arrow button 733. Multiple

control bars 735-738 also are displayed. Additional control bars can be accessed by using the down arrow 741. A back button 742 is provided for navigating back to the previous display window. Four keypad input buttons 744 are provided for immediate navigation to preset display windows and to manipulate the display window 731.

5           The standard touchpad 752 can be mounted onto a wall and hard wired. The standard touchpad 752 also can be used as a portable unit having a cradle for storing and re-charging the unit when not in use.

#### Portable tablet

10           A portable tablet 150 can be used to communicate with the BC system provided that required connectivity options are available. The portable tablet 150 is used to present all aspects of the standard touchpad devices as well as more detailed configuration options. In addition, the portable tablet provides video and web browsing capabilities. The portable table may have a 12" display and may be used in the distributed video  
15 network to control all televisions and video devices. As a result, a parent could use the portable tablet to flash a message on the children's TV – "its time for dinner." The portable tablet may be implemented using a web pad.

          The web pad interface includes an applications bar 756 that allows the user to switch between the various applications supported by the BC system. A tool bar 75 for  
20 selecting specific features, such as, for example, a particular appliance to control, is provided on the top of the display. A room selector arrow 753 also is provided. The portable table 150 is able to display a number of control bars (754, 755). A down arrow 758 provides selection of additional control bars associated with the appliance, if necessary. A back button 757 is also provided to move to the previous display screen.

25

### Video Distribution Network

As shown in Fig. 8, a BC system includes a control server 100 connected to a number of primary networks including: an Ethernet LAN 1, a PLC LAN 3, an RF LAN 4, an RS485 LAN, a WAN (connected by a POTS or ISDN line), and a video distribution network 2. The video distribution network 2 includes a AvCast daughter board 180, a media caster module 810, a cable caster module 820, and a web caster module 830. The AvCast daughter board 180 plugs into a slot on the control server 100. The AvCast daughter board 180 can include the following interfaces: video out/VGA out, video in, dual USB – printer, keyboard/mouse interface, IR interface, and PCMCIA slot (optional). The video board provides video I/O as well as IR command transmission. A keyboard and mouse combination can be used with the video board through a USB or USB-to-RF interface (in the case of a wireless keyboard or mouse). A second USB connector can interface with printers, digital cameras, and other peripheral equipment. Functionally, the board accepts video input and digitizes the video for use by the rest of the BC system using the MPEG4 standard. The video board also provides video output as a TV channel for broadcast on connected televisions within the home.

The media caster module 810 is a digitally-tuned audio-video modulator with user-selectable UHF or CATV channels. The media caster module 810 is individually addressable. The media caster module 810 allows signals from the control server 100 to be displayed on TVs 182 by converting the video output from the control server 100 to a TV channel. The resulting converted signal can be distributed to a number of TVs 182 using the cable caster module 820. Using the output TV channel, the control server 100 can broadcast video data, virtual control panels, security camera video output, messages, alarms, and control interfaces to any connected BC system interface.

The cable caster module 820 provides bi-directional signal-splitting with 6 dB of amplification to compensate for cable loss. The cable caster module 820 distributes a video signal feed to any connected TV 182 while providing enough amplification to ensure crisp TV pictures despite long cable runs and signal-splitting.

The web caster module 830 converts SVGA and audio inputs to a TV signal. The converted signal can be distributed to multiple TVs 182 and interfaces (e.g., 190 or 150) using the cable caster module 820. The web caster module 830 allows the data displayed on a PC screen 190 to be viewed on a TV 182. As a result, the TV 182 can be used as a second monitor for viewing, for example, web pages.

A gateway 105 offers broadband connection to a CATV system. The gateway 105 connects with the control server 100 through the high-speed Ethernet link 1 using, for example, a Cat5 cable. When used with the video distribution network 2, video signals can be routed through the media caster module 810 and cable caster module 820 to other  
5 TVs 182 using standard co-axial cable. In addition, the video signal from the gateway 105 can be fed directly into the cable caster module 820 for distribution by co-axial cable throughout a building.

The gateway 105 provides a high-speed link enabling services such as, for example, video on demand, from the CATV connection. The high-speed link also  
10 provides a fast Internet connection for browser software running on the portable tablet 150 or the 90. Services, such as teleshopping, can be provided through the video distribution network 2, if supported by the cable service provider. The gateway 105 also provides a high-speed data link to the rest of the home network 1 supporting real-time video capability. The gateway 105 can be implemented as a standalone unit or as a plug-  
15 in module in the control server.

### **Smart Appliances**

Smart appliances (e.g., 135) are network ready appliances that can be connected to the BC system without additional modification or interfaces. Once connected to the BC  
20 system, a smart appliance can be controlled by the control server 100. In addition, the smart appliance can be remotely controlled through use of a virtual control panel displayed on a BC system interface, such as a portable tablet 150. A smart appliance has either a communications module or a smart module that connects to the internal appliance controller to provide compatibility with the control server 100. The smart module and  
25 virtual control panel are described in detail in copending U.S. Application No. 09/378,509, titled "DISTRIBUTED LIFE CYCLE DEVELOPMENT TOOL FOR CONTROLS" which is incorporated by reference in its entirety.

### **Retrofit Damper**

A wireless forced air damper for zoned HVAC control is shown in Fig. 9. The  
30 damper 900 is available in industry standard sizes to replace floor, wall, or ceiling registers. The damper 900 communicates with a smart HVAC zone controller 133 using wireless RF communications signals 901. A sensor 910 can be placed in the area serviced by the damper 900 to report local conditions to the zone controller 133. The sensor 910



communicates through the RF network 3, the PLC network 4, or through direct wiring to controller 133. Alternatively, the sensor 910 can be included in the damper 900 as described below. Additionally the sensor can be a wireless sensor 915. The zone controller 133 can be implemented as a stand-alone unit. Alternatively, the zone controller 133 can be supervised by the control server 100. If incorporated in the BC system, the zone controller 133 can be controlled by any of the BC system interfaces, such as the portable tablet 150. In addition, home manager software can be used to control zone controller 133 according to a number of predetermined modes of operation. Thermostats can be provided to provide user control of individual zones within a building. Existing wired thermostats 155 can be coupled to the zone controller to allow user control of the HVAC system. Additionally, wireless thermostats 157 can also be used. The wireless sensor 915 and thermostat 157 can be incorporated into a single unit.

A block diagram of a damper 900 is shown in Fig. 10. The damper 900 includes a register 1010 for controlling air flow through the damper 900. An RF transceiver 1050 receives control signals 901 from the zone controller 133 and transmits status/sensed data to the zone controller 133. A power supply 1030, such as, for example, a battery or other self-contained power source, powers the damper's electrical components so that the damper is self-contained and does not require any additional wiring for power. A mechanism 1020, such as, for example, a solenoid, a spring, a shape memory wire, or a magnetic latching mechanism, is coupled to the register 1010. The mechanism 1020 actuates the register to allow air flow in response to a signal received from the controller 1040. A magnetic switch or latching mechanism having thousands of latching cycles may be used as the mechanism 1020 to reduce power consumption and to extend the operational life of the damper between replacing/recharging of the power supply 1030. For example, the latching system can have one or two magnets. A capacitor can be charged from the battery using a trickle charge. In response to a control signal the capacitor can cause an induction, which actuates the magnet that holds register in one operation state. A second magnet or gravity may be used to return the register to its other operational state. A variable mechanism also may be used to control the register such that the register can be partially opened to regulate air flow (e.g., 100% open, 80% open, 50% open, and closed).

The controller 1040 can monitor the power supply 1030. When the power supply 1030 reaches a minimum charge threshold, the register 1010 is placed in an open state so that the register 1010 is left in the open position if power fails. In addition, the controller

1040 may notify the zone controller 133 that the power supply has reached a minimum threshold. Once notified, the zone controller 133 alerts the user that the power supply 1030 needs to be replaced/recharged. Alternatively, the zone controller 133 may poll the damper 900 to send a measurement of the power supply's remaining charge to the zone controller 133. Upon receipt of the measurement, the zone controller 133 performs the threshold analysis and alerts the user if necessary. A cover or door that is accessible from the room is provided to ease access to the power supply 1030.

When the fan unit on the air conditioner or the furnace is on, or when a preset condition occurs, the zone controller broadcasts a control signal to the controller 1040 to cause the mechanism to activate the register 1010. In addition, the zone controller 133 may selectively open or close dampers 900 based on a control program, a mode of operation, or upon a request from a user interface. Drain on the charge of the damper's power supply 1030 may be reduced by waiting until air flow has stopped before closing the register 1010 to limit the force needed to close the register 1010. A sensor 1060 may be connected to the controller 1040 to measure temperature at the damper 900. The measurement is supplied to the zone controller 133 as input to zone and comfort control software operating in the zone controller 133 or the control server 100.

The zone controller 133 is shown in Fig. 11. The zone controller 133 can be implemented using a universal controller 110. The zone controller 133 includes a processor 1110 for controlling and monitoring the dampers 900. A memory 1120 is provided to store climate control software and for operation and identification of the dampers 900. An RF transceiver 1130 transmits control commands to and receives responses from the dampers in response to the commands. The dampers 900 are periodically polled by the zone controller 133 for status and sensor data. The data can be stored in the memory 1120 for analysis by the processor 1110 or the data may be transmitted to the control server 100 for storage and analysis. If no response is received from a damper 900 after being polled a number of times, the zone controller 133 notifies the user or control server 100 that the damper 900 is not responding and may need servicing. An optional I/O interface 1140 is provided for connection with external sensors 910. An RS-232 interface 1150 allows peripheral equipment, such as a handheld unit or a modem, to be connected to the zone controller 133. An RS-485 interface 1160 is provided to connect the zone controller 133 with the control server 100.

Each damper 900 is assigned a unique HVAC control ID number. The zone controller 133 uses the control ID number to identify a damper. Each installed damper

900 is dedicated to a single zone controller 133 and rejects interference from any other controllers, unless released by an authorized security code stored in the damper 900. Initial configuration of the dampers 900 can be accomplished according to one of the following methods.

5           According to a first method, zone controller 133 is placed in an initialization mode. Once the zone controller 133 has been placed in the initialization mode, the dampers 900 can be powered up one at a time. Upon powering up, a damper 900 broadcasts a message with the control ID to the zone controller 133. Configuration software in the zone controller 133 acknowledges the received broadcast message, stores  
10 the control ID, and prompts the user to identify the location of the damper. After the user enters the location, the zone controller 133 awaits receipt of the next initialization message and repeats the process until the locations of all dampers 900 are identified.

          According to another method, barcodes can be used to configure the dampers 900 upon installation. When the damper is installed, a barcode on the damper 900 is scanned  
15 using a handheld device with a barcode reader. The barcode encodes the control ID for the damper 900. After reading the barcode, the handheld device prompts the installer to enter the location of the damper 900. The handheld device then associates the control ID with the entered location and stores this information in a table. Alternatively, barcodes identifying predetermined locations are placed in corresponding slots that accommodate  
20 the dampers 900. The installer scans the barcode in a slot using the handheld device. The installer then scans a barcode on the damper to read the damper's control ID and associates the damper with the location. After installation of the dampers, the damper control ID and the location data are downloaded to the zone controller 133 by connecting the handheld device to a port on the zone control 133.

25           According to another method, a barcode identifying the damper's control ID number can be peeled off the damper and placed on a location sheet. The sheet is scanned to determine a damper's control ID number and location. Once scanned, the data is downloaded to the zone controller 133.

          After configuration of the dampers, according to any of the methods described  
30 above, the zone controller 133 controls the damper units 900 through RF control signals according to the instructions of the zone controller's operational programming. The zone controller 133 can broadcast control messages that are addressed to all dampers, to a set of dampers, or to a specific damper using the control ID numbers.

The above-described system is not limited to dampers. The control system could be applied to other flow control devices, such as hydronic systems using, for example, a valve instead of a register. Although the actuation devices and flow control mechanisms would be specific to the environment, the control circuitry and operation would be  
5 substantially the same.

### ***HOME MANAGER SOFTWARE***

The home manager software incorporates a number of fundamental modes of operation. Six exemplary modes are: a stay mode, an away mode, a bedtime mode, a  
10 sleep mode, a vacation mode, a wake-up mode, and a custom mode. The stay mode is configured to operate when the home is occupied. In this mode, certain aspects of the home, such as comfort control, are set automatically by the home manager. Other aspects, such as lighting scenes, are independent of the mode and are set either by the occupant or based on time of day occurrences.

15 The away mode implies that the home is occupied but no one currently is at home. When operating in the away mode, the BC system can override other programming, such as, for example, lighting control, to simulate occupancy and to arm the security system. During operation in the away mode, other system operations, such as energy saving control, can conserve energy by cutting back on hot water or comfort settings.

20 A bedtime mode (not to be confused with a sleep mode described below) can be incorporated in homes that have children. The bedtime mode is used when the children have gone to bed but there are still one or more adults awake in the home. Bedtime mode activates certain monitoring systems, such as, for example, child monitoring, checking to make sure certain televisions and other entertainment devices are off, and alerting the  
25 adults if certain lights come on (e.g., the children's rooms or bathrooms). Using this mode, parents can monitor sleeping children or be alerted when children wake up.

Sleep mode is used to put the house to sleep. While in sleep mode, the BC system arms the security system, and ensures that all doors are closed and locked, all lights and appliances are off, and that comfort settings are altered appropriately.

30 Vacation mode provides an enhanced state of security when a family is away from the home for an extended period of time. In this mode, lighting and entertainment systems may be used to simulate occupancy. Energy hungry systems, such as, for example, comfort control and hot water, may be reduced to minimum settings. Appliances may be monitored for unnatural activity, such as, for example, activation of

the coffee pot (which normally would not switch on in the morning if the family were on vacation). However, the vacation mode can make allowances for house sitters who periodically bring in the mail or check on the house.

Wake-up mode is a choreographed schedule of events that happens as the house  
5 leaves sleep mode and enters stay mode. A number of timed events take place in the  
wake-up mode that can be customized for any particular residence. For example, prior to  
the alarm clock going off, comfort settings can be altered. If an HVAC zoning system is  
in place, the comfort settings can be adjusted in bedrooms and bathrooms first. Wake-up  
mode then increases the setting for the hot water heater, turns on the coffee pot, and  
10 adjusts other home systems in preparation for a family getting out of bed. A typical  
wake-up schedule would include: determine wake-up time based on day and weather,  
increase hot water temperature, increase temperature in bathrooms, shut off electric  
blankets, turn on the coffee pot, ramp up lights to simulate sunrise, activate wake-up  
alarm, turn on televisions for news, adjust comfort control for whole house. This list is  
15 exemplary and not comprehensive as any particular residence has a unique sequence of  
events. Other features can be programmed into the mode as desired by either the user or  
the service provider.

Custom modes also may be provided these modes may be programmed by the  
user, downloaded from a service provider over the Internet, or field programmed by a  
20 service provider technician on site.

There are a number of hidden modes that are invoked by features within the home  
manager. An example of a hidden mode is the fire mode. If a fire is detected by the  
security system, lights are adjusted to aid exit, doors are unlocked, gas to the house is shut  
off, the HVAC systems are shut down, and emergency numbers are called. Other hidden  
25 modes include: distress (robbery), medical emergency, and appliance failure.

Architecturally, each device connected to the BC system subscribes to the various  
features offered in the house manager modes through priority blocks. Each feature  
responding to a mode has an associated priority setting, for example, a security feature  
responding to a fire mode has a higher priority level than a bedtime mode setting. Fig. 12  
30 shows the relative positioning of the modes, the various features running on the system,  
the prioritization of each feature, and control of the field device. Features shown as  
custom may require additional programming to interface to the home management  
software.

Each feature also has an associated set of software functionality based on the hardware components available. The BC system automatically functions as described once the hardware is recognized by the BC system.

Enhanced security beyond that provided by a conventional security system is provided by the home manager. The enhanced security feature may supplement a conventional security system present in the home that is connected to the control server 100. Settings available in the enhanced security system include: armed/away mode, armed/stay mode, un-armed, system fault, medical emergency, police emergency, and fire emergency.

The settings for the security system relate to home manager modes in the following way. Both vacation mode and away mode invoke the away setting in the security panel. Both the armed/home and un-armed settings relate to the stay mode for the home manager. Although the armed/home setting does not relate directly to a specific mode, it can be set either by the existing security system or by the home manager on an individual basis.

The home manager can set or receive any of the armed/un-armed modes either locally or from a remote location (e.g., through a remote user or security service provider). Behavior of each of these sub-systems is described below.

#### Gas Shut-off Valve

In the fire emergency mode, the gas shut-off valve shuts-off the main gas supply to the house. This feature can be applied to any form of flammable fuel, such as natural gas, heating oil, or propane. In all other modes, the shut-off valve is in the normal state.

#### Water Shut-off Valve

In all modes, the shut-off valve is in the normal state.

#### Lighting Interface

In the armed/away setting, the lighting interface can be set to a pre-defined state. The predefined state can include setting individual lights on and off at prescribed times to simulated occupancy. To configure simulated occupancy, the lights are monitored for a period of one week, or as desired by the user. The light activity during this time is recorded by the control server 100 and captured according to a homeowner prompt to copy the activity. After the activity has been stored in the control server database, mode

the lights behave as they did during the recorded period whenever the security feature is placed in the away armed.

In the fire emergency mode, perimeter (outside) lights are set to flash at a 50% duty cycle with a 1 second cycle time to attract attention to the home. In addition, lights designated as exit lights are set to a level prescribed by the homeowner. During system configuration, lights are defined as exit lights, perimeter lights, or normal lights. In this way, the homeowner can establish an escape route using the lighting. All other lights are shut off.

In all other modes the lights are set in their normal state.

#### Door Locks

Doors are locked in the armed/away mode, and are unlocked in the medical emergency mode and the fire emergency mode. In all other modes, the door locks are in the normal state.

#### HVAC Interface

The HVAC interface can include communications to a sophisticated whole house HVAC zoning system or simply a connection to a programmable communicating thermostat. In the fire emergency mode, the HVAC system is shut down to prevent smoke from being distributed throughout the house. In all other modes, the HVAC system is in the normal state.

#### Health Monitoring

In the medical emergency mode, any health monitoring equipment that is connected to a person on a routine basis can be activated (if it isn't already). In all other modes, the monitoring equipment is in the normal state.

#### Child Detection

In the armed/stay mode, if a child is alone in the house, all cook tops are disabled from use without a password to unlock them. In the fire emergency mode, a security company is notified that a child is in the house. In all other modes, the child detection is in the normal state.

### Elder Tracking

In the medical emergency mode, the security company will be notified that a elderly or disabled person is in the house. In the fire emergency mode a security company is notified that an elderly or disabled person is in the house. In all other modes,  
5 the elder tracking is in the normal state.

### Security Cameras

Security cameras are accessible remotely by the BC system. The control server  
100 captures a camera image and digitizes it for local display or for access from a remote  
10 browser. Data compression can be used to save memory space. In the police emergency  
mode, the security cameras are automatically set to record on a suitable recording device,  
such as a VCR, if available. In all other modes, the security cameras are in the normal  
state.

### AVCast

In the fire emergency mode, all television sets in the house are set to the control  
server TV channel. The control server displays the message "FIRE" on the television  
screens. If a location of the fire is known, that location is also placed on the screen, for  
example, "FIRE – basement". In all other modes, the AVCast system is in the normal  
20 state.

### Away Mode Monitoring

Away mode monitoring is not to be confused with the Armed/Away mode  
described in the enhanced security section. Away mode monitoring relates to the ability  
25 to monitor or control the home while away. The home manager supports a number of  
different hardware methods for this task including a high-speed broadband connection as  
well as telephone dial-up. In either case, the control server 100 provides firewall  
protection against unauthorized access. Away mode monitoring is also supported by web  
enabled phones or phones with a mini-browser capability. Any device with a browser can  
30 be used to access the home manager to control or monitor any aspect in the home.

### Appliance Maintenance

Appliance maintenance allows for remote access of appliances within the home.  
Appliances can include, for example, any kitchen or laundry appliance, water heater,



HVAC system, lighting, audio/visual, sprinkler, or comfort control. Connectivity to each appliance is provided by a telephone modem or a broadband connection to the control server, or the like. The control server 100 acts as the interface to the appliances and serves as a firewall to prevent unwanted tampering. All appliance control functions  
5 available within the home are allowed from outside of the home provided that the user is authorized to do so. In the event that a catastrophic failure is detected, a service provider can shut-off gas or water to the house to prevent an explosion or water damage.

Some appliances are capable of a certain amount of self-diagnosis, such as detecting a clogged filter. Under these conditions, the appliances can prompt the user to  
10 initiate repairs by displaying a message on a local user interface. In other instances, the appliance must be diagnosed either remotely or by a service provider on site. The control server's role in appliance diagnosis is to provide access to data by a remote site and to provide any necessary service prompts locally. The service provider may shut off the appliance if continued operation would damage the appliance.

15

#### Enhanced Comfort

Enhanced comfort control involves any aspect of home automation that automatically improves personal comfort. A number of devices, when connected to the control server 100, can be incorporated into the enhanced comfort feature. Examples of  
20 such devices include HVAC control, programmable thermostats, a zone control system, ceiling fans, air filtering, humidity control, and automatic blinds.

HVAC control encompasses the broadest aspect of comfort control. HVAC control also can be impacted by an energy management or an enhanced security feature, if available. Programmable communicating thermostats provide the greatest impact on the  
25 ability to manage comfort in the home. Fundamentally, the home manager communicates with the thermostat and allows the homeowner to program and configure the thermostat. In addition, other features within the home manager are able to override or alter the actions of the thermostat if needed, for example, when the enhanced security system shuts down the air-blower in case of a fire. Under the energy management feature, the  
30 thermostat setting can be adjusted to shed load during high tariff conditions or when the home is unoccupied.

Zoning control is a feature that can provide benefit to virtually every home. There are always instances where one area of the home is hotter or colder than another area. A zoning system uses temperature sensors and variable dampers to adjust the temperature of

each zone independently. The home manager supports two forms of zoning: hardwired and wireless.

5 A hardwired zoning system involves dampers installed inside ductwork communicating to the control server through a central HVAC zoning package, or directly through PLC communications. Similarly, the temperature sensors are connected to the control server 100 either through PLC or through the zoning package.

In the case of a wireless zoning system, RF communications are used to communicate to all temperature sensors and dampers. In this instance, the retrofit damper described above can be incorporated.

10 Main HVAC control can be provided through direct connection from the control server 100 to the HVAC zone controller unit 133 or to a communicating thermostat, which in turn controls the packaged unit. If the control server 100 is taken off-line for some reason, the HVAC zone controller 133 or communicating thermostat can revert to a conventional operation mode.

15 Other devices, such as, for example, ceiling fans, humidifier/de-humidifiers, air filters, adjustable skylights, and automatic blinds can respond to an algorithm for comfort control implemented in the HVAC controller 110 or the control server 100.

#### Energy Savings

20 The primary method for achieving energy savings is to reduce settings or turn off large energy consuming appliances during non-critical times or peak tariff times. The away mode controlled by the home manager system can lower thermostats, reduce temperature of the hot water heater, coordinate HVAC and appliances based on peak tariff conditions by adjusting thermostats to appropriate extremes of the comfort zone, restricting use of appliances to off-peak times, using automatic blinds and skylights to  
25 reduce HVAC demand, and synchronizing HVAC and hot water heater control with the sleep mode by cutting back temperatures during sleep time and bringing them back up as part of the wake-up cycle.

### Family Manager

The family manager can be used in conjunction with the away mode monitoring to allow family members to connect to the system remotely. The family manager manages family data and automates certain tasks, such as, for example, maintaining the family calendar, maintaining a family address book, maintaining a family task list with alarms and reminders, and providing a kitchen/laundry assistant. The family manager is capable of being sorted and searched in a variety of different ways. A family member can access the entire family task list or just the member's personal tasks.

The family calendar contains events of the following profiles: single time events, periodic events (weekly, monthly, yearly), and alarmed events. Events can be assigned to one or more family members and carry details such as start time, end time, and priority. The family address book is segmented by family member and has annotations for entries related to, for example, family, business associates, service providers, theaters, and shops. Closely associated with the calendar is the task list. Tasks are assigned a degree of importance, time needed for completion, and family member assigned to the task.

The kitchen and laundry assistant centers around maintaining an inventory of products in the home such as food and laundry supplies. The assistant maintains shopping lists and supports e-grocery and e-commerce. A method for scanning products, such as barcode or RF ID, is supported to introduce new products into inventory and remove them when discarded. Discarding or use of an item can automatically prompt e-commerce services for re-stocking. The kitchen assistant focuses on meal preparation by recommending recipes or compliments based on products in inventory. The kitchen assistant also supports recipe instructions accessed from Internet sites. A screen shot of the cooking assistant is shown in Fig. 14.

### Home Automation

The home automation feature consists of a variety of modes that can be invoked from the stay mode, the bedtime mode, or the sleep mode. This feature consists of settings for groups of devices associated with certain activities. There are a number of default modes plus a set of user defined modes provided by this feature referred to as activity modes. Default activity modes include: television, reading, dinner, formal dinner, and party. The homeowner can add activity modes, such as, for example, gaming, for playing cards, or night swim, to turn on back yard lights.

**BC SYSTEMS****Meter Network**

The meter network and its link to the control server is explained with reference to  
5 Fig. 15. Water meter 1510 and heat meters (1520,1530) are connected with a bus 1501  
output that allows the meters to be networked via Cat5 cable to a bus master unit 1500.  
The bus master unit 1500 converts the bus signals to a format readable by the control  
server 100. The electricity meter 1540 has a pulse output that requires an additional bus  
coupler 1510. The bus coupler 1510 accumulates the pulses and allows connection to the  
10 bus 1501. Each coupler has pulse inputs for up to 4 meters. The bus 1501 has an open  
protocol such that any product that conforms to bus standards can be connected to the  
network.

Ideally the bus master unit 1500 is located in the same position within the house  
as the control server 100 and connects to the control server 100 through one of the control  
15 server's RS-232 ports.

The control server 100 allows each meter to be read by an authorised external data  
collection service. As a result, a wide variety of monitoring services can be offered, such  
as, for example, data collection, data analysis, and payment. Such services benefit the  
end-user through improved visibility of energy usage leading to better energy  
20 management. The home manager software can display energy consumption data and  
trends and to give tips for reducing consumption.

Energy DataVision (EDV) is an online data display package that enables energy  
users to monitor energy usage patterns via the web. IMServ's data collection service can  
remotely interrogates meters to access meter reads. Each meter has an identification  
25 number assigned to it. The monitoring services is given an access code to log into the  
control server 100 and use the EDV system to create a variety of reports regarding energy  
usage for the building. EDV can graph usage trends from month-to-month, day-to-day,  
date-to-date, hour-to-hour. An example of an EDV screen shot is shown in Fig. 16.

Commercial diagnosis analysis is shown in Fig. 17.

30

**Central Locking and Door Access System**

The central locking system, shown in Fig. 18, includes an RF key fob 1040, a  
receiver 1810, a motorized door bolt, and sensors to detect an open/closed door, door bolt  
position, and open/closed windows. A bus coupler 1830 is provided for connection to the

motorized door bolt. The motorized door bolt is activated and deactivated using the key fob 1840. The key fob 1840 transmits a lock signal and an unlock signal to the RF receiver 1810. The RF receiver relays the signals to the control server 100 to control one or more motorized door bolts. The motorized door bolts also can be controlled using  
5 other BC system interfaces, such as, for example, a portable tablet 150 (through control module 120), a PC interface 190, or through the Internet portal 5. A second bus coupler 1820 provides inputs from the window and door sensors to the control server 100 indicating an open/closed state of the doors and windows.

The control server 100 can interface with an existing door access system by using  
10 one of the bus coupler outputs to trigger the door controller (i.e., the opening/closing mechanism). The central locking system allows the user to check that all windows and doors are in the correct position before automatically locking them. The same key fob 1840 can be used with the door access system to open the common access door either from inside or outside the building. This reduces the number of keys that need to be used  
15 in any one location.

The key fob technology ensures security by appropriate coding. More than one key fob can be accommodated to allow each family member to have his or her own key. On activating the close function from the key fob, the control server 100 checks that all doors and windows connected to the system are closed. A warning is given (e.g., by  
20 continually flashing the door/hall lights) if the all sensors do not detect a closed position. If all doors and windows are closed, the system activates the locks. After the locks have been activated another check is performed and if all doors have successfully locked and indication is given (e.g., flashing the door/hall light once).

In the event of a power failure, the doors remain secure but in the event of a fire or  
25 other emergency they are easily opened from the inside and do not impede an escape route.

The home manager software for the control server 100 can include the central locking features.

### 30 House Security System

A home security network is shown in Fig. 19. The required sensors can be hardwired to an existing electronic security system 1900. The existing security system 1900 is linked into the control server 100 through a serial link 1901. Alternatively, RF controlled motion detectors 1900 and smoke detectors 1920 can send signals to the

control server 100 for analysis. The control server 100 provides telephone connection and web services that are need for the security system. The status of the security system can be monitored by a remote server using the Internet portal 5, dedicated ISDN, DSL, or POTS service, or any of the home interfaces, such as portable tablet 150 or PC interface  
5 190.

The existing network can be extended by adding the sensors to the appropriate LAN. In this case, the home manager software can be customized to provide specific system features tailored to the location. The security system using the control server 100 can perform all standard functions such as intruder alarm (through door and window  
10 switches or motion detectors) and alarm generation (either locally or remotely).

### Lighting System

A lighting network for use with the BC system is shown in Fig. 20. The lighting network comprises a lighting system LAN 2000. A number of bus couplers are  
15 connected to the lighting system LAN 2000. Each bus coupler is directly wired to a number of lamps, switches, or sensors. For example, bus couplers 2030 and 2040 are each dedicated to a lamp group, bus coupler 2020 receives signals from a number of switches, and bus couple 2010 receives inputs from sensors (e.g., motion and sun detectors). The bus couplers can be mounted in an electrical distribution box with the  
20 loads and inputs connected through a conventional mains cable.

The lighting system LAN 2000 can be implemented using an EIB or other LAN. The EIB LAN uses a bus converter to connect the LAN to the control server 100 using an available RS-232 port of the control server 100. The lighting network can operate even if the control server 100 has a failure. However, interaction with other systems, such as  
25 central locking or security, would not be available. A networked lighting system offers flexibility that allows the relationship between switch and lamp be changed simply by re-configuring the system. In addition, lamps, switches, and sensors attached to the lighting LAN 2000 can be shared and controlled by other systems connected to the control server 100. For example, the central locking system can put the house into standby mode when  
30 closed ensuring that no lights are left on when the house is empty. A light sensor can be used to detect sun rise and sun set so that the control server 100 can control the lights in a way to simulate occupation. Optionally, motion sensors can be used to switch lights off when a room is unoccupied or to switch them on when someone enters.

The lights also can be controlled using any of the BC system interfaces, such as, for example, PC 190, portable tablet 150 or through a remote interface connected through Internet portal 5.

5           Temperature Control System

A temperature control system is shown in Fig. 21. A heating LAN (e.g., an EIB LAN) can be used to control the temperature of rooms and provide zone control. The heating LAN connects the control server 100 to control valves, to room thermostats, and to room displays through a number of bus connectors. Alternatively, the heating LAN  
10 can be controlled by a universal controller 110 or a zone control 133 under supervision of the control server 100 (as described in the next section). As shown in Fig. 21, the control server 10 communicates with room thermostats through the heating LAN while bus couplers drive on/off valves, proportional valves, and dampers. Alternatively, RF controlled dampers and thermostats can be used as described above with regard to Figs.  
15 9-11.

Linking the heating LAN to the control server 100 gives access to the other systems so that, for example, the central locking system could put the heating system into standby mode when the house is locked. The window sensors used either by a central locking system or a security system can be used by the heating system to turn off room  
20 radiators when a window in the corresponding room is open for longer than a certain period of time.

A network of thermostats and valves allows a comprehensive software user interface offered by the home manager to effectuate zone and profile control.

25           Zone and Profile Temperature Control System

The universal controller 110 offers a very flexible temperature control system that can be linked to the control server 100. An LCD touch-pad 112 gives the user access to the system for changing temperatures, times, and other system management functions. The universal controller 110 is designed for mounting in an electrical distribution box.  
30 The box can be placed adjacent to the control server 100 or close to the valve/damper array for the heating system. The universal controller 110 links to the control server 100 using an RS-485 network interface.

The control panel 112 is wall mounted and connects to the universal controller through three sets of twisted-pair wires. Each universal controller 110 has up to 16

configurable analogue/digital inputs and twelve configurable relays output pairs. To add additional inputs and outputs a second universal controller 110 can be networked into the system. Up to three control panels can be placed at different positions around the home. An additional power supply allows two more control panels to be added if desired.

5           Once installed, the universal controller 110 needs to be configured. Configuration should be carried out by trained personnel using a PC running configuration software. The temperature control system allows up to 16 zones for either heating or cooling systems or 10 zones for combined heating and cooling. For example, each room in the house could be configured as a single zone. A temperature sensor in each room allows  
10 the user to set the required temperature and control the temperature controlling a valve/register to the room radiator feed or air damper. For combined heating and cooling systems, a valve is added to control the fan coil feed.

Each zone is programmed with a profile of temperatures by day of the week and time of day. As a result, only those rooms, which are normally occupied at particular  
15 times or days need be heated or cooled. The control panel 112 allows the user to override these profiles at a given time. The profiles can also be over-ridden by the control server 100 so that, for example, the heating system can be turned down if the central locking system reports that the house is locked and unoccupied. An outside air temperature sensor can be added to allow improved temperature control algorithms that  
20 account for ambient weather and temperature conditions.

The universal controller 110 can interface directly with a fire alarm system or individual smoke detectors allowing the universal controller to close all dampers and turn of the boiler and air circulating fan upon detection of a fire.

A wide variety of other sensors can be added to complement the functions offered  
25 by the system. For example, CO, CO2, flammable gas sensors could also be incorporated for home safety.

The universal controller 110 has a monitor function that allows current status of all connected devices to be viewed. The monitor function can be made available to the control server 100 and to any user interface (e.g., 150 or 190) connected to the control  
30 server 100, including a telephone connection. The home manager software can deliver a java file that is displayed using browser software on a local PC 190, or over a remote connection using Internet portal 5. An example of a screen shot for control of the HVAC is shown in Fig. 23.



### Networked Appliances

An appliance network is shown in Fig. 24. The networked appliances can communicate with the control server 100 using PLC LAN 3. An appliance is networked simply by plugging the appliance into the wall outlet connecting the appliance to the control server 100 through the PLC network. As a result, no additional wiring or re-  
5 configuring is necessary each time an appliance is installed or reconfigured.

Connecting appliances to the control server 100 provides a number of benefits due to the sharing of data with other networked devices and the connection to external service monitoring companies through a phone line or Internet connection.

The home manager software is able to display virtual control panels for each  
10 appliance as shown in Fig. 25. As a result, the appliance can be controlled remotely under the supervision and monitoring of a portable web pad 150 within the home, or from a remote location using the Internet portal 5. When combined with the AvCast option, the home manager pages can be displayed on the TV screens in the home. As a result,  
15 during advertisements, for example the user can switch to the oven channel to see how the roast is doing. The appliance's virtual control panel has the same appearance as the physical controls panel on the appliance.

Service companies can offer remote monitoring facilities to reduce the cost of repairs enabling them to offer extended warranty coverage for all such connected  
20 appliances.

### ***INTERACTIVE MARKETING***

According to another aspect of the BC system, users' actions may be monitored in order to provide better service to the users of the BC system. The BC system allows  
25 consumer and commercial marketing companies, for example, to understand what the users are doing in their homes at all times. An advantage of using the BC system to monitor consumer activity, is that the user is not required to fill out surveys, report data manually, or otherwise change patterns of daily behavior in order to permit the collection of data. In addition, the BC system allows diagnostic information to be gathered to  
30 improve operation of system components and build infrastructure systems within the premises.

Through use of the control server, communication modules, and monitoring components, such as a smart module or retrofit plug, data can be sent using the Internet portal, to service provider for monitoring and analysis. Using the diagnostic components

of the system, the monitoring company can monitor use of appliances, systems, and components within the home to determine exactly what activities are being performed by each appliance, including the exact time the appliances were used and the duration of the use. For example, a networked washer and dryer can be monitored by a service provider  
5 to determine what cycle the washer is in. When the cycle is finished the washer display or user interface, for example portable tablet can display a coupon for detergent, fabric softener, or anti-static dryer towels. If the appliance malfunctions, the control server can turn off the appliance before permanent harm is done and send a message to the user service provider that repair is required. In response, the service provider can supply  
10 instruction to the user for simple repairs that do not require a technician's assistance. In addition, merchants can monitor the appliance's usage in order to provide better warranties that are based on the specific customer's actual usage.

RF tags can be used to improve appliance performance. For example, RF tags can be included in clothing so that the appliance informs the user when clothes do not match  
15 the selected cycle. Coupons or and advertisement can be displayed for the type of clothes washed. For example, if delicates are being washed, a coupon for Woolite can be displayed. The advantage of the BC system over prior couponing systems is that the coupons can be displayed to the user when the user can take advantage of the coupon. Additionally, food RF tags can be monitored by control server to remind the user that  
20 certain food items are running low or are soon to expire or should be disposed of. At the same time, coupons can be sent and displayed to user of those items. Alternatively, a shopping list can be automatically generated and sent to a shopping delivery service so that the user does not even have to order or shop for designated items.

***TV CHANNEL RECORDER***

Techniques may be used to map the time of programming watched to identify exactly what the television was tuned to at any particular time. Because of the ability to catalog time and tuning the data logged by the control server 100, market researchers can determine what was being display based on the channel, location, and time. With this information, market researchers can precisely determined what information was displayed on the TV and determine specific viewing habits of a household. If personal RF tags, key fobs, or remote controls are also used then the control server 100 also can identify who was in the room when the TV was tuned to the channel and determine who was viewing a program or commercial.

Furthermore, the action of the TV channel recorder can be combined with an Internet activity recorder designed to monitor web surfing habits and PC usage habits. These features allow performance of web usage monitors of a nature substantially the same as the well known TV usage monitoring services, such as, for example, ACNielsen performs, but without intrusive use of logs or manual methods. It is even possible to link radio monitoring through a suitably adapted radio. The combination of TV monitoring, radio and/or PC usage monitoring, and in-home activity monitoring permits unsurpassed analysis of a household's economic activities. Prior to this, TV, PC, and home activity monitors were applied independently to various homes and statistical methods were used in an attempt to extrapolate the observed results to all homes of particular econometric groups.

No holistic, whole household view was possible because of the intense intrusion that the manual log methods imposed on a given household. A complete 360° view of household activity is possible (with permission from the household) with the BC system. The integrated data from the BC system capture all of the media influences being presented in electronic form. As a result, more sophisticated statistical analysis of household response to the media influences presented is permitted. True cause and effect analysis of advertising effectiveness can be performed, which are far superior to current methods.

In the final case, store point of sale data from participating local stores or RF tag data from tags attached to purchased goods or bar codes scanned from purchased goods can be used to close the loop on media influence measurement. Goods can be test marketed using various forms of promotion, including electronic and print media known to have been sent to a household, known to have been viewed, surfed or listened by

particular household members engaged in known activities at known times and the resulting effectiveness measured with unparalleled accuracy without the distorted effect of requiring manual logs of activities to be kept by the household participants.

5 ***RETROFIT REFRIGERATION MONITORING UNIT***

Figs. 26A and 26B show a refrigeration monitoring system. As shown in Fig. 26A, a refrigeration appliance 2600, such as, for example, a refrigerator or freezer, can be retrofitted to monitor for food properties, such as, for example, spoilage, and to alert the operator of the refrigeration appliance so that appropriate action can be taken, if  
10 necessary.

A refrigeration appliance 2600 can be retrofitted for monitoring by adding a retrofit plug 2650 (described above) to allow the appliance to communicate with a remotely located computer, such as, for example, a control server 100, a gateway, or a building monitoring service. The retrofit plug 2650 includes an alternative power source,  
15 such as a battery, that allows the plug to operate in the event of a power failure or outage at the location of the refrigeration appliance 2600. An LED indicator can be included on the outside of the retrofit plug 2650 to indicate a battery low condition. The retrofit plug 2650 also can monitor the power level of the battery and signal a monitoring service or user when the battery should be changed.

20 The refrigeration appliance 2600 includes a compartment 2610, such as, for example, a freezer or a refrigeration compartment. A sensor 2620 can be included or retrofitted to the refrigeration appliance 2600. The sensor 2620 can be retrofitted by drilling a hole in the appliance 2600 to allow placement of the sensor 2620, such as a thermistor or another temperature-sensing device, inside the compartment 2610. A  
25 special seal or ring (sized to the hole and including insulation characteristics) can be inserted in the hole to act as an anchor for the sensor 2620. A cable or interface connection 2621 couples the sensor 2620 to the retrofit plug 2650. The retrofit plug 2650 includes a serial or other port to accept the interface connection 2621. The sensor 2620 provides data on the sensed condition within the compartment 2610, for example,  
30 temperature, to allow the retrofit plug 2650 to monitor conditions within the refrigeration appliance 2600.

The retrofit plug 2650 can process the sensed condition and perform analysis of the data. In one example, the plug can be programmed to calculate the speed at which

temperature is rising in the appliance to determine how long it will be until food spoilage occurs. This information can then be provided to a user or monitoring service so that appropriate action can be taken. Alternatively, the sensed data can be sent to a control server 100, a gateway, or a monitoring service to perform the analysis function.

5 Temperature measurements can be taken in real time or at intervals designated by the user.

The retrofit plug 2650 can be installed by connecting the retrofit plug 2650 to the main power supply 2640 of the appliance controller 2630. During normal operation, the retrofit plug 2650 can use PLC communication to provide data about the refrigeration  
10 appliance. Alternatively, other communications interfaces can be used. The retrofit plug 2650 also may include a communications circuit implemented by a modem or a RF communication device. In the case of a modem, a phone jack and a communications port 2655 are provided as shown in Fig. 26B. In the event of a power failure, the retrofit plug 2650 can alert a user or monitoring service that power is out. The retrofit plug 2650 also  
15 may dial a repair service if it is determined that there is a malfunction within the refrigeration appliance 2600. The retrofit plug also monitors the temperature within compartment 2610 and can provide an estimation of how long until food spoilage occurs. The estimate can be updated if sensed conditions within the compartment 2610 change. The retrofit plug 2650 also can perform other analyses. For example, if it is determined  
20 that the compressor is on longer than expected, combined with a rising temperature in the compartment, the retrofit plug may determine that a door open condition has occurred and may provide a message to the user or monitoring service of the open door condition.

Even if power is not lost, if the compartment 2610 reaches a predetermined temperature, the retrofit plug 2650 may perform certain actions. For example, the retrofit  
25 plug 2650 may call using the modem, or transmit using the RF device, a monitoring service, the operator of the device, or a controller, such as a control server, to indicate that food spoilage is imminent or how long until spoilage will occur. Alternatively, a repair service can be contacted to fix the problem associated with the refrigeration appliance. The retrofit plug itself, as described above, can supply diagnostic data to aid in repair of  
30 the appliance, if necessary. In this way, food can be monitored and spoilage prevented to save an operator the cost of replacing the food. In addition, liability issues can be reduced by keeping records that although power was lost, or the refrigeration appliance malfunctioned, food temperature was maintained at an adequate level such that spoilage

did not occur. The retrofit plug 2650 may simply provide the temperature or other power monitoring data to a control server, gateway, or monitoring service, which can perform analysis of the data and determine if any action is necessary. For example, if used in conjunction with the control server 100, a message can be displayed on a user interface that the freezer is not working, the door has been left open, or that a repair service should be called.

As shown in Fig. 27A, in place of a retrofit a plug, a box 2700 can attach to the outside of refrigeration appliance 2600 (or the compartment 2610). According to one implementation, the unit 2700 can be implemented using a communications module (described above). In the implementation shown in Fig. 27A, a hole is cut and the unit with sensor 2705 is inserted into the hole. A suitable seal is provided to ensure adequate refrigeration is maintained. The unit 2700 can use the seal to seat itself on the refrigeration appliance 2600. Other means of fastening, such as, for example, adhesive, bolts, or screws also can be used. The seal may be inserted in the hole or be provided as part of the unit 2700 and sensor 2705.

The unit 2700 attaches to a power line 2601 to provide power to all components of the unit 2700. In addition, a back-up power source 2710, such as, for example, a battery is included to provide power in case of main power loss or outage. An external LED or some other indicator may be provided on the unit 2700 to alert the operator of a low battery condition.

A small processor or monitoring circuit 2720 monitors temperature inside the refrigeration appliance 2600. The monitor circuit 2720 is connected with a communications circuit 2730. The communications circuit 2730 can be implemented using, for example, a wireless transceiver, a wireless transmitter, or a modem. The communications circuit 2730 can include a phone jack for connection to a phone line 2735, if a modem is used. In the case of a temperature event, the unit 2700 is programmed (by external device such as a key pad with an interface, through the modem, or by insertion of a memory chip, such as a flash memory) with a number to call to alert an operator or monitoring company of the temperature or condition within the appliance, indicating that food spoilage will occur without intervention. Alternatively, if a wireless communication device is used, a message could be sent to a gateway, a control server, or a communication link to alert a user or monitoring service of the temperature event. The monitoring circuit 2730 also can be programmed to perform all of the monitoring function and analysis that is provided by the retrofit plug or communications module.

The sensor 2705 and unit 2700 also can be implemented as separate units connected by a cord or other interface 2704 as shown in Fig. 27B. The unit 2700 can be mounted on the refrigeration appliance 2600 using an adhesive or using a form of attachment, such as, for example, screws, bolts, or other means of fastening.

5 A number of implementations have been described. Nevertheless, it will be understood that various modifications may be made. For example, advantageous results still could be achieved if steps of the disclosed techniques were performed in a different order and/or if components in the disclosed systems were combined in a different manner and/or replaced or supplemented by other components. Accordingly, other  
10 implementations are within the scope of the following claims.

What is claimed is:

1. A device for monitoring an appliance that receives power from a power source, the device comprising:

a first coupler that couples the device to the power source;

a second coupler that couples the device to the appliance;

5 a monitoring circuit connected between the first coupler and the second coupler to monitor power supplied by the source to the appliance; and

a communications circuit connected to the monitoring circuit,

wherein the monitoring circuit provides data based on the monitored power to the communications circuit.

10

2. The device of claim 1 wherein the communications circuit includes a receiver that receives a signal from the first coupler to control the monitoring circuit.

3. The device of claim 1 wherein the communications circuit includes a transceiver  
15 that receives a signal from the first coupler to control the monitoring circuit and to transmit monitored power data.

4. The device of claim 1 wherein the communications circuit comprises a power line carrier transceiver and a power line driver coupled to the monitoring circuitry and the first  
20 coupler.

5. The device of claim 1 wherein the monitoring circuit measures current drawn by the appliance.

25 6. The device of claim 5 wherein the monitoring circuit includes a processor, that determines an operating state of the appliance based on the measured current.

7. The device of claim 5 wherein the monitoring circuit includes a memory that stores the measured current and periodically sends measured current data to the first  
30 coupler.

8. The device of claim 5 wherein the monitoring circuit includes a memory that stores an electronic signature and a processor that determines an operating state of the appliance based on the electronic signature.



9. The device of claim 8 wherein the processor determines an operating state of the appliance and transmits the determined state to the first coupler.

5 10. The device of claim 1 further comprising a modem connected to the monitoring circuit for transmitting data based on the measured current.

11. The device of claim 1 further comprising a radio frequency transmitter connected to the monitoring circuit for transmitting data based on the measured current.

10

12. The device of claim 1 further comprising a serial port connected to the monitoring circuit to receive data about the appliance.

13. The device of claim 1 further comprising a battery, wherein the monitoring circuit  
15 receives power from the first coupler and the battery supplies power to the monitoring circuit when power is not received by the first coupler.

14. The device of claim 2 further comprising a switch connected to the first coupler  
20 wherein the switch is opened in response to the control signal to prevent power from the source from being supplied to the appliance.

15. The device of claim 2 further comprising a switch connected to the first coupler to adjust the amount of power received by the appliance in response to the control signal.

25 16. The device of claim 1 wherein the first coupler comprises a first pin for connection to a live line and a second pin for connection to a neutral line.

17. The device of claim 16 further comprising a first power line and a second power  
30 line connecting the first and second couplers, wherein the second coupler includes a first slot connected to the first pin through the first power line and a second slot connected to the second pin through the second power line.

18. A system for monitoring an appliance that receives power from a source, the system comprising:

a power line connected to the source;

a circuit connected to the power line and the appliance to monitor power supplied to the appliance; and

a processor connected to the power line,

5 wherein the circuit sends a signal to the processor through the power line and the signal is based on the power supplied to the appliance.

19. The system of claim 18 wherein the circuit comprises:

a first coupler that couples the circuit to the power line;

10 a second coupler that couples the circuit to the appliance;

a monitoring circuit connected to the first coupler and the second coupler to monitor power supplied by the source to the appliance; and

a communications circuit connected to the monitoring circuit,

15 wherein the monitoring circuit provides data based on the monitored power to the communications circuit for output to the first coupler.

20. The system of claim 19 wherein the circuit comprises a plug and the first coupler comprises a first pin for connection to a live line and a second pin for connection to a neutral line.

20

21. The system of claim 20 wherein the monitoring circuit further comprises a first power line and a second power line connecting the first and second couplers, and the second coupler comprises a first and second slot, with the first slot connected to the first pin through the first power line and the second slot connected to the second pin through  
25 the second power line.

22. The system of claim 18 wherein the processor receives signals transmitted on the power line from the circuit and determines a state of operation of the appliance based on the signals.

30

23. The system of claim 18 wherein the circuit includes a receiver for receiving signals sent from the processor on the power line.

24. The system of claim 23 wherein the appliance's operating state is controlled based on the signals sent to the circuit from the processor.

25. The system of claim 22 further comprising a connection to a service provider,  
5 wherein the processor comprises a control server, that sends signals to the service provider about the operation of the appliance.

26. The system of claim 22 further comprising a connection to remote service  
10 provider, wherein the processor comprises a gateway, that sends signals to the service provider about the operation of the appliance.

27. The system of claim 22 wherein the processor diagnoses the signals to determine if an appliance service.

15 28. The system of claim 27 further comprising a display wherein the processor sends a message to the display alerting a user if the appliance needs service.

29. A device for monitoring an appliance that receives power from a source, the device comprising:

20 first means for coupling the device to the power source;

second means for coupling the device to the appliance;

means for monitoring power supplied to the appliance; and

means for communicating data based on the monitored power received from the  
monitoring means,

25 wherein the monitoring means provides the data to the communications means for output to the first coupling means.

30 30. The device of claim 29 wherein the communications means includes a receiver that receives a signal from the first coupling means to control the monitoring means.

31. The device of claim 29 wherein the communications means includes a transceiver that receives a signal from the first coupling means to control the monitoring means and to transmit monitored power data.

32. The device of claim 29 wherein the monitoring means measures current drawn by the appliance.

33. The device of claim 29 wherein the monitoring means determines power used by the appliance.

34. The device of claim 29 wherein the monitoring means determines an operating state of the appliance based on the power used by the appliance.

35. The device of claim 29 further comprising a means for switching connected to the first coupler to open in response to the control signal to inhibit power from the source from being supplied to the appliance.

36. A retrofit plug adapted to be received by an appliance that receives power from a source, the retrofit plug comprising:

a live pin;

a neutral pin;

a first line connected to the live pin;

a second line connected to the neutral pin;

a first slot, connected to the first line, for receiving a pin from the appliance;

a second slot, connected to the second line, for receiving a neutral pin from the appliance;

a transformer connected to monitor the first and second lines;

a measurement circuit connected to the transformer for measuring current supplied to the appliance; and

a power line carrier transceiver for encoding a power line carrier signal based on the measured current.

37. A wireless damper comprising:

a register;

a controller regulating the amount of air flow provided by the register; and

a radio frequency communications circuit,

wherein the radio frequency communications circuit provides a signal to the controller to adjust the amount of air flow provided by the register.

38. The damper of claim 37 further comprising a register regulation mechanism connected between the register and the controller, wherein the regulation mechanism opens and closes the register in response to a signal from the controller to regulate air flow through the damper.

5

39. The damper of claim 38 wherein the register regulation mechanism comprises a variable switch which variably adjusts the amount of air flow through the damper.

10

40. The damper of claim 38 wherein the register regulation mechanism comprises a magnetic latch which opens and closes the register.

15

41. The damper of claim 37 further comprising a battery that supplies power to the damper.

42. The damper of claim 41 wherein the controller monitors a power level of the battery and sends a signal for transmission by the radio frequency communications circuit when the power level reaches a predetermined amount.

20

43. The damper of claim 41 wherein the controller opens the register if a power level of the battery reaches the predetermined amount.

25

44. The damper of claim 38 further comprising a battery that supplies power to the controller, the register regulation mechanism, and the radio frequency communications circuit.

45. The damper of claim 38 further comprising a sensor for determining a condition at the damper.

30

46. The damper of claim 45 wherein the controller adjusts the register regulation mechanism in response to the condition determined by the sensor.

47. The damper of claim 46 wherein the controller receives the determined condition from the sensor and sends a signal with the determined condition to the radio frequency communications device for transmission of the determined condition signal.

5 48. The damper of claim 45 wherein the sensed condition is temperature.

49. The damper of claim 37 wherein the radio frequency communications circuit comprises a radio frequency transceiver.

10 50. The damper of claim 37 wherein the controller includes a processor that sends a signal to the radio frequency communications circuit to identify the damper.

15 51. The damper of claim 37 wherein the controller includes a processor that determines if a signal received by the radio frequency communications circuit is addressed to the damper.

20 52. The damper of claim 51 wherein the controller includes a memory for storing damper identification and the processor determines if a signal is addressed to the damper using the stored damper identification.

25 53. A wireless air flow control system comprising:  
a wireless damper including a battery; and  
a zone controller;  
wherein the zone controller sends a signal to the wireless damper to control the amount of air flow through the damper.

30 54. The wireless air flow control system of claim 53 wherein the wireless damper comprises:  
a register;  
a damper controller regulating the amount of air flow provided by the register; and  
a radio frequency communications circuit,  
wherein the radio frequency communications circuit receives the air flow control signal and the damper controller adjusts the amount of air flow in response to the air flow control signal.

55. The wireless air flow control system of claim 54 further comprising a register regulation mechanism connected between the register and the damper controller, wherein the regulation mechanism opens and closes the register in response to signals  
5 from the damper controller to regulate air flow through the damper.

56. The wireless air flow control system of claim 55 wherein the register regulation mechanism comprises a variable switch that adjusts the amount of air flow through the damper.  
10

57. The wireless air flow control system of claim 55 wherein the register regulation mechanism comprises a magnetic latch that opens and closes the register.

58. The wireless air flow control system of claim 54 wherein the damper controller monitors a power level of the battery and sends a signal for transmission by the radio frequency communications circuit to the zone controller when the power level reaches a predetermined amount.  
15

59. The wireless air flow control system of claim 58 further comprising a display on which the zone controller displays a message identifying that the damper's battery power level is low.  
20

60. The wireless air flow control system of claim 58 further comprising a display on which the zone controller displays a message identifying that the damper's battery needs replacing.  
25

61. The wireless air flow control system of claim 53 further comprising a sensor configured to sense a condition and provides an indication of the condition to the zone controller, wherein the zone controller sends a control signal to the wireless damper  
30 to regulate the air flow based on the sensed condition.

62. The wireless air flow control system of claim 53 further comprising a user interface that provides a signal to the zone controller which controls the damper in response to the signal from the user interface.

63. The wireless air flow control system of claim 62 wherein the user interface comprises a thermostat.

5 64. The wireless air flow control system of claim 62 wherein the user interface comprises a computer.

65. The wireless air flow control system of claim 54 further comprising a control server that controls the zone controller in coordination with other building  
10 functions under control of the control server.

66. The wireless air flow control system of claim 54 further comprising a building air flow generation mechanism wherein the zone controller opens and closes the damper in response to activation and deactivation of the air flow generation mechanism.

15 67. The wireless air flow control system of claim 54 wherein the damper controller includes a processor wherein the processor sends a signal to zone controller identifying the damper.

20 68. The wireless air flow control system of claim 54 wherein the damper controller includes a processor that determines if a signal received by the radio frequency communications circuit is addressed to the damper.

25 69. A wireless damper comprising:  
a means for regulating air flow;  
a means for controlling the amount of air flow provided by the air flow regulating means; and  
a means for communicating,  
wherein the means for communicating provides a signal to the control means to  
30 adjust the air flow.

70. The damper of claim 69 comprising a means for adjusting the air flow regulation means in response to signals from the control means.



71. The damper of claim 70 wherein the air flow adjusting means comprises a variable switch that adjusts the amount of air flow through the damper.

72. The damper of claim 70 wherein the air flow adjusting means comprises a magnetic latch, that opens and closes the air flow adjusting means.

73. The damper of claim 69 further comprising a means for supplying power to the damper.

74. The damper of claim 73 wherein the control means monitors a power level of the power supply means and sends a signal for transmission by the communication means when the power level reaches a predetermined amount.

75. The damper of claim 73 wherein the control means opens the air flow regulation means if a power level in the power supply means reaches a predetermined amount.

76. The damper of claim 69 comprising a means for sensing a condition at the damper.

77. The damper of claim 76 wherein the control means adjusts the air flow regulation means in response to the sensed condition.

78. The damper of claim 69 wherein the communications means comprises a radio frequency transceiver.

79. A refrigeration appliance comprising:  
a compartment,  
a sensor for sensing a condition within the compartment;  
a power supply;  
a monitoring circuit connected with the power supply monitoring the sensed condition; and  
a communications circuit,

wherein the monitoring circuit sends a signal through the communication circuit in response to the sensed condition.

80. The appliance of claim 79 wherein the compartment is a freezer.

5

81. The appliance of claim 79 wherein the sensed condition is temperature.

82. The appliance of claim 79 wherein the monitoring circuit includes a processor that determines when food spoilage will occur based on the sensed condition.

10

83. The appliance of claim 80 wherein the monitoring circuit sends a signal through the communications circuit indicating when food spoilage will occur.

84. The appliance of claim 80 wherein the monitoring circuit sends a signal through the communications circuit indicating food spoilage has occurred.

15

85. The appliance of claim 79 further comprising a battery connected to the monitoring circuit, wherein the monitoring circuit monitors power supplied to the appliance, and if power supplied is interrupted, sends a signal using the communications circuit.

20

86. The appliance of claim 85 wherein the signal indicates that no power is being supplied.

87. The appliance of claim 85 wherein the signal indicates when food spoilage will occur.

25

88. A retrofit unit for monitoring a refrigeration appliance including a power supply, the unit comprising:

30

a sensor for sensing a condition within the appliance;

a monitoring circuit connected with the power supply monitoring the sensed condition; and

a communications circuit,

wherein the unit is inserted in the appliance and the monitoring circuit sends a signal through the communication circuit in response to the sensed condition.

89. The retrofit unit of claim 88 wherein the sensed condition is temperature.

5

90. The retrofit unit of claim 88 wherein the monitoring circuit includes a processor that determines when food spoilage will occur based on the sensed condition.

91. The retrofit unit of claim 88 wherein the monitoring circuit sends a signal through the communications circuit indicating when food spoilage will occur.

10

92. The retrofit unit of claim 88 wherein the monitoring circuit sends a signal through the communications circuit indicating food spoilage has occurred.

15

93. The retrofit unit of claim 88 comprising a battery connected to the monitoring circuit wherein the monitoring circuit monitors power supplied to the appliance and if power supplied is interrupted the monitoring circuit sends a signal using the communications circuit.

20

94. The retrofit unit of claim 93 wherein the signal indicates that no power is being supplied.

95. The retrofit unit of claim 93 wherein the signal indicates when food spoilage will occur.

25

96. A retrofit system for monitoring a refrigeration appliance including a power supply, the system comprising:

a sensor for sensing a condition within the appliance;

a monitoring unit connected to the sensor and including:

30

a monitoring circuit connected with to the sensor to monitor the sensed condition; and

a communications circuit,

wherein the sensor is inserted in the appliance and the monitoring circuit sends a signal through the communication circuit in response to the sensed condition.

97. The retrofit system of claim 96 wherein the monitoring unit is mounted on the appliance and attached to the power supply.

5 98. The retrofit system of claim 96 wherein the sensed condition is temperature.

99. The retrofit system of claim 96 wherein the monitoring circuit includes a processor that determines when food spoilage will occur based on the sensed condition.

10

100. The retrofit system of claim 96 wherein the monitoring circuit sends a signal through the communications circuit to indicate that when food spoilage will occur.

15

101. The retrofit system of claim 96 wherein the monitoring circuit sends a signal through the communications circuit to indicate that food spoilage has occurred.

20

102. The retrofit system of claim 96 comprising a battery connected to the monitoring circuit, wherein the monitoring circuit monitors power supplied to the appliance, and if power supplied is interrupted, sends a signal using the communications circuit.

103. The retrofit system of claim 102 wherein the signal indicates that no power is being supplied.

25

104. The retrofit system of claim 102 wherein the signal indicates when food spoilage will occur.

30

105. A retrofit appliance monitoring system comprising:  
an appliance including a power supply;  
a retrofit plug attached to the power supply; and  
a sensor connected to the retrofit plug for sensing an appliance condition, wherein the retrofit plug generates a signal based on a sensed condition.

106. The retrofit appliance monitoring system of claim 105 further comprising:

a control server; and

a user interface;

wherein the control server displays a message on the interface in response to the signal from the sensor.

5

107 The retrofit appliance monitoring system of claim 106 wherein the sensed condition is temperature and the signal indicates how long until food spoilage occurs.

108. The retrofit appliance monitoring system of claim 107 wherein the sensed  
10 condition is temperature and the signal indicates that power has been lost.

109. A building control system comprising:

appliances;

a communications network connected to the appliances; and

15

a control server connected to the communications network,

wherein use of the appliances is monitored by the control server.

110. The building control system of claim 109 comprising a retrofit plug  
connected with one of the appliances for monitoring the appliance, wherein the retrofit  
20 plug sends monitored appliance data to the control server.

111. The building control system of claim 109 wherein the communications  
network is a power line carrier network.

25 112 The building control system of claim 111 wherein the control server  
includes building manager software that controls the appliances according to a number of  
modes of operation.

113. The building control system of claim 112 wherein the modes of operation  
30 are one of: a stay mode, a wake-up mode, a bedtime mode, a sleep mode, and a custom  
mode.

114. The building control system of claim 109 further comprises a video  
distribution network and display device.

115. The building control system of claim 114 wherein the control server includes a video module providing a video channel for display on the display device wherein the control server displays messages on the control channel.

5

116. The building control system of claim 114 wherein the control server includes a video module providing a video channel for display on the display device.

117. The building control system of claim 109 wherein the display device is a television and the control server records the view channel and time.

10

118. The building control system of claim 117 wherein the recorded data are used to determine what content is being viewed at a particular time.

15

119. The building control system of claim 118 including a radio frequency personal identification device, wherein the control server records the identification in relation to the recorded data to determine who was watching the content.

120. The building control system of claim 119 wherein the control server monitors items purchased and used in the home.

20

121. The building control system of claim 120 further comprising a monitoring service for receiving the monitored item information and the content viewing information to determine effectiveness of marketing advertisements.

25

122. The building control system of claim 109 comprising a radio frequency receiver, wherein the control server monitors items used in the building by reading radio frequency tags attached to the items.

123. The building control system of claim 109 further comprising a display, wherein the control server monitors use of one of the appliances and provides messages in response to the use of an appliance.

30

124. The building control system of claim 123 further comprising a monitoring service that monitors use of the appliances as reported by the control server.

5 125. The building control system of claim 123 wherein the messages are coupons for items used in the building.

10 126. The building control system of claim 109 further comprising a user interface, wherein the user can display a virtual control panel of one the appliances to control the appliance.

127. The building control system of claim 126 wherein the interface is a portable tablet.

15 128. The building control system of claim 126 wherein the interface is a computer.

20 129. The building control system of claim 109 wherein the communications network is a radio frequency network.

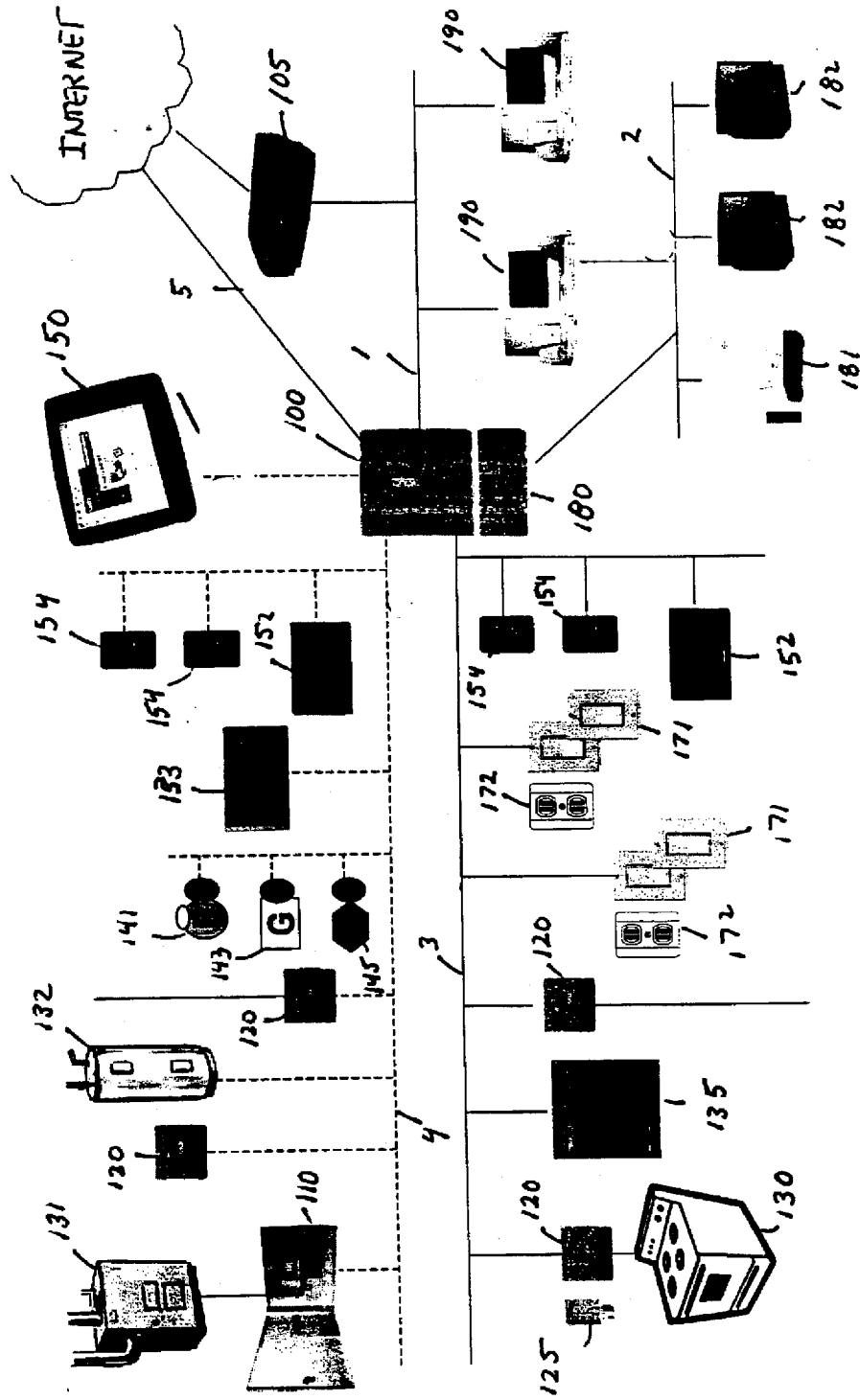


FIG. 1



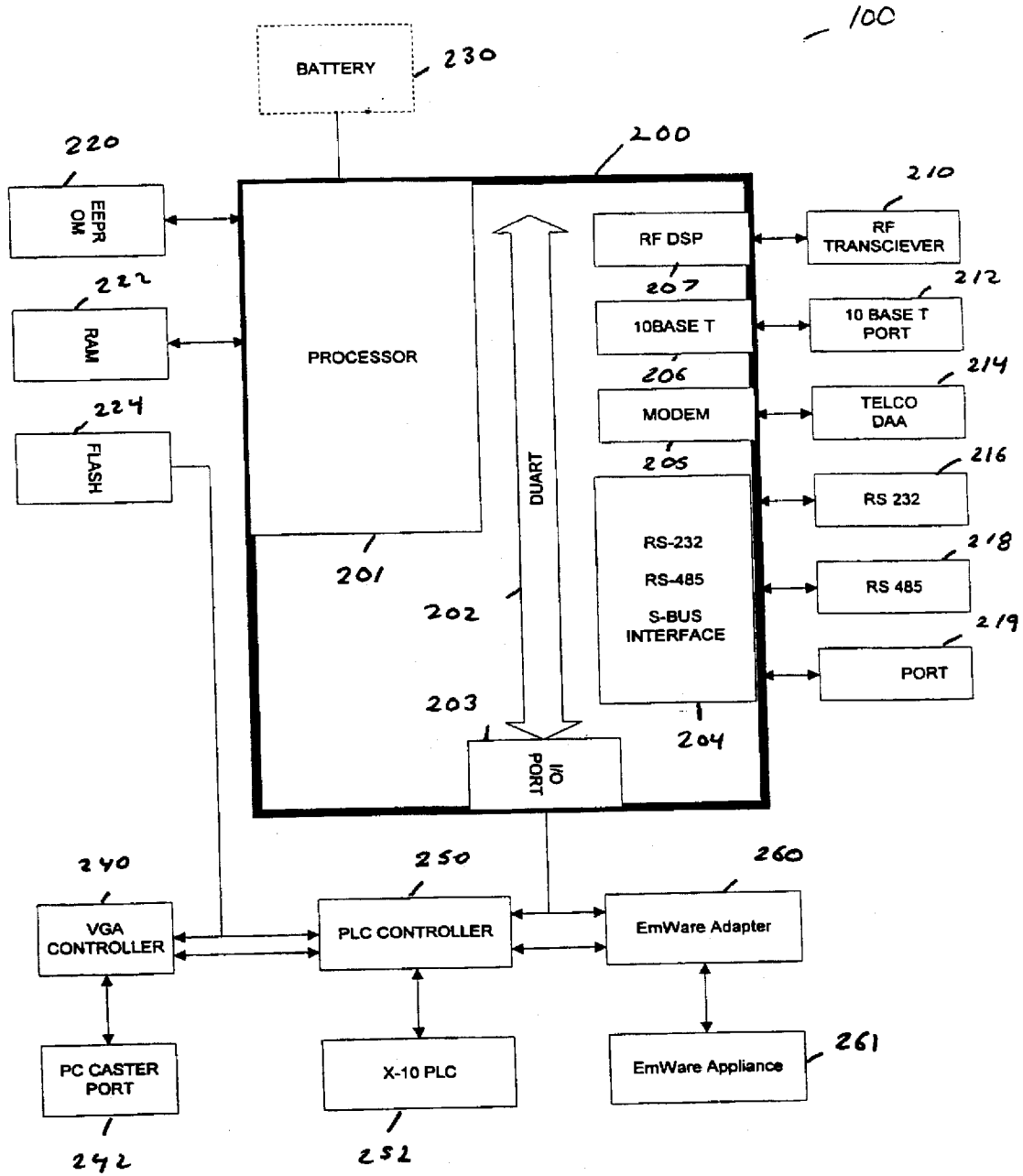


FIG. 2

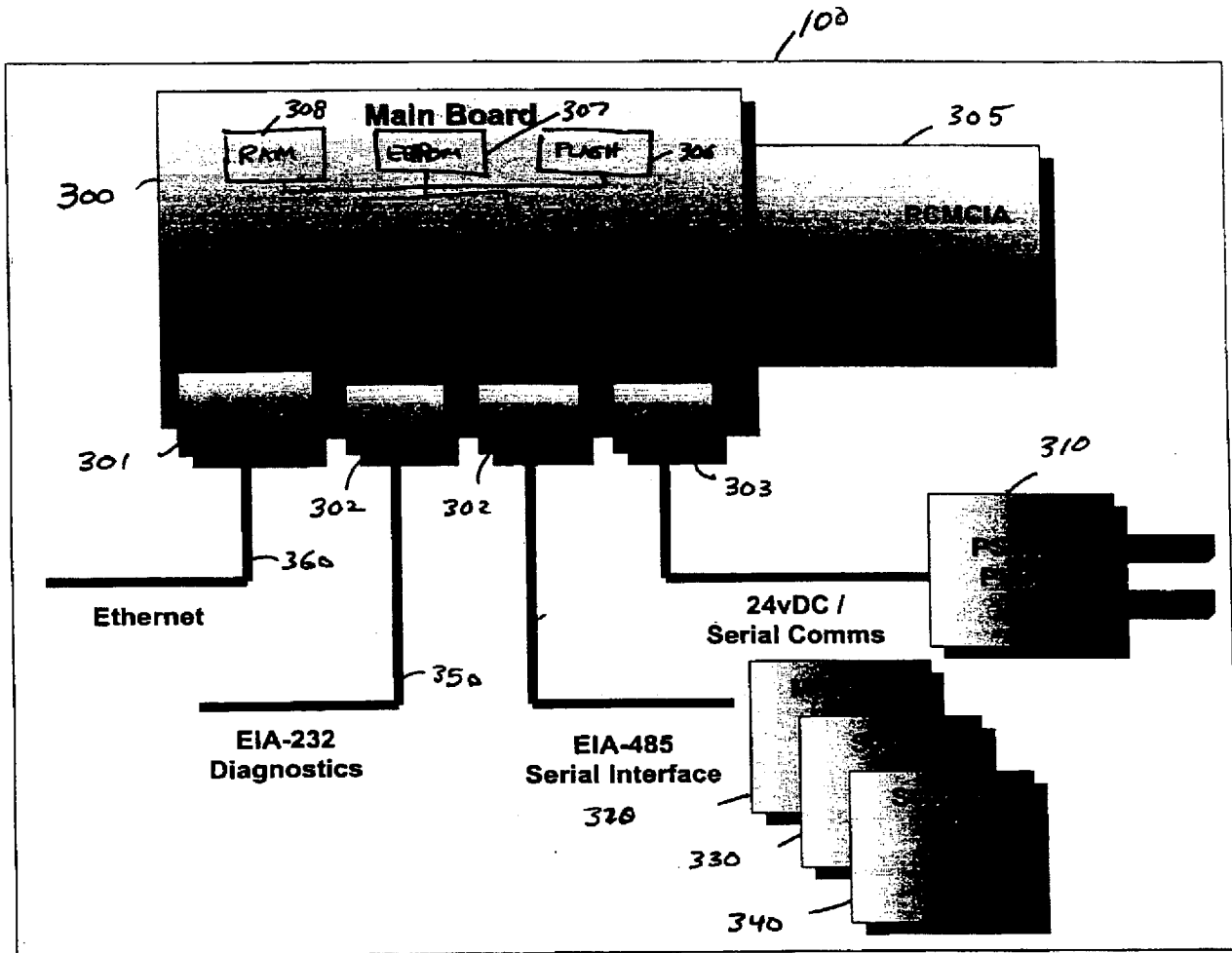


FIG. 3

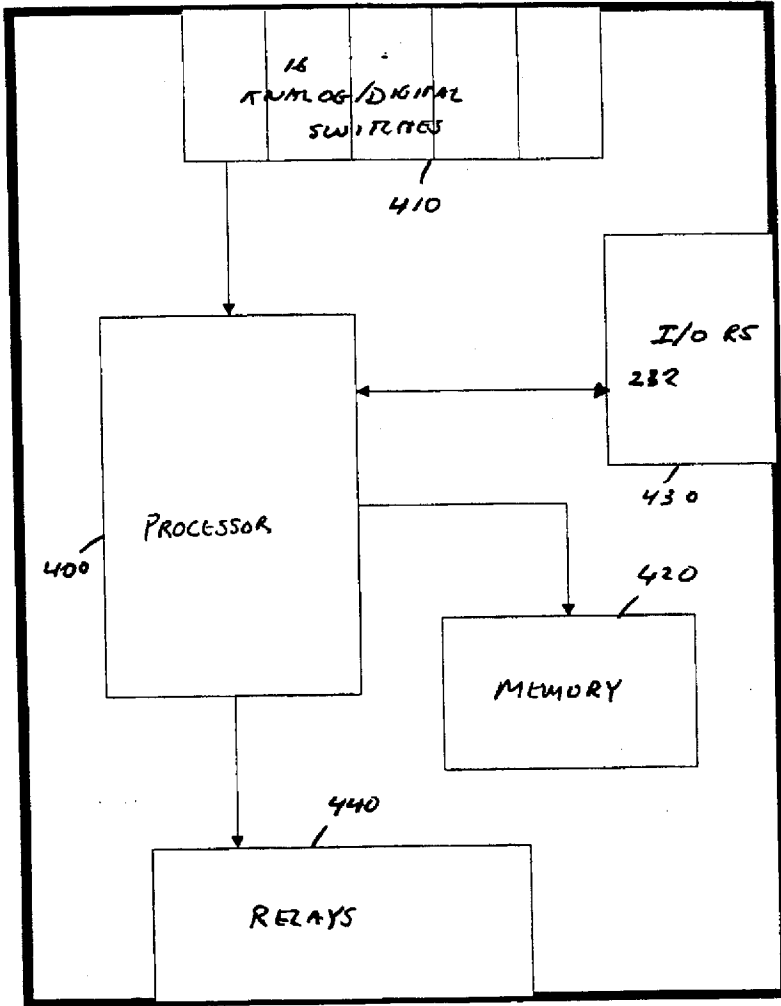


FIG. 4

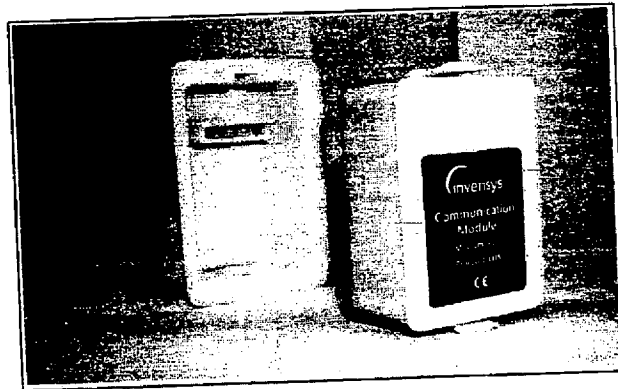


FIG. 5

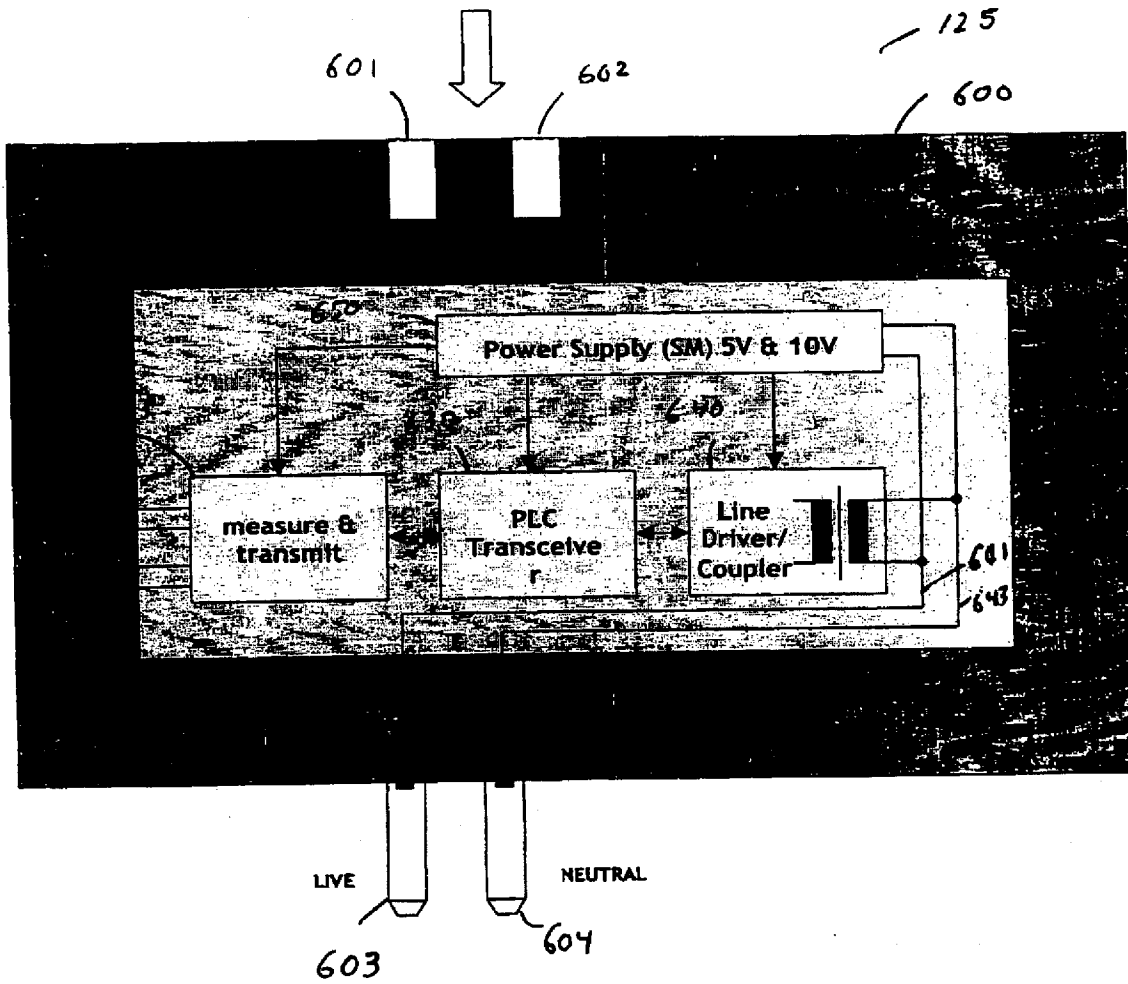


FIG. 5B

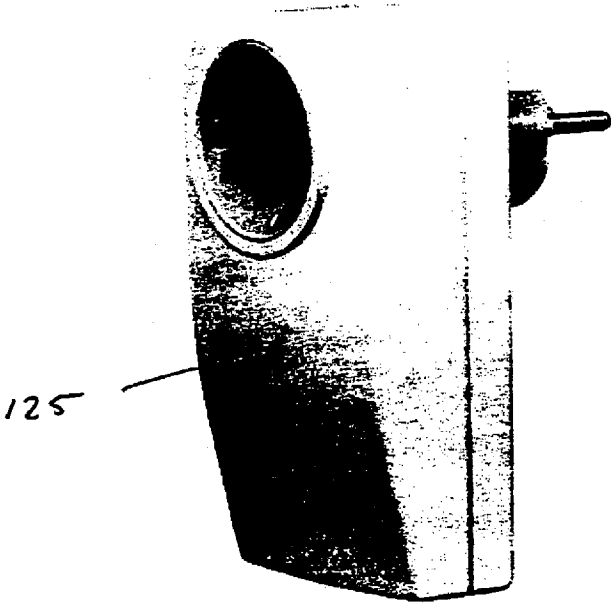


FIG. 6A

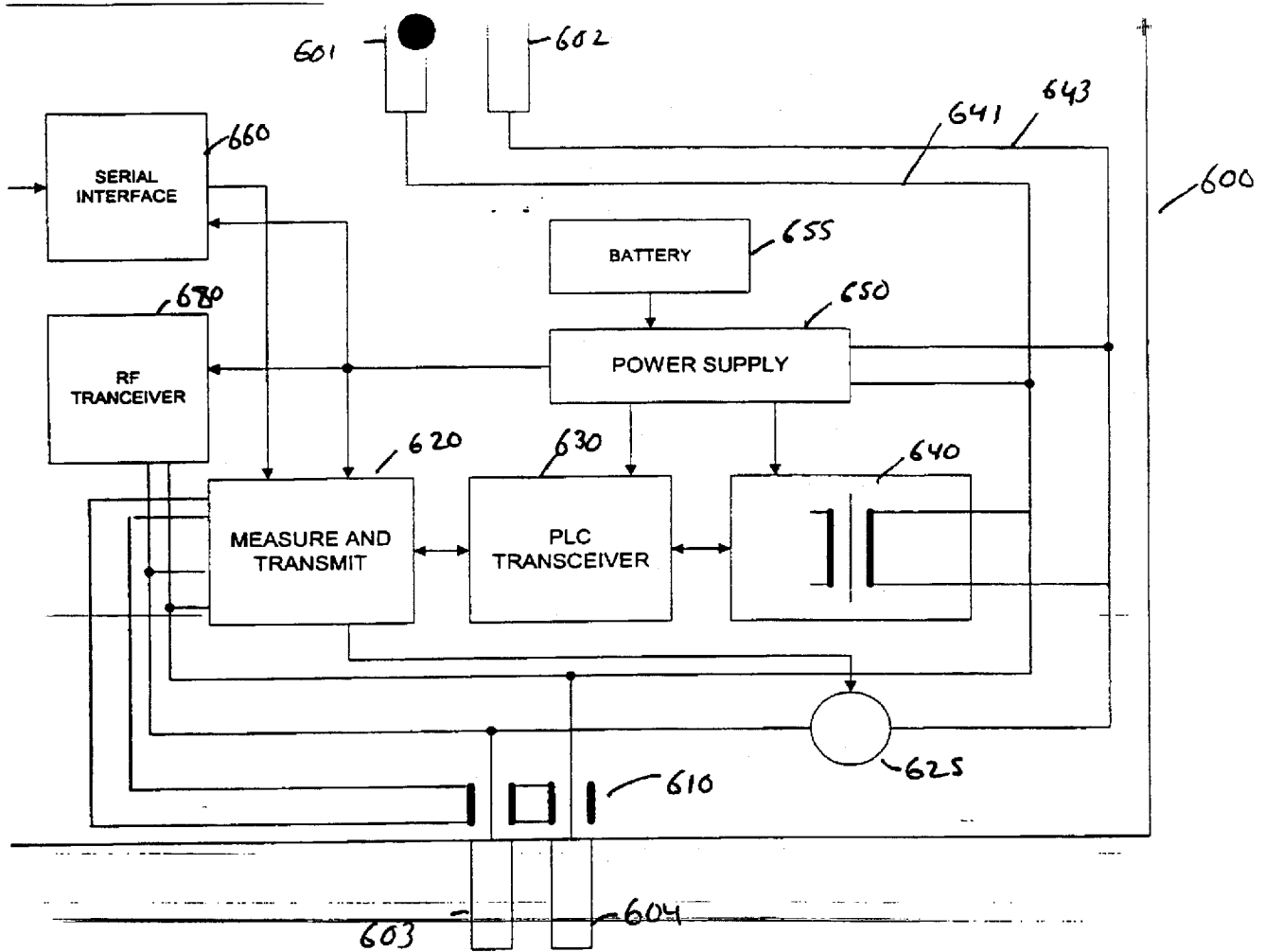


FIG. 60.

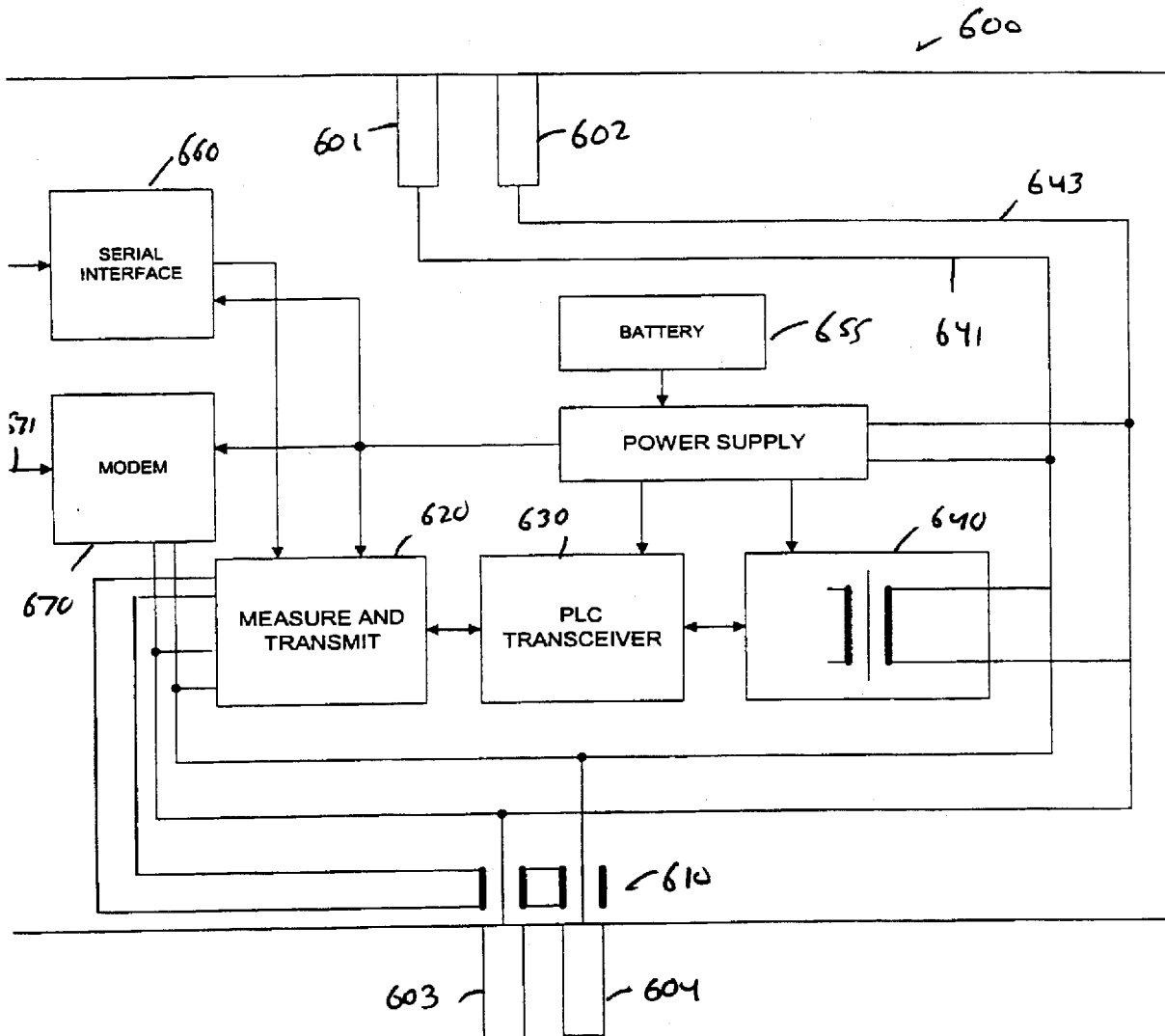


FIG. 6C



10/33

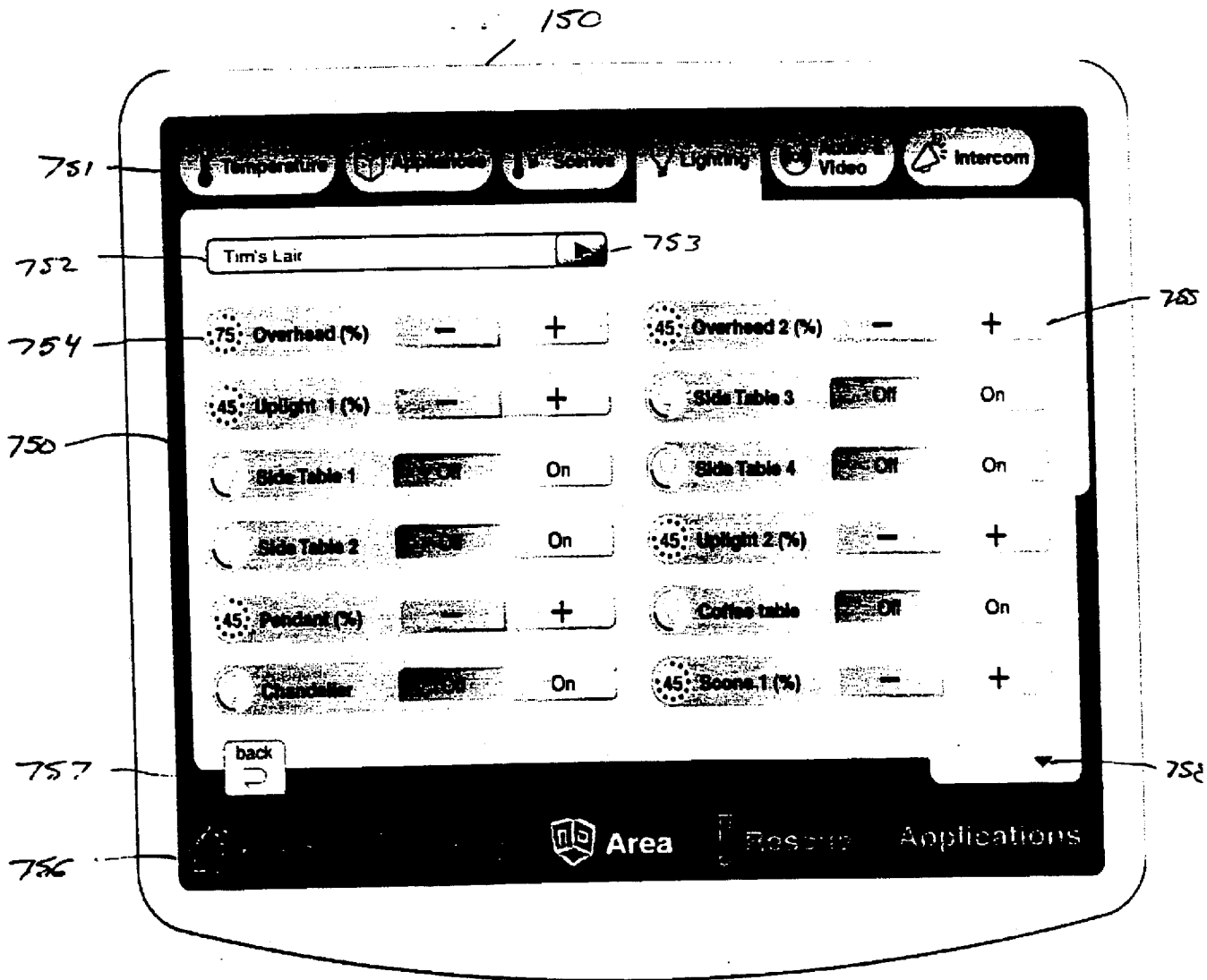


FIG 7C

11/33

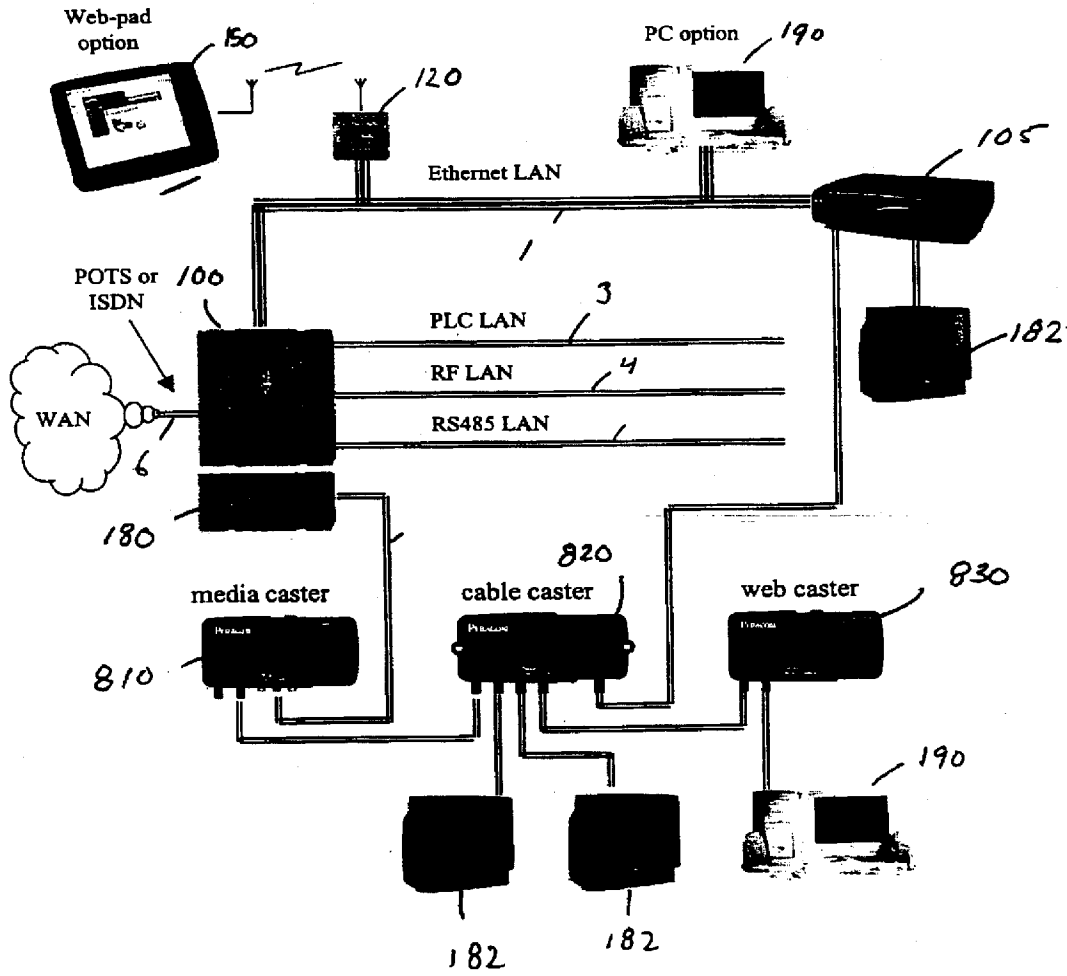


FIG. 8

12/33

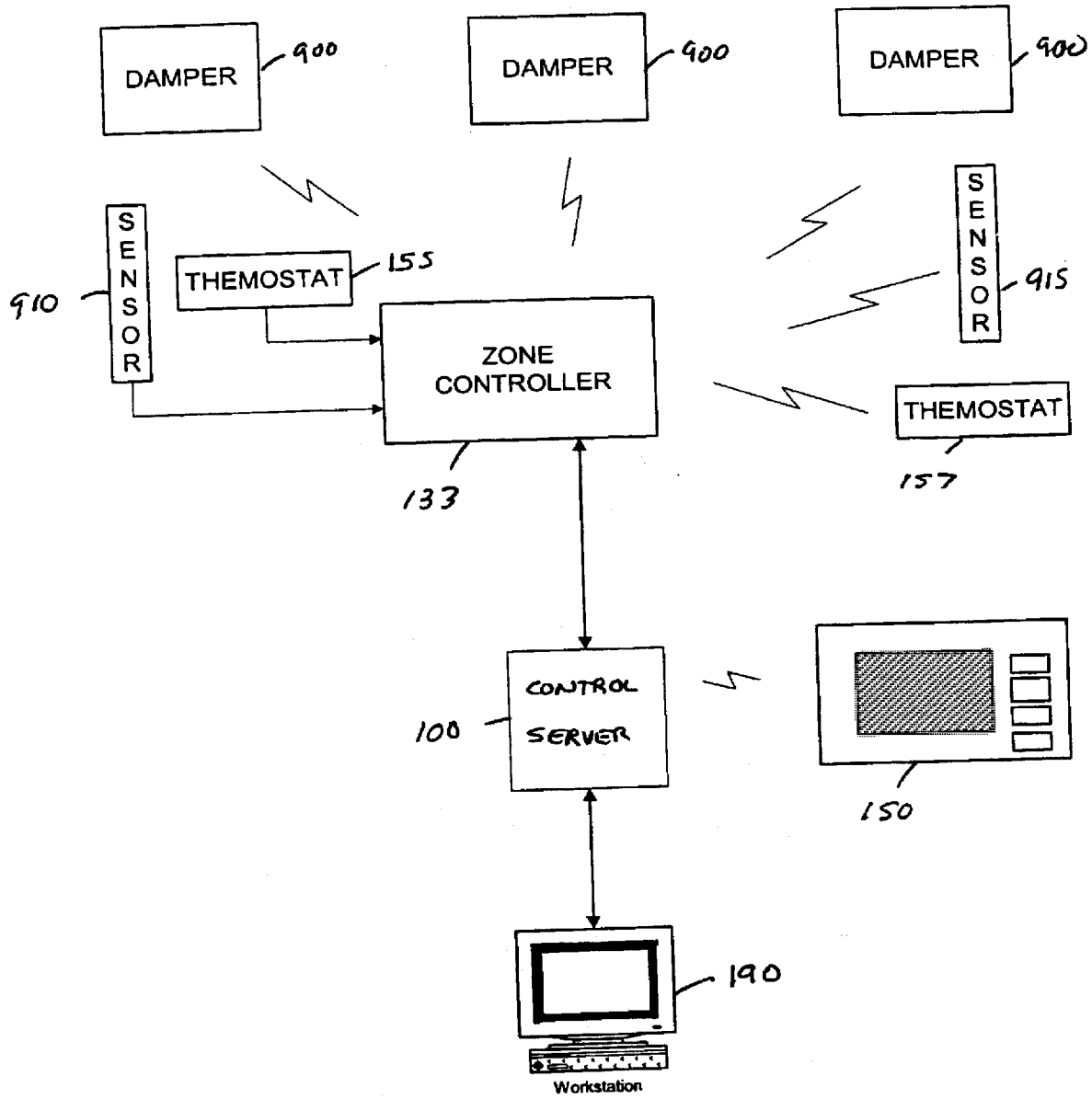


FIG. 9

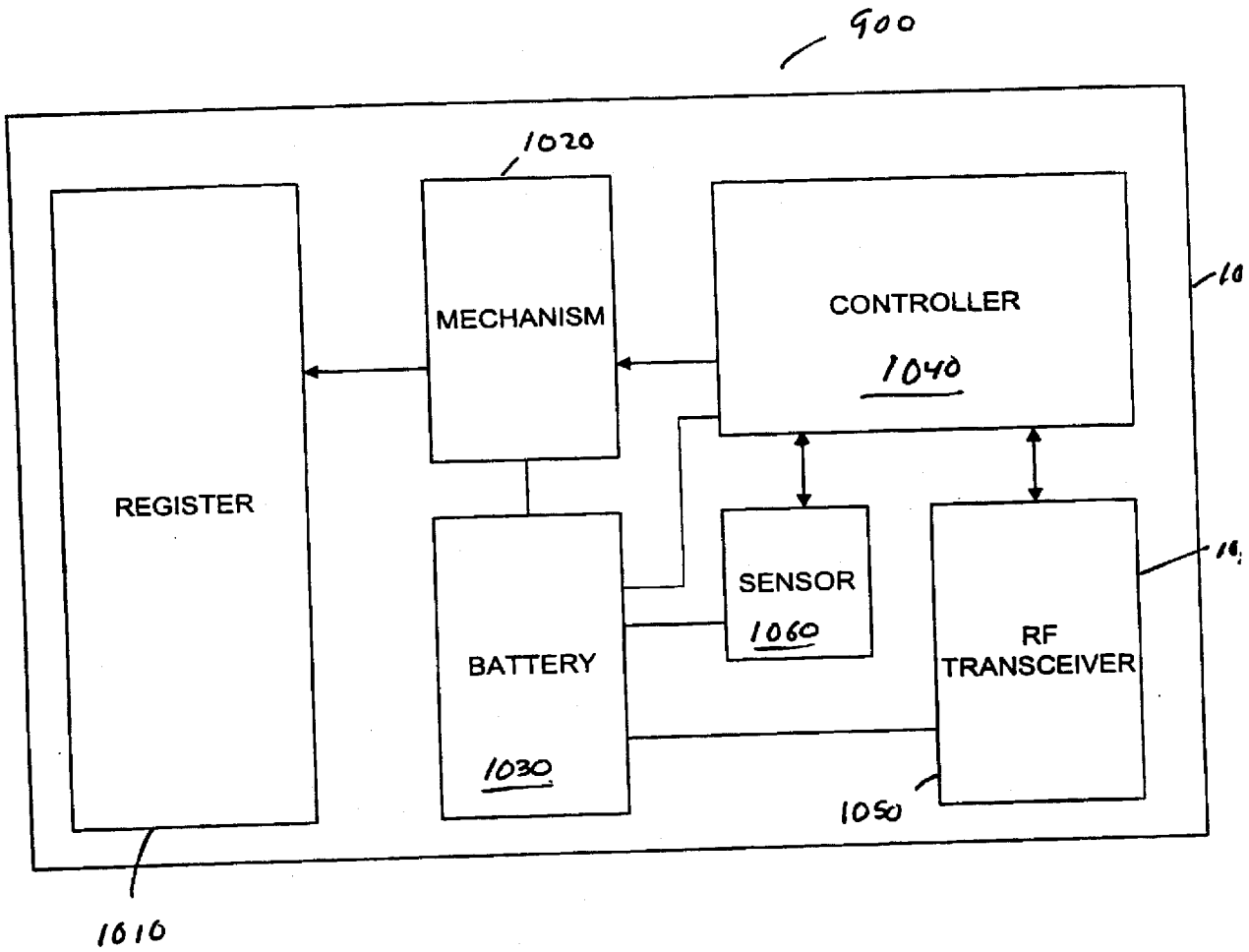


FIG. 10

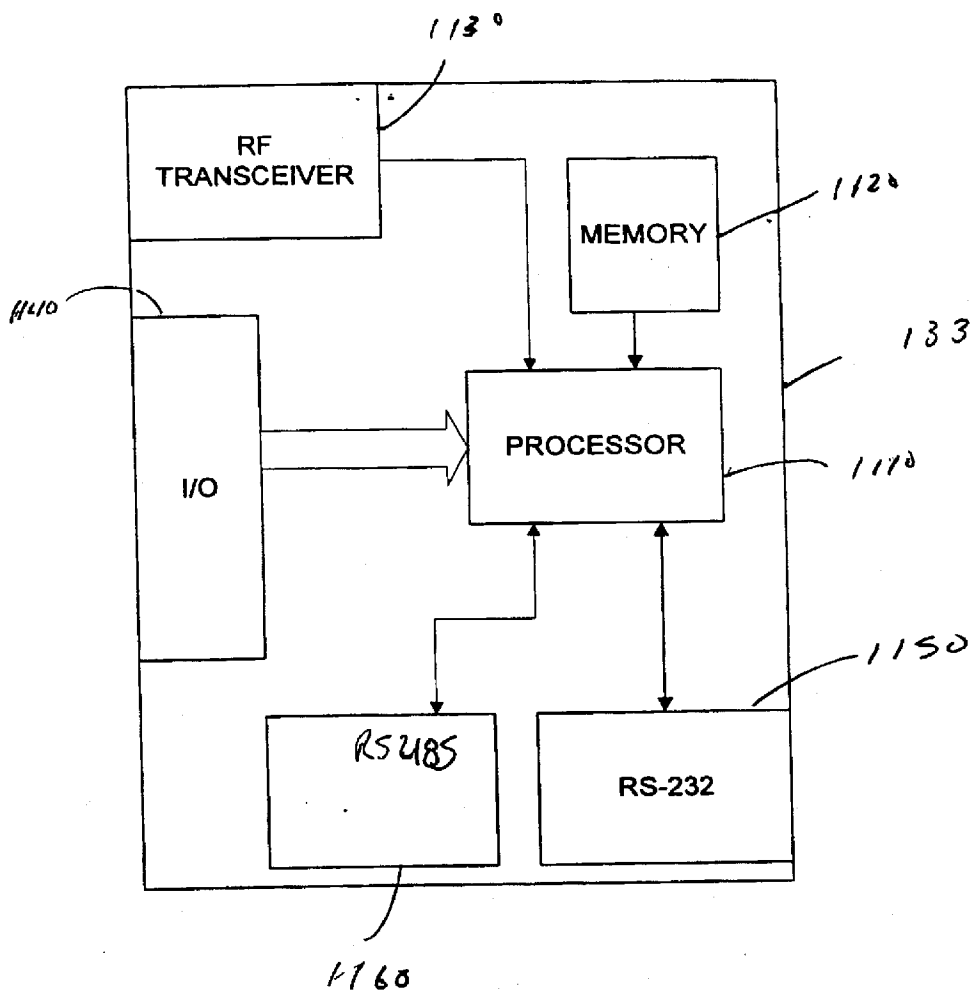


FIG. 11

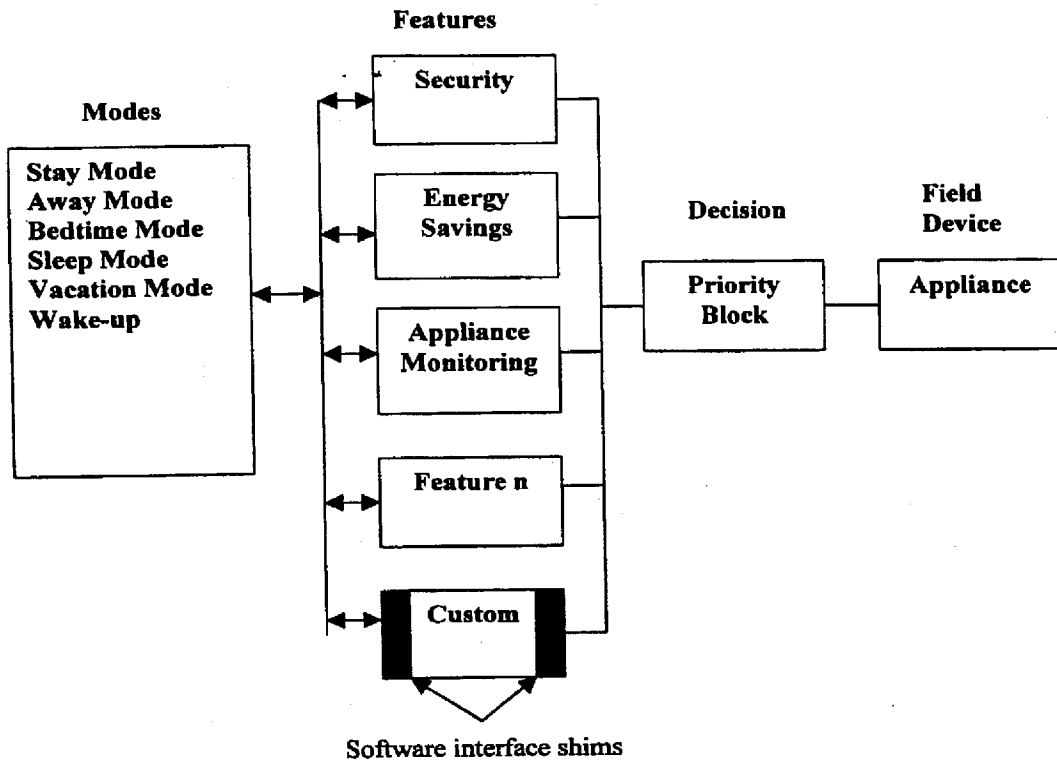


FIG. 12

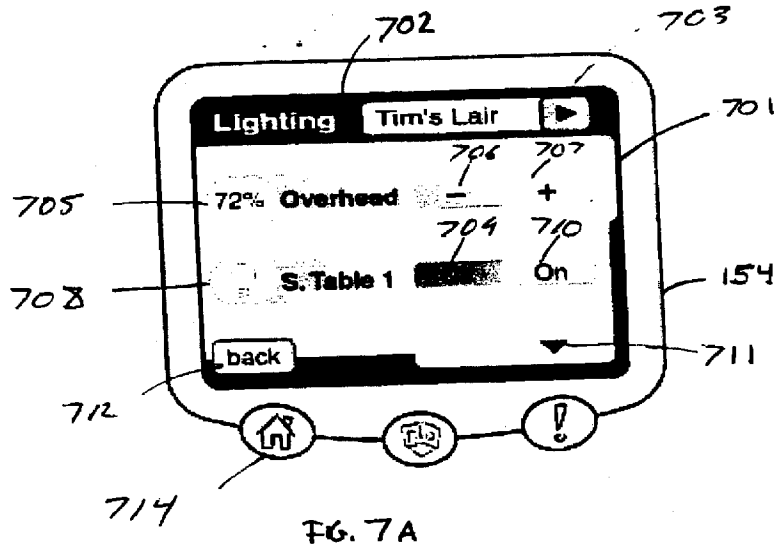


FIG. 7A

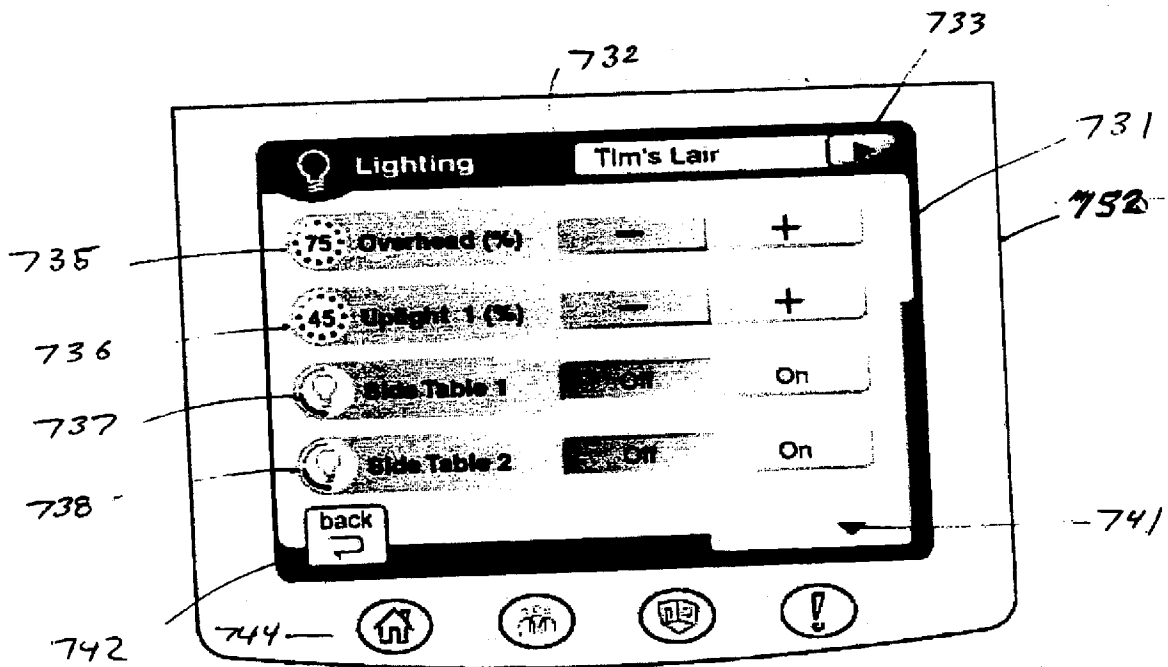


FIG. 7B

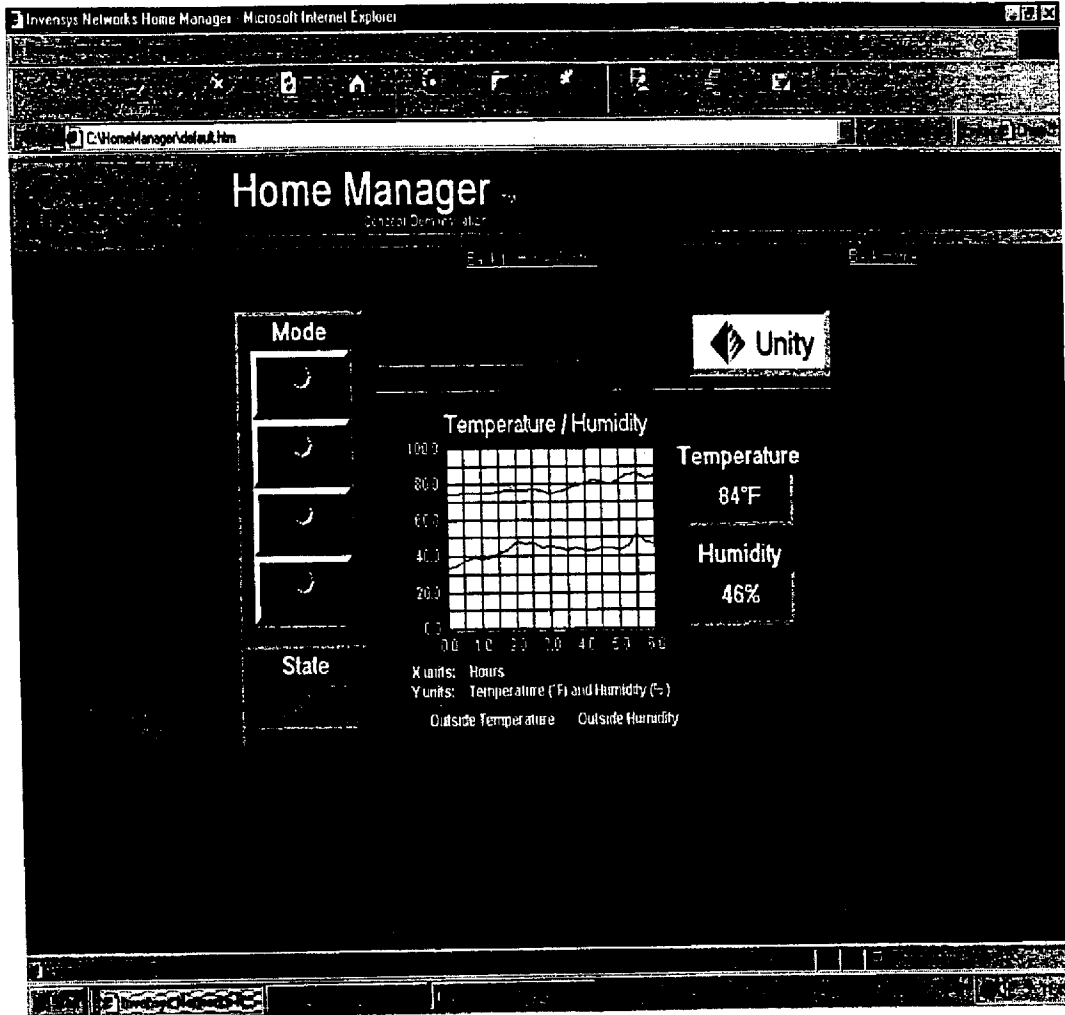


FIG. 13



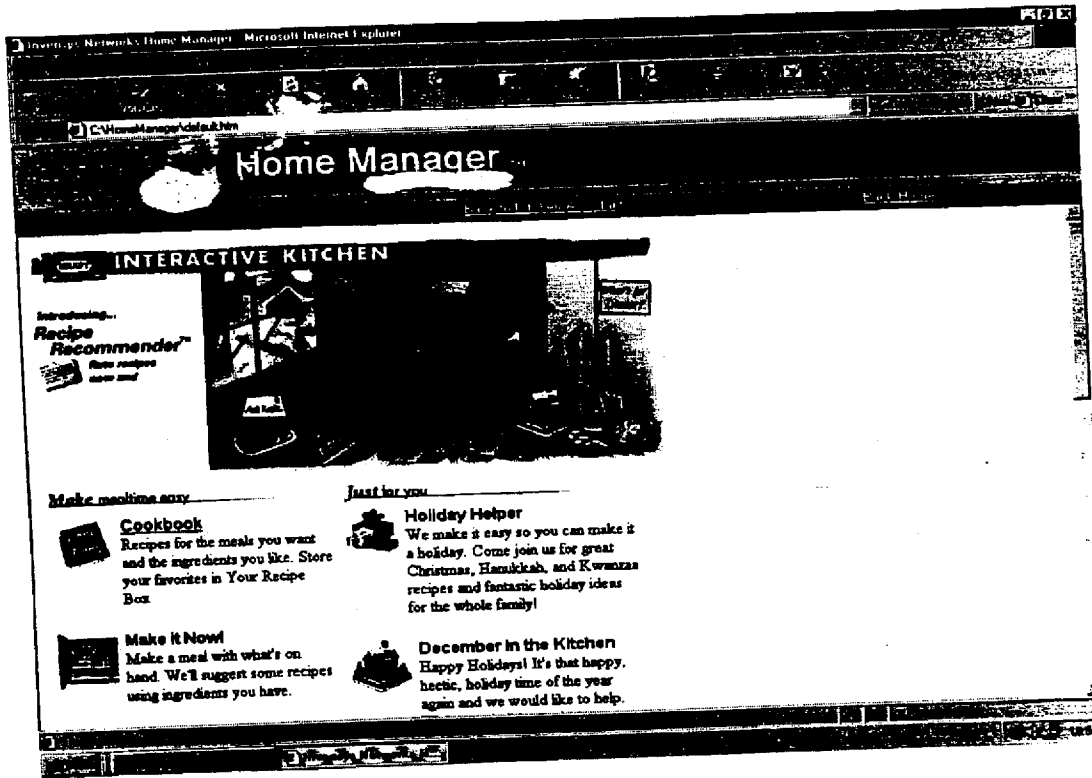


FIG. 14

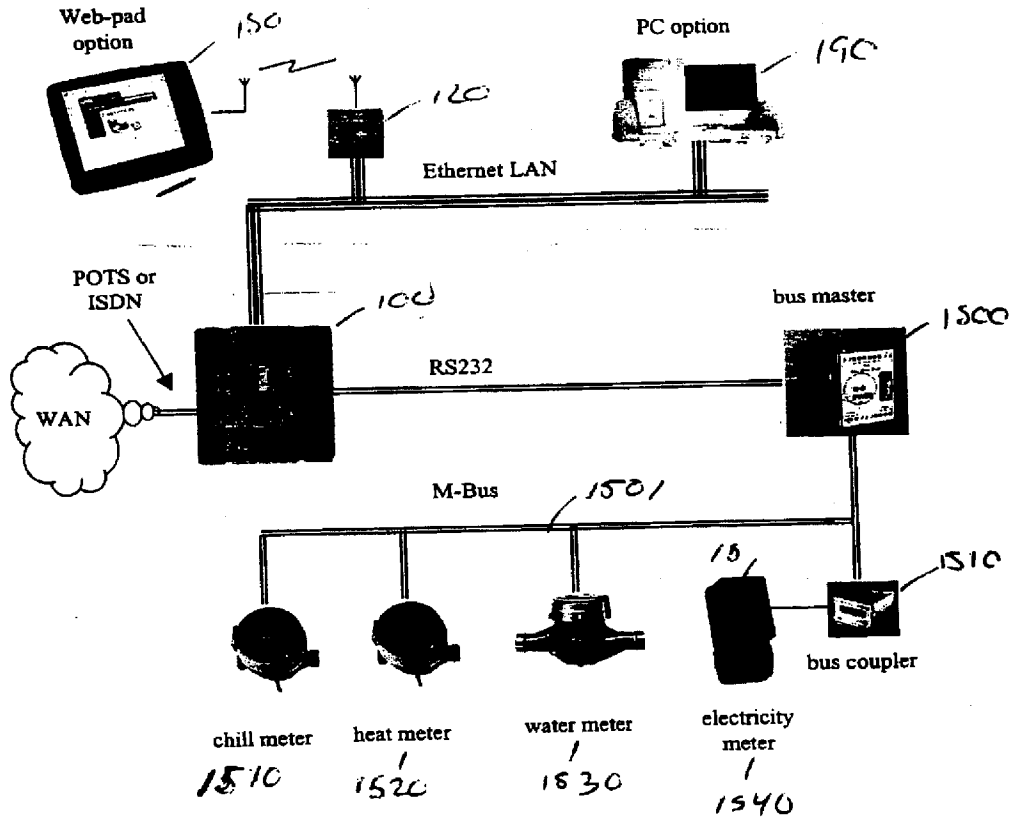


FIG. 15

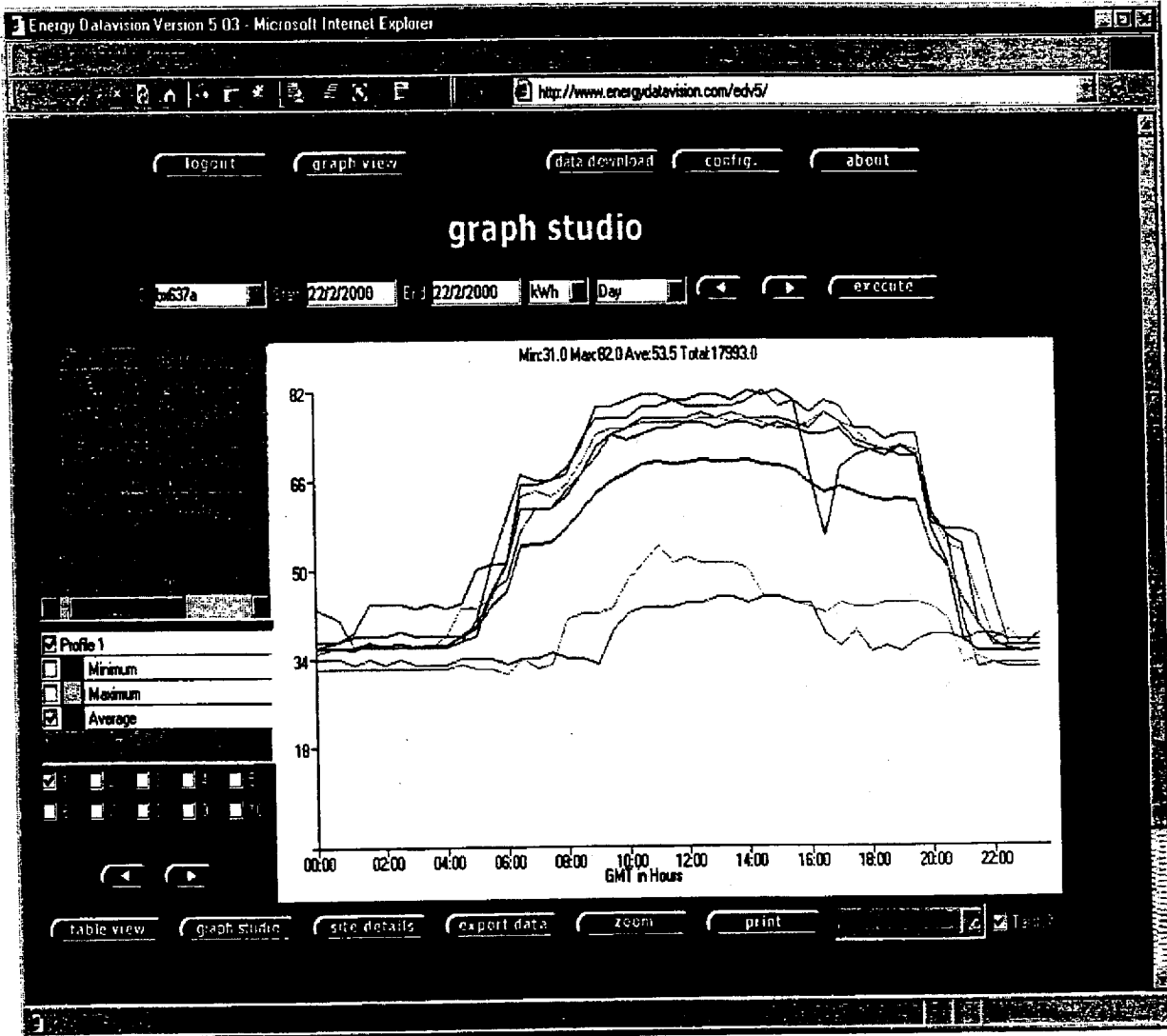


FIG. 16

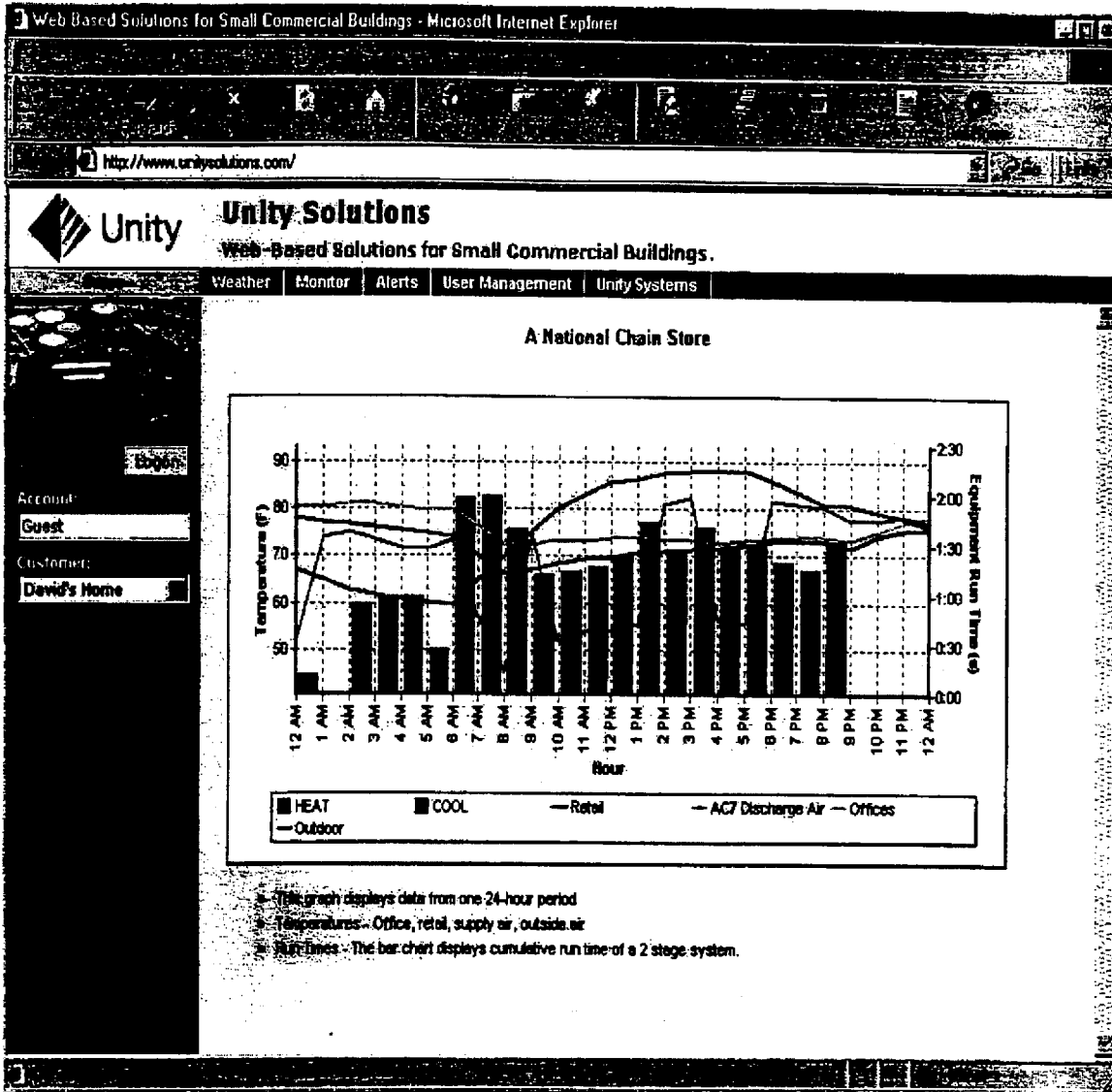


FIG. 17

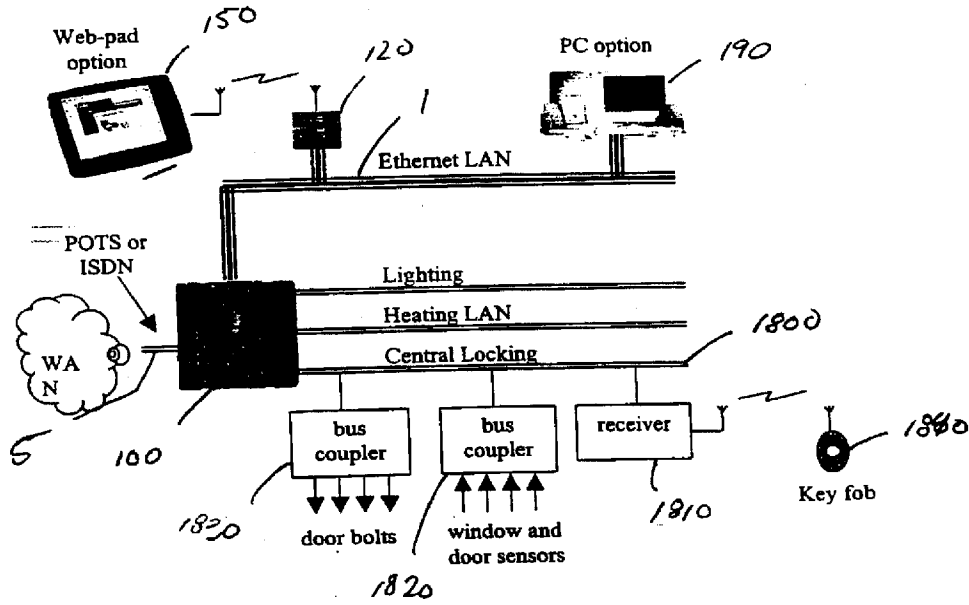


FIG 18

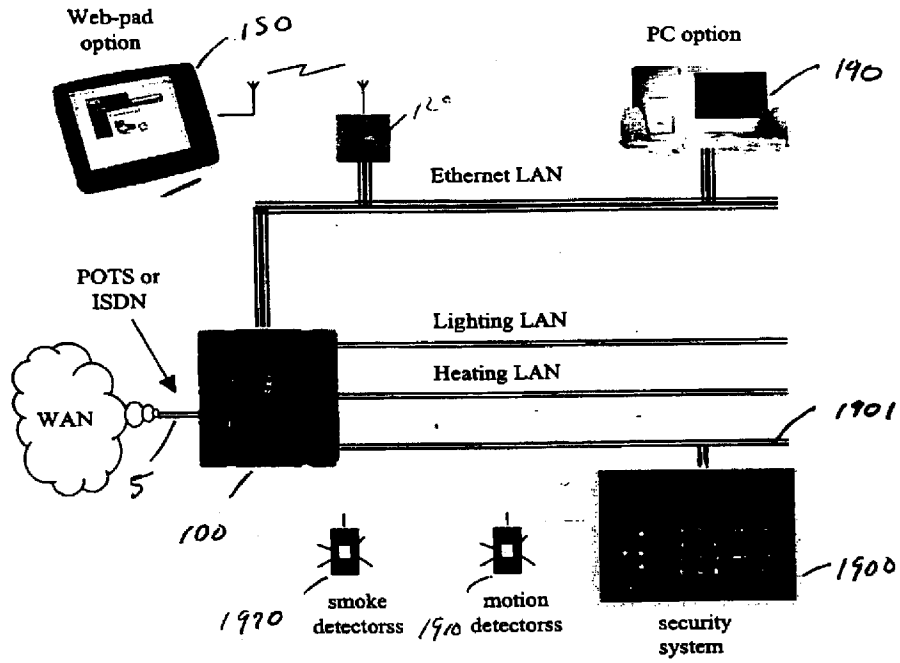


FIG. 19

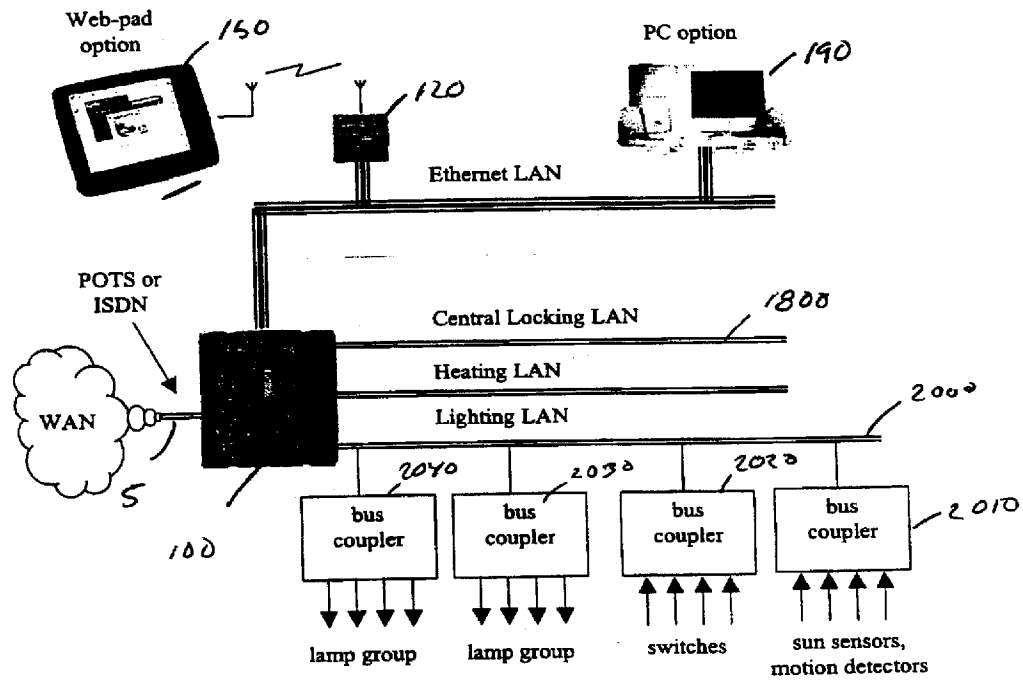


FIG. 20

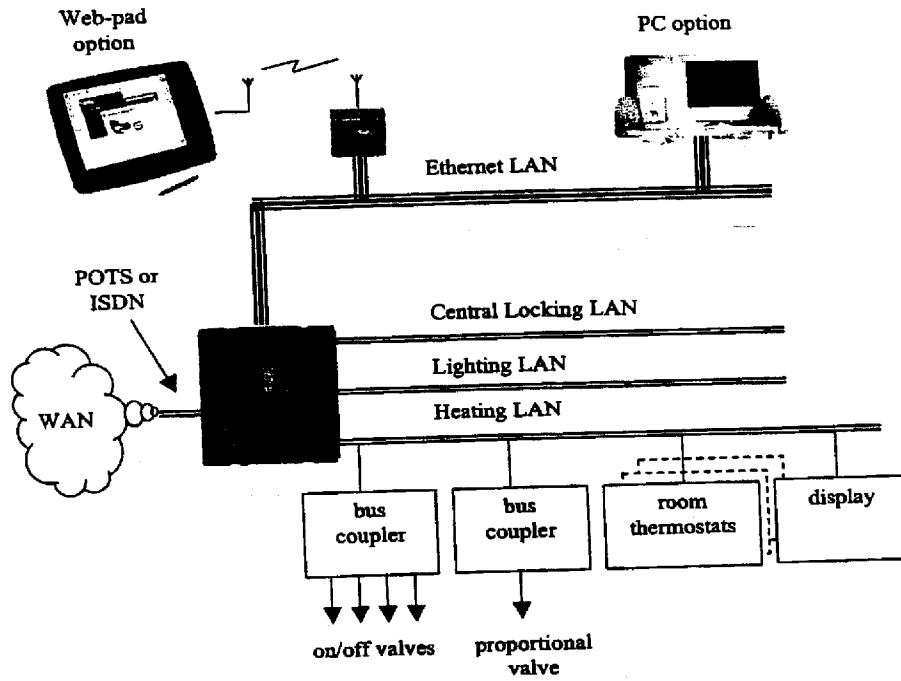


FIG. 26



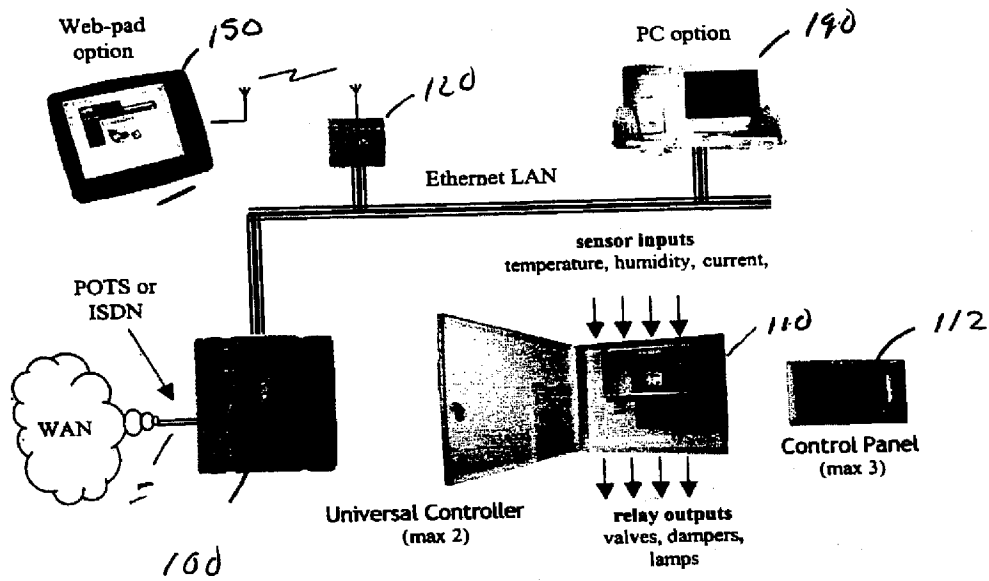


FIG 22

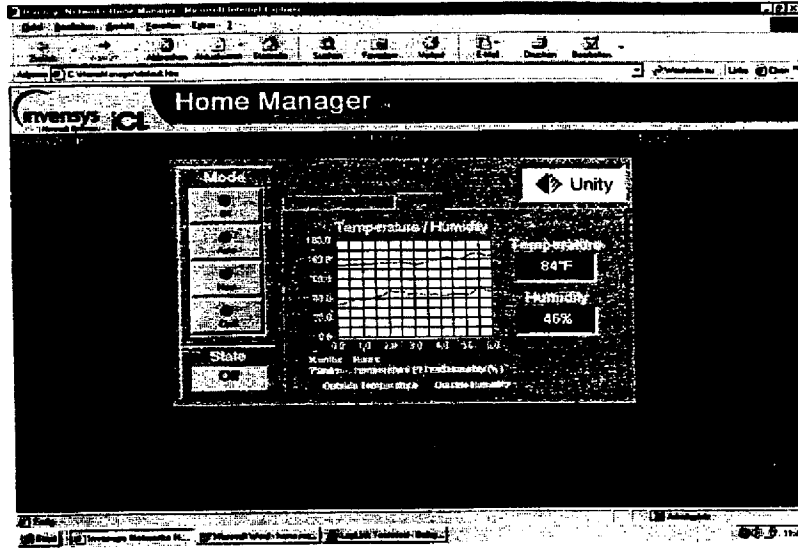


FIG. 23

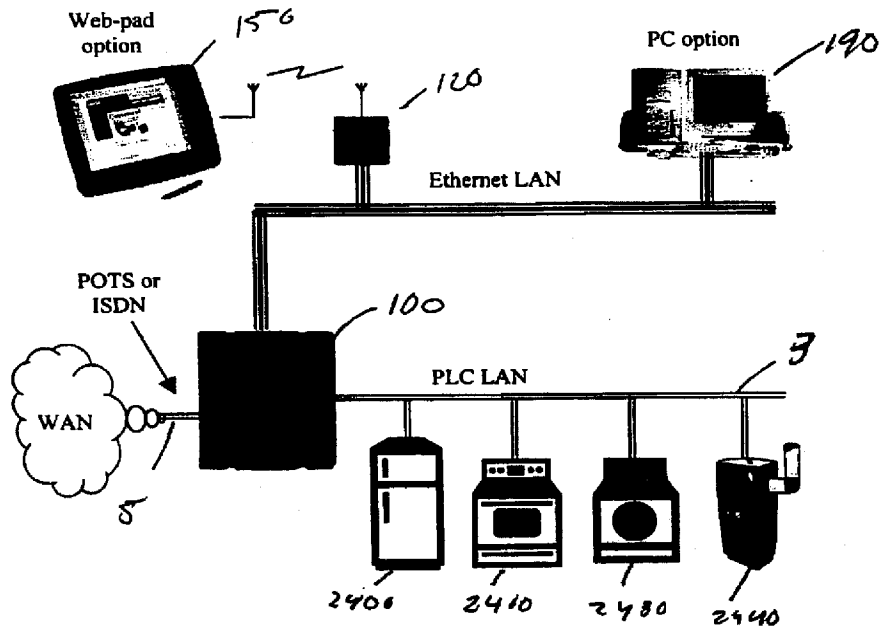


FIG. 24



*FIG. 25*

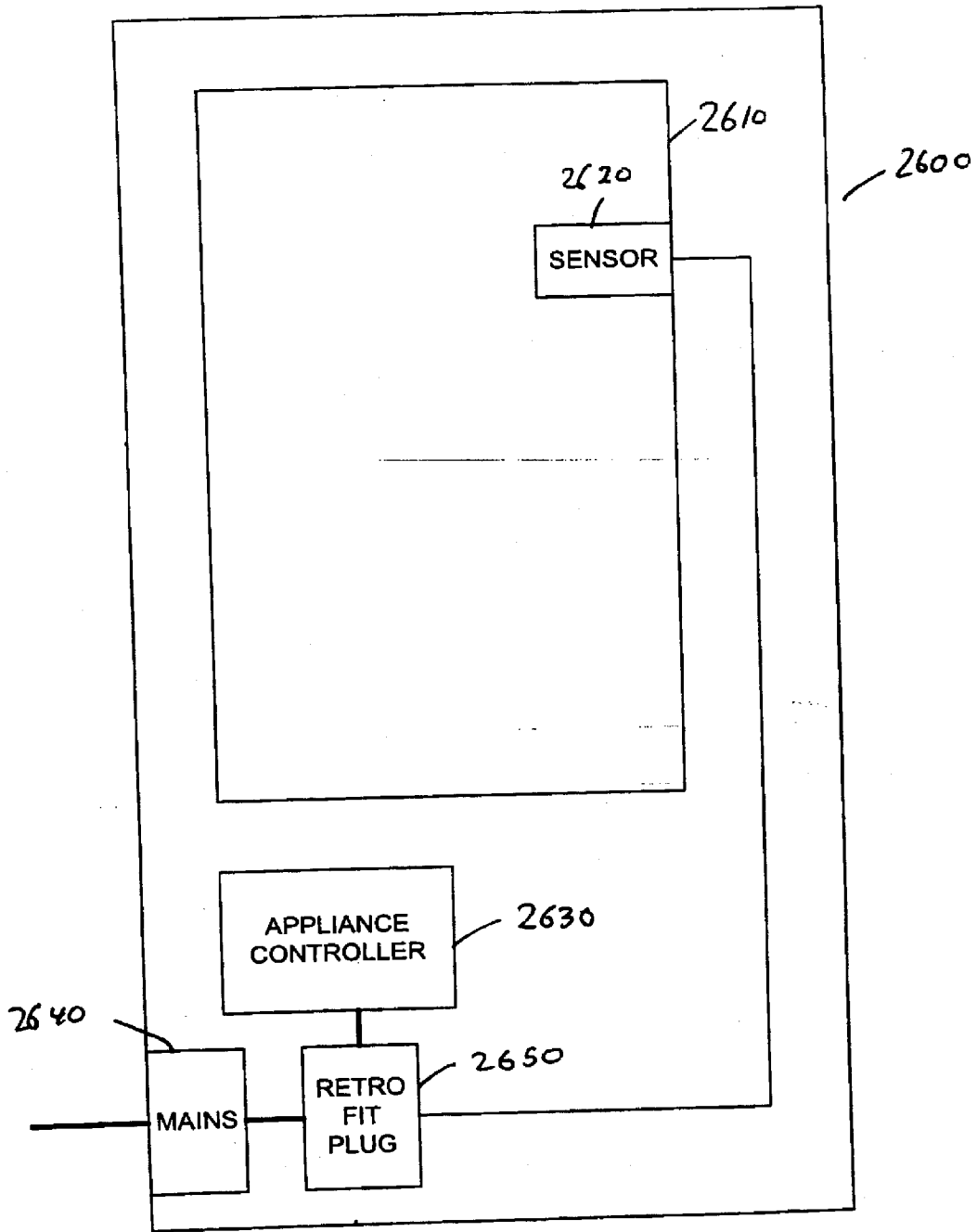
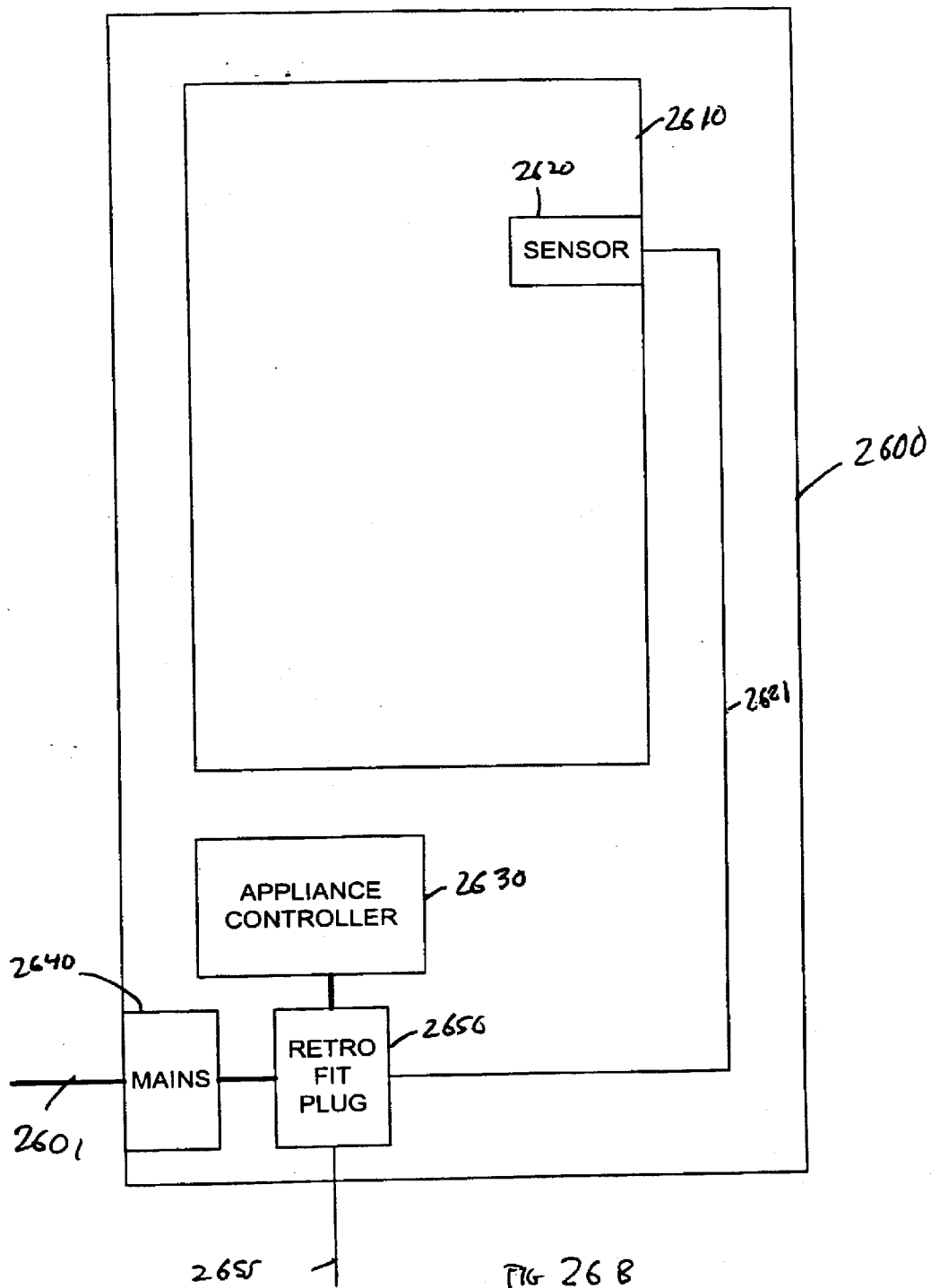


FIG. 26A



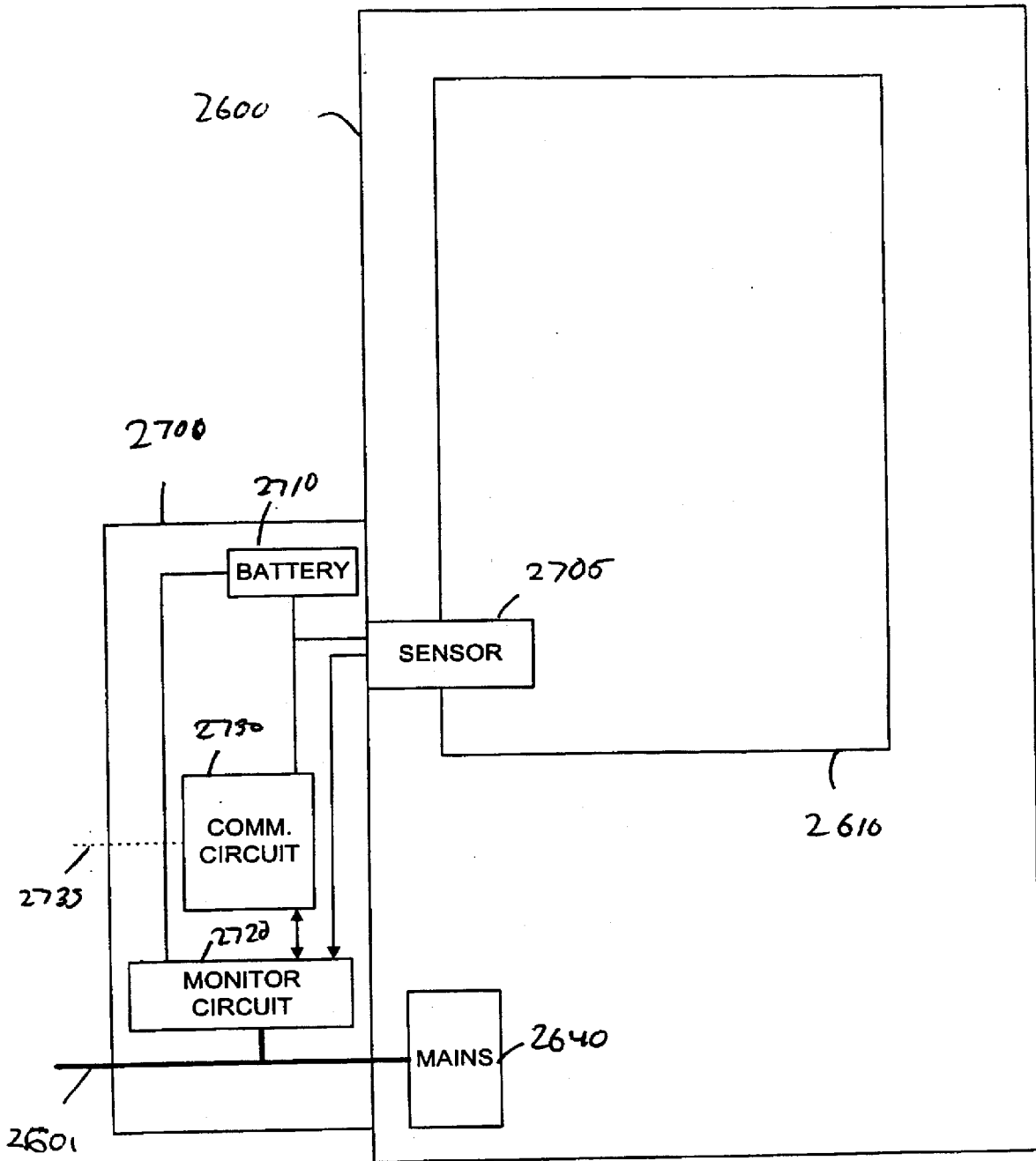


FIG. 27A

33/33

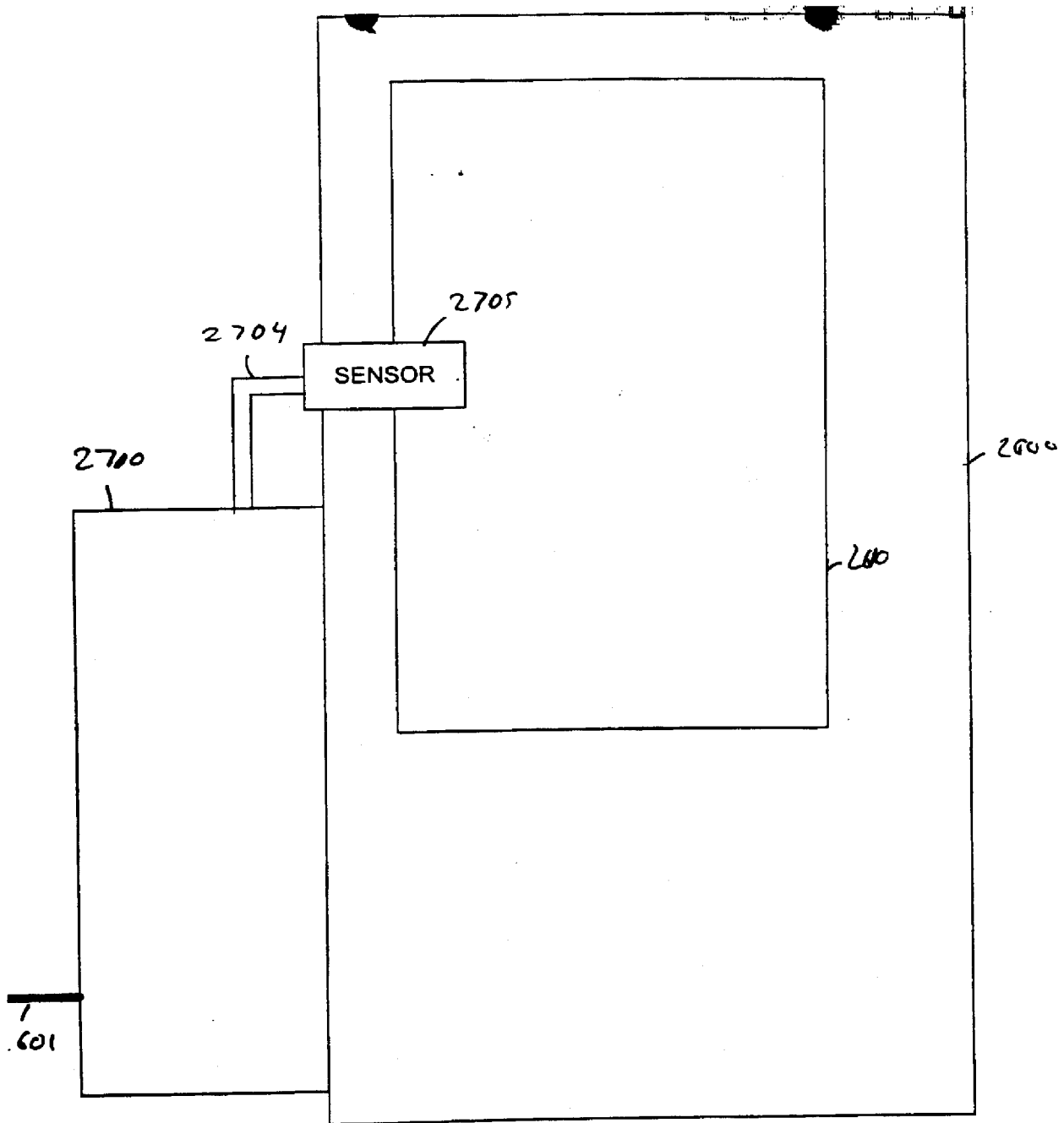


FIG. 27B



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
27 December 2001 (27.12.2001)

PCT

(10) International Publication Number  
WO 01/99078 A2

(51) International Patent Classification<sup>7</sup>: G08C

Rohana; 55 Ayer Rajah Crescent, #4-01/07, Singapore 139949 (SG).

(21) International Application Number: PCT/IB01/01235

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(22) International Filing Date: 11 June 2001 (11.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
09/597,857 20 June 2000 (20.06.2000) US

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant: EUTECH CYBERNETICS, INC. [SG/SG];  
Blk 55 Ayer Rajah Crescent, #04-01/07, Singapore 139949 (SG).

**Published:**

— without international search report and to be republished upon receipt of that report

(72) Inventors: WEWALAARACHCHI, Bandu; 55 Ayer Rajah Crescent, #4-01/07, Singapore 139949 (SG). GUNASEKERA, Priyantha, M., V.; 241, Bukit Butok, East Avenue 5, #06-285, Singapore 650241 (SG). GUNASINGHAM, Haritharan; 522 East Coast Road, #06--1, Nasuas Block, Singapore 458966 (SG). LIYANARACHCHI,

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



WO 01/99078 A2

(54) Title: SERVICE-ORIENTED COMMUNITY AGENT

(57) Abstract: A system and method provide the creation and operation of remote real-time data monitoring and control systems. Such applications include a communications gateway coupled to real-time devices. The communications gateway transforms the real time data collected from disparate and non-interoperable systems in a single common data format. The communications gateway provides an object server with a list of the real-time devices to which the communications gateway is connected, and their attributes. The object server publishes this list. Subscribers can access this list, and request subscriptions to specific attributes of certain devices. The object server creates a data object corresponding to the requested information. A subscriber includes a service agent which accesses the object server. In addition, a subscriber may also comprise presentation cells, which provide a representation and mapping of data objects and hence underlying devices and systems, to allow a user to manage and control such systems. Subscribers including presentation cells may be personalized to function as personal agents. Such personal agents can be programmed to monitor and control certain subsystems, and to alert certain people when specific events occur in these subsystems.

**SERVICE-ORIENTED COMMUNITY AGENT**BACKGROUNDA. Technical Field

The present invention relates to systems providing for personalized, distributed, portable real time data acquisition and control, and more particularly to a service oriented environment for managing and controlling such systems.

B. Background of the Invention

Real-time systems are necessary where there is a need to guarantee real-time response to achieve a required quality of service of various underlying devices, communications networks, operating systems, middleware components and application components. Thus, real-time systems are widely applied to diverse applications domains such as manufacturing, facilities management, power systems management, financial analysis systems, and telecommunications.

The complexity of real-time systems arises from the need to respond to concurrent events occurring within a single application (or within multiple applications) at the same time. Also, a real-time system must provide some way of managing configuration management, fault management, static and dynamic

scheduling, and fault tolerance. However, some applications may be hard real-time applications and others soft real-time applications. This results in increased complexity in managing and correlating data and information generated by the different systems into a single coherent system model.

A common strategy for implementing a real-time system is through a hierarchical architecture, where the system is separated into control, supervisory and management layers. The control layer is generally hard real-time in nature, whereas the supervisory and management layers may have decreasing needs for strict guarantee of time, and in many cases are implemented in software.

Hierarchical real-time architecture systems are increasingly being implemented using the client-server model, in which the centralized database stores real time data and acts as a server to graphical user interface clients. Information is transferred from the control network to the real-time database through an input/output server.

One example of such a hierarchical real-time system is a Supervisory and Control Data Acquisition (SCADA) system. In conventional SCADA systems, the real time data is captured from external sensors, control devices, or applications, and is logged to a centralized database. In response, controls on workstations are executed to manage the remote devices. All actions are performed from a centralized location. Basic control functions include alarm, trend, scan, and status

operations.

One problem with conventional SCADA systems is that they are completely centralized. In a client-server system, all of the remote data information is loaded up into the central database, and then remote clients access the system. A problem with this design is degraded performance due to the single point of access, as many remote clients attempt to access the real time data through the single database server. This conventional design thus induces a scalability problem which limits the number of concurrent users.

One solution then is to use multiple real time databases, which partition the data being gathered according to geographic, management, or functional criteria. The problem here is configuration management. Traditionally, configuration is done by mapping input and output points to the database fields. If there are multiple databases, then the system designer has to change the mapping of the remote sensors to the databases, and maintain these mappings over a large number of remote devices and databases. Changes in partitioning of data induce further configuration maintenance. In addition, multiple, partitioned databases make it very difficult to introduce new types of data into the database configuration, and provide for new mappings.

Another solution is an object-oriented framework for the development of personalized workflow applications that provide real time functionality, while

maintaining scalability to any number of users, and integration with existing legacy application systems. However, such solutions require that the users model up front, the environment of the real-time devices that need to be monitored and/or controlled.

This can be better understood with the help of an example. Such solutions involved the system administrator/user defining the data objects and their logical relationships at a prior time, where the data objects and their relationships preferably corresponded to the logical or physical organization of devices and in the system being modeled. An example of such a system is shown in Fig. 1A, where there is shown a set of data objects in an object server. A top level parent data object is defined to represent a building, here Building Center, which two floors, represented by the data objects of 1<sup>st</sup> Floor, and 2<sup>nd</sup> Floor. Each of these data objects has further data objects representing different rooms, Room 1 and Room 2. Each Room data object then has both leaf data objects such as Temperature and Ventilation System, and a parent data object Light Control which itself has leaf data objects for two different Light Banks. This organization of data objects preferably represents the actual building being modeled. When the data objects are created, the building is therefore virtually "reconstructed."

Further, addressing of data objects in the object server is preferably provided by hierarchical naming. Each data object is addressed by its path in the object server. For example, the temperature of Room 1 of 1<sup>st</sup> Floor is accessed by

“Building Center.1<sup>st</sup> Floor.Room 1.Temperature.” Addressing of data objects may also be done with variables. For example, a presentation cell 150, 160, 170 or 180 in Fig. 1B may access any of the leaf data objects of Room 1 by addressing “Building Center.1<sup>st</sup> Floor.Room 1.x”, where x is a variable used to select which leaf data object to obtain. Likewise, any address component can be replaced by a variable. When an address of a data object is resolved, the object server obtains the value of the data object using the index and size parameters stored in the underlying leaf data objects.

In the above example, the server would need to be taken off-line and reconfigured, and then taken back up again, every time that a new object is introduced, or every time that some attribute of an object is modified/added. Thus such systems are problematic in that such modifications must be made by the system administrator/user with the server off-line. Thus such a system does not provide real-time data at the time that such modifications are being made.

Fig. 1B depicts such a system by which objects corresponding to real time devices, and their attributes corresponding to different real time data available from those real time devices, are represented and/or updated on presentation cells 302 on the client device.

Fig. 1B shows that an object 100, having “n” attributes, is created on the server side of the system. Each data attribute 110, 120, 130, and 140, has its own

address. That is, as described above, only the naming structure in such a system is hierarchical. In actuality, data attributes 110, 120, 130, and 140 have a flat structure. That is, there is no hierarchy employed in the data structure, and each attribute has a separate address on the server side. Each data attribute 110, 120, 130, and 140 is entirely self-contained. The object does not have an address of its own in the system.

Via the network, a copy of the object 100A is created on the client device. Further, a copy is also made of the addresses for each data attribute 110A, 120A, 130A, and 140A. The client device includes presentation cells 150, 160, 170 and 180. Each of these presentation cells 150, 160, 170 and 180 subscribes to a data attribute 110A, 120A, 130A and 140A. Based on the addresses of each data attribute 110A, 120A, 130A and 140A, the presentation cells 150, 160, 170 and 180 can access the values of the data attributes that they subscribe to.

In such a system, the user of the client device is required to define the objects and their data attributes up front – the object model cannot be built dynamically. As can be noted from the steps described above, the user must define all the attributes of each object up front, so that each of these attributes can be assigned its own address. Thus, each time a system employing such a method is used for a different object model, the object model needs to be built to correspond to that particular use of the system. For instance, even if such a system is used only for building

maintenance purposes, a separate object model will have to be pre-defined for each distinct building. Dynamic object modeling is not possible with the systems described above.

Thus there exists a need for a solution which permits dynamic modeling of the environment by the user.

Further, current real-time device management/control systems permit access to the real time data from one centralized place, and from one particular medium (for instance a particular computer). This creates a problem because a user of the system may not always be at that centralized place, or have access to that particular medium. For instance, if real time updates of the data were contingent on a computer situated in a user's office being powered on, the user would not be able to obtain the updated real time data from her home if her computer at work were turned off. Further, the user would not be able to access the real time data from a different medium, such as a telephone.

Thus there exists a need for making such management/control systems virtual, and accessible from different places through different mediums of the users' choice.

Another problem with currently existing real time device management/control solutions is that they do not manage Quality of Service (QOS) requirements. By definition, a real-time system provides a result in response to an event in a time



scale that is adequate to meet the quality of service and performance needs of the application. Different publishers of data often offer different QOS capabilities. Thus subscribers to the data may wish to choose different publishers based on the QOS offered by them. In addition, different subscribers may be satisfied with different levels of QOS. Subscribers who did not have high QOS requirements may be able to obtain the data at a lower cost than those who require the same data at a higher QOS.

Thus there exists a need to manage QOS requirements of subscribers with the QOS capabilities of publishers of data. Further, there is a need to guarantee end-to-end quality of service to every application, regardless of its implementation, communications protocols, or other integration factors.

#### SUMMARY OF THE INVENTION

The present invention overcomes the limitations of currently existing real-time data acquisition and control systems by providing a framework which facilitates dynamic building of the object model by allowing dynamic publication of data. In addition, the present system permits a user to access the real time data through various mediums of the user's choice. Further, the present system manages the QOS capabilities of publishers of real-time data as well as the QOS requirements of

subscribers to the real time data.

The present invention uses complex data structures, instead of the above-described flat data structures used by some current systems, in order to create a dynamic object server. "Object" structures containing attributes are now created. Instead of allocating an address to each attribute, each object is allocated one address, and there are pointers to the various attributes within one object structure. This facilitates dynamic object modeling.

A system in accordance with the present invention comprises of real time devices, a communications gateway, an object server, and a subscriber to the data. The communications gateway is communicatively coupled to selected ones of the real time devices to receive real time data from the devices. This real time data is received in a format according to a communications protocol associated with the devices; various different devices may have different, non-compatible, proprietary formats. The communications gateway converts the real time data by reformatting it into standardized data format that is independent of the original format used by the devices. The standardized data format specifies for each item of real time data a content and source of the real time data. In this manner, data from many different devices, having different original source formats is converted into a single, standard data format.

The object server is communicatively coupled to the communications gateway

and receives from it, a list of the real time devices to which the communications gateway is coupled, as well as their attributes. (These various logical attributes correspond to attributes of individual devices, or collections of devices.) The object server then publishes this list. Once a subscriber requests information about one or more attributes of one or more devices, the object server creates data objects corresponding to the requested devices, along with the attributes of the data objects. The object server then stores the real time data in the data objects that it has created. In this manner, dynamic modeling of the environment becomes possible, because real time devices can define what they have to offer.

For example, in a building management system, the real time data from the field devices will be for many different types of field devices, such as lights, heating units, thermostats, window controls, ventilation systems, elevator banks, and so forth. As received by the communications gateway, the data from the many different field devices is very low level, and disaggregated in the sense that the communications gateway has no knowledge that relates data from different field devices (e.g. readings from different temperature sensors in the same tank). However, when a subscriber expresses interest in a particular device or attribute, the object server dynamically creates a corresponding data object. At this time, the real world data can be organized in a logical manner, such as an abstraction for each floor of the building, within each floor, a number of rooms, and within each room

controls for lights, temperature, window position, and so forth. The organization of the data (e.g. hierarchical organization by floor, room, and type of control) is not present in the original real time data received by the communications gateway, but rather, is provided by the object server. Further, it is to be noted that the organization of the object server does not need to be defined up front by the system administrator/user to represent the real world system being managed. Instead, any real world system can be dynamically modeled on demand.

A system in accordance with the present invention may further comprise of a personal agent. Such a personal agent would comprise of a service agent that could subscribe to some attributes of certain objects from the list published by the object server, as well as presentation cells that would provide a representation of these attributes.

This personal agent may reside on a server different from the object server, and may be accessed by users through several different mechanisms, such as through telephone, through browsers, etc. That is, users can then access the published real time data from any place, and through different mediums.

In another aspect of the present invention, a system in accordance with the present invention manages the QOS capabilities of publishers of real time data, and the QOS requirements of subscribers to real time data. If the QOS requested by a subscriber can be provided by a publisher, the requested QOS is provided to the

subscriber. If the QOS requested by subscriber cannot be provided by a publisher, the subscriber may be given the option of receiving the desired data from another publisher who can provide the requested QOS. Further, if the channel connecting the subscriber to the publisher is the limiting factor, an alternate channel capable of supporting the requested QOS may be selected.

Accordingly, the present invention represents a substantial improvement over existing approaches for implementing real-time object-oriented systems.

The features and advantages described in this summary and the following detailed description are not all-inclusive, and particularly, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specification, and claims hereof. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the inventive subject matter, resort to the claims being necessary to determine such inventive subject matter.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is an illustration of an example of a collection of data objects in an object server.

Fig. 1B is an illustration of a currently existing representation of data objects corresponding to real time devices, and their attributes.

Fig. 2 is an illustration of one embodiment of a system in accordance with the present invention.

Fig. 3 is an illustration of an example personal agent and a cell library of presentation cells.

Fig. 4 is an event trace of the operation of one embodiment of a system.

Fig. 5 is an illustration of a representation of data objects corresponding to real time devices, and their attributes.

Fig. 6A is an illustration of quality of service management including one subscriber.

Fig. 6B is an illustration of quality of service management including two subscribers.

Fig. 7 is an illustration of a system where the subscriber subscribes to real time data and republishes it.

Fig. 8A is an illustration of how cell templates are created.

Fig. 8B is a screenshot of a sample cell template.

Fig. 8C is an illustration of how cell templates are used.

Fig. 9 is an illustration of a system used in an energy trading application.

The figures depict a preferred embodiment of the present invention for purposes of illustration only. One skilled in the art will readily recognize from the following discussion that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the invention described herein.

#### DETAILED DESCRIPTION OF THE INVENTION

Embodiments of the present invention are now described with reference to figures where like reference numbers indicate identical or functionally similar elements and the left most digit(s) of each reference number corresponds to the Fig. in which the reference number is first used.

#### SYSTEM ARCHITECTURE

Referring now to Fig. 2, there is shown the software architecture of one embodiment of a system in accordance with the present invention. It is comprised of real time devices 202 and 204, a communications gateway 210, an object server 220, and a subscriber 230 including a service agent 240.

#### Real time Devices

The real time devices 202 and 204 are the components that collect real time data. For instance, for a building maintenance system, these could be temperature sensors, light controls, fan controls, etc. In industrial applications, these devices could include flow meters which measured flow rates and/or pressure differentials. In energy trading systems, these devices could be, for instance, energy meters which measured current power consumption and/or total energy usage. These real time devices collect real time data in various different formats. In particular, each device may collect data in a format according to a communications protocol associated with the device. One of ordinary skill in the art will note that various different devices may have different, non-compatible, proprietary formats.

#### Communications Gateway

The communications gateway 210 provides an interface between the real time devices 202 and 204, and the object server 220. The communication gateway 210 is responsible for receiving real time data from the real time devices 202 and 204, which will be in various proprietary, device-dependent data formats, and converting it to a standard, device independent data format. Each communication gateway 210 is specific to communicating with particular devices 202 and 204, and is adapted to convert the protocol of such devices to the standard data format. The



communication gateway 210 operates with such protocols as BACnet (building automation), LonTalk (control networks) OPC (process control), MAPI (email applications), TAPI (telephony applications), and various programming protocols such as DDE, ODBC, and OLE.

More particularly, the input format to a communication gateway 210 comprises a low level byte stream of data packets containing real time data formatted according to a particular device protocol. In the typical device protocol, the data packets include a device ID, a parameter name, a type (application level and protocol specific), a data length, and the real time data. The real time data is itself typically unstructured.

The communication gateway 210 converts this information into a standardized data format that includes fully structured and typed data, with an indication of the source and the value of the data. The indication of source specifies the particular device 202 or 204 which generated the data. This reformatted data is preferably in the format of <name, value> pairs, where the name indicates the data source, and the value is the structured real time data. In this manner, unstructured, raw real time data from many different sources, having different and often incompatible protocols, is restructured into a consistent representation and format.

#### Object Server

The object server 220 is communicatively coupled to the communications gateway 210, and receives from the communications gateway 210, a list of the devices 202 and 204 to which the communications gateway 210 is coupled, and their attributes. The object server 220 then publishes this list, which can be used by various subscribers 230, to determine which devices and/or attributes the subscribers 230 are interested in.

Once one or more subscribers 230 have indicated an interest in subscribing to information from any of the devices 202 or 204 to which the object server 220 has access via the communications gateway 210, in one embodiment of the present invention, the object server 220 will then create a data object containing data from the indicated real time device 202 or 204. The section on system operation describes in detail how this is done. The object server 220 enables the subscriber 230, via its service agent 240, to subscribe to this data, and provide real time updates of such data to the presentation cells 302 they service. The published data is in the form of <name, value> pairs, as described above.

#### Subscriber

The subscriber 230 subscribes to the data published by the object server 220,

by means of a service agent 240 included in the subscriber 230. A subscriber 230 may be a personal agent, or it may be a subscriber and re-publisher. If the subscriber 230 is a personal agent, it will include presentation cells 302 for presenting the data to the user. If the subscriber 230 is a subscriber and a re-publisher, another personal agent will have to subscribe to it. Such a scenario is described in further detail with reference to Fig. 6.

In either case, a subscriber 230 must include a service agent 240. A service agent 240 is an entity that interfaces between a presentation cell and the object server 220 to provide the presentation cell with updates of the data objects from the object server 220, and to update the data object with inputs from the presentation cell. One skilled in the art will note that a service agent 240 can service a number of different presentation cells 302 in various different personal agents 300. A service agent 240 provides access to all data objects in a single object server 220. A service agent 240 is associated with a subscriber 230 by a drag and drop operation.

The features of a service agent are more fully described in U.S. Patent No. 6,067,477.

Each service agent 240 also includes references to each of the presentation cells 302 which it services, and for each of these presentation cells 302, the address of the data object which contains the data of interest to the presentation cell.

### Personal Agent

A personal agent 300 comprises a service agent 240 described above, as well as a network of presentation cells 302. The user can interconnect presentation cells and service agents 240 so as to create control and monitoring applications which represent the user's personal workflow.

A personal agent is a user customizable graphical interface through which the user interacts with the system of the present invention. A user may have multiple personal agents configured on their remote computer, each with its own collection of presentation cells and service agents 240.

Referring to Fig. 3 there is shown an example of a personal agent 300 including several presentation cells 302, including a slider presentation cell 302a, a level indicator presentation cell 302b, a numeric display presentation cell 302c, and text presentation cell 302d. The slider presentation cell 302a is a control cell that allows the user to graphically manipulate the slider, in response to which the presentation cell outputs a value corresponding to the relative position of the slider between the upper and lower boundaries, and a user defined range for these boundaries. Presentation cells such as these are placed into a personal agent 300 by selecting the type of presentation cell from the cell library 305 and dragging and dropping it in the personal agent 300. A presentation cell 302 can take inputs from

either a service agent 240, or another presentation cell 302.

In this example, the slider presentation cell 302a controls a temperature, as indicated by text presentation cell 302d which is merely a text label. The slider presentation cell 302a would typically be coupled to a temperature data object in an object server 220, such that direct manipulation of the slider sends a request to communications gateway via object server to update

the stored data in the data object. Numeric presentation cell 302c and level indicator presentation cell 302b display the current value of some data object. In this example, the slider presentation cell 302a, the numeric presentation cell 302c, and the level indicator presentation cell 302b are all coupled to a same data object, so that changes in the slider position are reflected, in real time, by corresponding changes in the height of the level indicator and the value of the numeric display upon confirmation of the requested change by communications gateway.

Presentation cells 302 include various user configurable properties, such as data inputs and outputs, valid ranges of data inputs and outputs, position, border, and the like. In particular, the selection of the data objects in an object server 220 that are the inputs and outputs of a presentation cell 302 is managed through simple drag and drop operations.

In the preferred embodiment, various types of presentation cells are provided,

including standard presentation cells, background presentation cells, and telephony presentation cells.

Standard presentation cells are used to control and monitor devices 202 and 204. Standard presentation cells include four further types of cells:

**State monitors:** these are presentation cells that monitor the transition of a control point between two (or more) states, and graphically depict discrete changes in state. Exemplary state monitor presentation cells include bitmaps (which select a different bitmap to display depending on the state of the control point), colored shapes (which change color), text labels (which change text strings), and rotors (which rotate and change color dependent on state).

**Value monitors:** these are presentation cells that monitor and graphically depict continuous changes in the value of an attribute of a control point. Exemplary value monitor presentation cells include numeric displays and level indicators, as shown in Fig. 6, at 302c and 302b respectively.

**Controls:** these are presentation cells that allow user modification of an attribute of a field device or control application. Control cells include buttons to increment, decrement, or toggle a value (with user defined value changes); to pulse a value while depressed; numeric input dialogs for direct input of a numeric amount; and slider controls for continuously variable inputs (such as slider control 302a).

**Navigate cells:** these are presentation cells that enable the user to

navigate between different personal agent windows.

Background presentation cells display a passive bitmap image or text label, and are not associated with any field device.

Telephony presentation cells represent a mechanism for interpreting commands and monitoring field devices over a telephone system.

Examples of various types of presentation cells are further detailed in U.S. Patent No. 6,067,477.

#### SYSTEM OPERATION

Fig. 4 is an event trace depicting the operation of a system in accordance with one embodiment of the present invention. The interactions between the devices 202 and 204, the communications gateway 210, the object server 220, and the service agent 230, are shown.

The devices 202, 204 first initialize 410 with the communications gateway 210. The initialization process 410 includes informing the communications gateway 210 of the existence of these devices 202, 204, and the attributes that they have to offer. The communications gateway 210, in turn, communicates this information to the object server 220 by identifying 420 the devices 202 and 204 coupled to the communications gateway 210, their attributes.

The object server 220 now publishes 430 a list of all the identified devices 202

and 204. In one embodiment, the object server 220 keeps a registration of object types. The registration information includes how to address the objects, as well as a list of attributes for each object type. The list of attributes includes both a name of an attribute, as well as the type of an attribute. Because object types are registered, the system knows which attributes an object has.

Now a subscriber 230 can subscribe 440 to a particular device, or to a specific attribute of a particular device 202, 204.

The object server 220 then dynamically creates 450 the data object corresponding to that particular device 202, 204. In one embodiment, the created object will only have the attributes requested by the subscriber 230. In an alternate embodiment, the created object may have all its possible attributes.

The object server 220 then obtains data from the communications gateway 210 in order to populate the data objects that it has created. The subscriber 230 then subscribes to the populated object model, and, in this manner, obtains the data that it wanted.

Fig. 5 depicts a server side 502 and a client side 504, where the server side 502 comprises the object server 220, and the client side 504 comprises a personal agent 590. The personal agent in turn comprises a service agent 570, and a plurality of presentation cells 582, 584, 586, and 588.

It is to be noted that the objects and their attributes are not initially published



on the server side. Instead, a mere listing 505 of objects, along with their attributes, is published by the object server 220, which gets this listing from the communications gateway 210. Fig. 5 depicts such a listing 505 of Object 1, with Attributes 1, 2, and 3, and Object 2, with Attributes 1, 2, and 3, and Object 3 with Attributes 1 and 2. When the service agent 570 from the client side subscribes to particular attributes of specific objects, those objects are created on the server side. The objects are complex data structures which are difficult to transmit as they are across the network layer. Thus, in one embodiment, the complex data structures is serialized into data packets and transmitted across the network layer, and the objects (i.e. complex data structures) are reassembled on the client device.

In this case, Object 1 510, and Object 2 520, are created on the server side. A proxy 530 of Object 1 and a proxy 540 of Object 2 are generated on the service agent 570, each object proxy reflects its original address. In one embodiment, the objects 510, 520 created on the server side could have all the attributes of the objects. In another embodiment, the objects 510, 520 created on the server side could have only the attributes subscribed to by the service agent 570. Similarly, in one embodiment, the object proxies 530, 540 could have all the attributes of the objects. In another embodiment, the object proxies 530, 540 could have only the attributes subscribed to by the service agent 570.

Once the object proxies 530, 540 are created, each of the presentation cells

482, 484, 486 and 488 subscribe to a specific attribute. This subscription at the attribute level is possible, in one embodiment, because each attribute can be individually identified. Attribute names of a specific object type are known. Servers are known. Thus once the "object ID" (also known as "object address") is known, the attribute can be identified. In one embodiment, the addressing path for an attribute may be Server\_Name(IP Address).Object\_ID.Attribute\_Name.

Referring to Fig. 4 again, it is to be noted that since the system supports real time devices, continual updates of the data are preferably provided to the subscriber 230. The devices 202, 204 will provide 480 the communications gateway 210 with these updates, and the communications gateway 210 will, in turn, provide 484 the object server with updates. However, the communications gateway 210 will only provide the updates at the QOS requested by the subscriber 230. This is described below in the section on QOS.

Controlling the devices 202 and 204 follows an inverse process. In this case, a presentation cell invokes its service agent 240 to update a data object in the object server 220, passing in the updated value and address of the data object. The service agent 240 communicates with the object server 220, passing it the updated value. The object server 220 then communicates this update to the communications gateway 210, which controls the devices 202 and 204 and confirms the update of value back to object server. The computation of the updated value is determined by

the presentation cell, which may, for example, map the position of a slider on the screen display to an updated value for a controlled field device.

The communications gateway 210 acts as a single point which makes the decision to follow the instructions from a client device. Fig. 5B represents a situation where multiple client devices are connected to a single object server 220. In particular, two client devices, client device 1 and client device 2, are communicating with an object server 220, which in turn communicates with a communications gateway 210. Devices 202, 204 may, in such a scenario, be controlled by either client device 1 or client device 2, or both. If client device 1 and client device 2 both attempt to control, say attribute 1 of device 202, then the communications gateway 210 will decide how to prioritize these requests. Thus, because there is a single point (the communications gateway 210) which makes decisions regarding which instructions to follow, there is no confusion even when multiple clients attempt to control an attribute of a device 202, 204 at the same time.

#### QUALITY OF SERVICE

In another aspect of the present invention, the Quality Of Service (QOS) capabilities of publishers can be matched with the QOS requirements of subscribers.

Fig. 6A illustrates that in a system in accordance with one embodiment of the present invention, the communications gateway 210 also identifies 610 to the object

server 220, the Quality of Service (QOS) that the communications gateway 210 can offer. The QOS may include a frequency at which the value of the real time data is revised, and a tolerance of the real time data, or any other useful metric that describes the QOS capabilities of the communications gateway. The QOS offered by the communications gateway will depend, at least in part, upon how fast it can get updated information from the devices 202 and 204.

When the subscriber 230 subscribes 440 to a particular object, the subscriber informs the object server 220 of the QOS requested 620 by the subscriber 230. The object server 220 will now ascertain whether the communications gateway 210 can provide the QOS requested 620 by the subscriber 230. If not, the object server 220 informs the subscriber 230 that the QOS that it desires cannot be provided by the communications gateway 210. The subscriber 230 can then choose to connect to another object server and/or communications gateway. Alternatively, the subscriber 230 can choose to accept the QOS that the communications gateway 220 can provide, even though is lower than the QOS originally requested by the subscriber 230.

If the object server 220 determines that the communications gateway 210 can provide the QOS requested 620 by the subscriber 220, the object server 220 will inform 630 the communications gateway 210 of the QOS requested by the subscriber 230. The object server 220 will then dynamically create the data objects

subscribed to by the subscriber 230, and the subscriber 230 will subscribe to these.

As discussed above, since the present invention supports real time systems, it is preferable that continual updates of the data be provided to the subscriber 230. However, the communications gateway 210 will only provide the updates at the Quality Of Service requested by the subscriber 230. Therefore, even if the devices 202 and 204 provide 480 to the communications gateway 210 at a higher speed, the communications gateway 210 will filter 482 these based on the QOS requirements of the subscriber 230, and only provide 482 the object server 220 with updates at a rate sufficient to satisfy the QOS requested by the subscriber 230. The object server 220, in turn, provides the service agent 240 with the updates 488.

In the case that there is more than one subscriber 230, there may be more points at which QOS filtering is performed – once at the communications gateway 210, and again at the object server 220. For example, Fig. 6B represents the embodiment where two subscribers (subscriber 1 and subscriber 2) are subscribing to object server 220. As before, the communications gateway 210 will inform 650 the object server 220 of the QOS it can offer. Subscriber 1 and subscriber 2 will each communicate to the object server 220 the QOS that they require.

With multiple subscribers 230, 605 the object server 220 must determine whether the communications gateway 210 can provide the QOS requirements of each of the subscribers. If not, in one embodiment, the object server 220 informs

subscriber 1 and/or subscriber 2, that the QOS that it desires cannot be provided by the communications gateway 210. Subscriber 1 and/or 2, can then choose to connect to another object server and/or communications gateway. Alternatively, subscriber 1 and/or 2, can choose to accept the QOS that the communications gateway 220 can provide, even though is lower than the QOS originally requested by the subscriber 230.

In the latter case, or in the case that communications gateway 210 can provide the QOS requested by both subscriber 1 and 2, in one embodiment, the communications gateway 210 will provide the greater of the QOS requirements of subscriber 1 and subscriber 2. The object server will then, in one embodiment provide subscriber 1 with the QOS that it requested, and provide subscriber 2 with the QOS that it requested.

Referring back to Fig. 4, it can be seen that this is an example of an instance in which there would be a second QOS filtering 486 (in addition to the QOS filtering 482 at the communications gateway 210) at the object server 220, before it provides the service agent 240 with updates 488. In another embodiment, both subscribers 1 and 2, may receive the highest QOS requested by any of the subscribers.

#### MULTIPLE SUBSCRIBERS AND RE-PUBLISHERS

Referring to Fig. 7, it can be seen that, in one embodiment, a "chaining"

feature involving subscribing to data and republishing it, can be performed. The system shown in Fig. 7 comprises an object server 720, a subscriber 730, and a personal agent 750. Both the subscribers comprise of service agents 740 and 760. However, only the personal agent 750 includes presentation cells 772, 774, and 776. Three servers 702, 704, and 706 are involved in this system. For example, the object server 720 resides on server one 702, the subscriber 730 resides on server two 704, and the personal agent 750 resides on server three 706. One of ordinary skill in the art will note that it is possible for the object server 720, the subscriber 730, and the personal agent 750, to be on less than three servers. Two or more of these could be on the same server.

In the scenario depicted in Fig. 7, the object server 720 serves as the original publisher of the data. The service agent 740 on subscriber 730 then subscribes to the data. Subscriber 730 then may or may not reformat the data, before it republishes it. Service agent 760 on personal agent 750 now treats subscriber 730 as the publisher of data, and subscribes to the data published by subscriber 730. Finally, a user can get access to the data subscribed to by personal agent 750, by means of the presentation cells 772, 774, and 776.

One skilled in the art will note that such "chaining" need not be limited to that described above, but can in fact be performed with subscribing and re-publishing multiple times.

### CELL TEMPLATES

In one embodiment of the present invention, it is possible to create “cell templates,” and publish them. A published cell template can be subscribed to and used when desired. Use of such pre-created cell templates saves time because each subscriber does not need to recreate it every time. Further, such pre-created cell templates also have the added benefit that experts in a field can set up appropriate cell templates, and subscribers with less experience can then benefit from their expertise. Creators of cell templates may, in one embodiment, permit subscribers to access the cell templates for free. In another embodiment, a fee may be charged for subscribing to cell templates. In yet another embodiment, certain cell templates may be available for free, while others are available for a fee.

#### Creation of Cell Templates:

Fig. 8A demonstrates how cell templates are created. An object type to which the cell template is to be linked is first assigned 810 to it. Next, the cells to be included in the cell template must be selected 820. One or more actions must then be assigned 830 to each of these cells. Each action must then be assigned 840 to an attribute of the object type.

Fig. 8B illustrates an example of a cell template. The object type 842 to which



the cell template is linked could be a room in a building. For the cell template shown in Fig. 8B, a rotor 844 and a slider 846 have been selected 820 for inclusion in it. The rotor 844 and the slider 846 are assigned 830 some actions, corresponding to some attributes, as depicted by 848. For instance, the rotor could be assigned the action of rotating when a fan in a room is turned on. The rotor could be assigned an action of blinking when the temperature in the room goes above a certain threshold. Similarly, the slider can be assigned the action of sliding in order to control a light level in a room. In addition, it can also be assigned the action of blinking when the level of light in the room goes below a certain threshold.

Once created, such cell templates can be published, so that subscribers can have access to them.

#### Use of Cell Templates:

Published cell templates can be subscribed to. Once a cell template is obtained, it can be used by mapping the desired objects on to it.

Fig. 8C represents how cell templates are used. Fig. 8C shows a cell template 850, and two objects 860, 870. In order to map the objects on to the cell template, the objects 860, 870 must be of the same type as the cell template 850.

Each object 860, 870 is then mapped on to the cell template 850. Each attribute of every object 860, 870 then automatically gets mapped on to the attributes

defined in the cell template 850. In addition, as shown in Fig. 8C, the addresses of the objects 860, 870 to be mapped on to the cell template 850 must also be provided. The objects 860, 870 to be mapped, along with their addresses, can be obtained from the list of publishable objects published by the object server 220.

Thus the cell template in Fig. 8B above can be mapped to a specific room in a particular building. The fan cell will then automatically be linked to a fan in the room, and the slider cell will then automatically be linked to the light level monitors/controls in the room.

#### SPECIFIC APPLICATIONS

The present invention can be embodied in several varied applications. The following are a few examples of some such applications.

#### Facility Management

One embodiment can be used for facility management. In a facility management system, the real time data that needs to be monitored and/or controlled could be for many different types of field devices, such as lights, heating units, thermostats, window controls, ventilation systems, elevator banks, and so forth.

An example would serve to illustrate how such a system could be used for facility management. Assume that the system is monitoring and controlling the management of a building. In response to specific events occurring in the building, specified personnel will be automatically notified. For instance, if an alarm takes place in the Heating/Ventilation/Air Conditioning (HVAC) system, the Building Engineer may be notified. Further, if the event remains unattended for a predetermined period of time, an alternate action may be taken by the system. For instance, if no action is taken on the alarm in the HVAC system for a predetermined period of time, the system may dispatch a work-order to a contracting company via the Internet.

In addition, the system also monitors the equipment, so that the contractor, in response to the work-order, could access real time data to detect the failure / *determine the fault accurately*. Thus the contractor could use the system to diagnose (and possibly fix) the problem.

In general terms, where the system is used for maintenance management, the field engineers may be the ones to connect the real time devices in the field to the communications gateway. The maintenance engineers can then monitor these devices from a remote location, by observing their output as published by the object server. Alternately, the maintenance engineers can set up personal agents to monitor certain systems of devices on their behalf. The personal agents can also be

set up to create alerts and/or notify the maintenance engineers or other appropriate people when certain events occur.

Another example of use of a system in accordance with the present invention follows. Assume a company builds industrial chemical dispensing machines, which are used in swimming pools and in large washing plants. These machines can be connected to the engineers who maintain them, via a such a system.

Here, the engineers could program the personal agents to monitor devices that are assigned to them, and to send a pager message to them when an alarm in such a device goes off. Upon receiving such an alert, an engineer could monitor the real time data from that device using the system, so as to diagnose, and perhaps fix, the problem.

In addition, experienced engineers may create cell templates containing predictive maintenance logic for various devices. If published, these templates could also be used by less experienced engineers. Such use could either be for a fee, or for no cost.

### Energy Trading

Another embodiment can be used for managing energy trading. Several possible scenarios can illustrate how the present invention can be applied to energy trading.

One scenario includes remotely monitoring total energy use for a building or facility, as well as current consumption of energy for the building or facility. This can be done by connecting the energy meters in the facility to a communications gateway, which in turn is connected to the object server which publishes this data. This published data can then be remotely accessed.

In an alternate scenario, the published data may not need to be physically monitored by anybody. Instead, one or more personal agents can simply be personalized to set up monitoring of certain attributes, and to control specific attributes. For instance, a personal agent may monitor total energy use in a facility. Further, if the total energy use exceeds a certain threshold level, the personal agent may switch off, for instance, the air conditioning system in the facility. Another example of personalizing a personal agent is starting a generator automatically when the power goes off.

In yet another scenario, multiple buildings may purchase energy on an aggregate basis. An example may help to illustrate this. For instance, assume that a building-owner owns 10 buildings in a town. The building owner may then purchase energy for all the 10 buildings together. The pricing and/or availability of energy may then be based on the aggregate energy requirements of the 10 buildings. In such a situation, only the aggregate energy requirements need be monitored. Thus even if the energy consumption by one building exceeds a certain

threshold, if the aggregate sum of the energy requirements of the other buildings does not exceed the total threshold for the 10 buildings, the energy requirements of all the building may be satisfied. The personal agent may thus monitor only the aggregate energy requirements and usage in this case.

Another possible scenario may be best understood by further elaborating on the above example. Assume that the above building owner has signed separate contracts with two energy suppliers, supplier A and supplier B to provide energy to the buildings. The contracts require the building-owner to buy energy at least 30 minutes in advance of when it is required. Also assume that supplier B is more expensive than supplier A. One embodiment may be used to accurately predict usage for the next 30 minutes. This system monitors real-time trends of energy usage from all subsystems utilizing energy in each building, where appropriate objects have been defined and presentation cells have been set up. Such subsystems could include Heat/Ventilation/Air-Conditioning (HVAC) and lighting, database applications (e.g. reservation systems), etc. The system could then aggregate the power requirements of all the 10 buildings owned by the building-owner. By default, the system would serve to buy power from supplier A, and resort to supplier B only when the requirement for energy exceeds the energy supply available from supplier A.

Further, a personal agent for such a system may also be programmed to keep

a watch on the Internet for new offers from other energy suppliers, and could automatically place a request for a quotation with energy usage data when such offers are available, or alternately, on a periodic basis (e.g. once an hour). In addition, the system could also notify the building-owner when such an offer is available, and confirm a deal and send an authorization when appropriate. In one embodiment of the present invention, this could be done by the building-owner programming his personal agent to perform these tasks.

One example of an “energy-exchange” functionality of one embodiment of a system in accordance with the present invention is depicted in Fig. 9. Fig. 9 depicts a building 910, a system 920 in accordance with the present invention, an energy supplier 930, and a local supplier 940 of energy. The local supplier 940 provides energy in a local area for contracts committed to by the energy supplier 930.

The building 910 first transmits 915 its real time energy requirements. This could include information regarding the occupancy of the building, its instantaneous energy usage, weather information, etc. The system 920 then transmits 925 this information to the energy supplier 930. The energy supplier 930 in turn provides 932 a real time price quote for the energy requirements of the building 910. Based on this price quote, the system 920 accepts 934 (or rejects) the deal offered by the energy supplier 930. The system 920 and building 910 then communicate with each other to confirm 936 the contract. Once the contract is confirmed, the energy

supplier 9330 transmits 938 a request for a local supplier 940 located in the same local area as building 910, to provide the building with the requested real time energy. The system 920 communicates 945 this request to the local supplier 940.

### Bandwidth Trading

Another system in accordance with the present invention can also be used to manage and control bandwidth trading. Similar to the energy trading application above, a personal agent can be set up to monitor bandwidth usage and requirements. Further, these can also be predicted by observing bandwidth usage per person, and occupancy of a facility. Again, this can be best understood by means of an example.

Assume a building-owner has signed two contracts for bandwidth purchasing with two different networks, Network A and Network B. Further, assume that the network connection is used by the building for two purposes: for providing Internet access to the tenants of the building, and for connecting the Building Management System to remote maintenance contractors.

Moreover, assume say that Network A provides a low cost package of unlimited access with a fixed bandwidth, while Network B offers a connection with a higher quality of service, which is more expensive. Thus Network A is sufficient for regular use in normal conditions, but Network B may be needed in urgent situations,



when a high quality of service is required. For instance, a high quality of service may be needed when a work-order is dispatched by the system to a maintenance contractor, and the contractor needs to monitor- real time system parameters to diagnose the problem. When a request for a higher quality of service is detected, the system may automatically switch to Network B.

#### Other Applications

The above are only a few examples of applications for which a system in accordance with the present invention can be used. Other instances where such a system can be used include creating a health portal, and for process control monitoring (e.g. in chemical plants). One skilled in the art will note that there are several other applications for which a system in accordance with the present invention can be used.

As will be understood by those familiar with the art, the invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. Likewise, the particular capitalization or naming of the modules, protocols, features, attributes, data structures, or any other aspect is not mandatory or significant, and the mechanisms that implement the invention or its features may have different names or formats. Accordingly, the disclosure of the

present invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

## CLAIMS

1. A computer implemented method for managing real-time data from distributed devices that control or monitor physical or logical entities, the devices having attributes representative of states of the entities, the method comprising:
  - identifying the devices communicatively coupled to a communications gateway;
  - publishing a list of the identified devices and their attributes;
  - responsive to receiving, from a subscriber, a request for at least one attribute of at least one device:
    - creating at least one data object corresponding to the requested device in an object server communicatively coupled to the communications gateway; and
    - establishing a link from the subscriber to the at least one data object; and
    - transmitting the real time data for the at least one requested attribute of the at least one data object to a service agent on the subscriber, wherein the service agent is communicatively coupled to the object server.
2. The method of claim 1, further comprising:

receiving a command directed towards the at least one requested attribute of the  
at least

one data object;

transmitting, via the service agent, the received command to the object server;

and

transmitting the received command to the device corresponding to the at least  
one data

object via the communications gateway.

3. The method of claim 1, further comprising:

receiving a defined cell template comprising at least one cell, wherein the defined

cell

template comprises a mapping of at least one attribute of a data object  
type onto the at least one cell in the cell template;

publishing the defined cell template on a remote host computer;

linking an instance of the defined cell template to at least one specific data object  
of the data object type; and subscribing the at least one cell in the cell  
template to a corresponding at least one attribute of the linked data object.

4. The method of claim 1, wherein the subscriber is a personal agent comprising  
at least one service agent and at least one cell, the method further comprising:

creating a personal agent on a client device, wherein the personal agent  
comprises:

at least one service agent;

at least one cell subscribing to an attribute of a data object via the service agent;

computing, by the at least one cell, a desired output from the real time data corresponding to the at least one requested attribute of the at least one data object; and

placing the personal agent on to a remote host computer.

5. The method of claim 4, further comprising:

providing access to the desired output of the personal agent via an interface chosen by the user.

6. The method of claim 4, further comprising:

publishing, as at least one data object with at least one attribute, the desired output

of the personal agent, where the published data object may be subscribed to by a second subscriber.

7. The method of claim 4, further comprising:

allowing access to the personal agent, by permitting its withdrawal from the remote host computer;

allowing modification of the at least one cell of the personal agent; and

placing the modified at least one cell of the personal agent to a remote host computer.

8. A computer implemented method for managing quality of service requirements of subscribers, with quality of service capabilities of communications gateways, wherein the communications gateways provide real time data for distributed devices that control or monitor physical or logical entities, the devices having attributes representative of states of the entities, the method comprising:

receiving, from at least one communications gateway, a quality of service level that the at least one communications gateway can provide;

receiving, from at least one subscriber, a quality of service requested by the at least one subscriber; and

responsive to the quality of service level being sufficient to meet the quality of service requested by the at least one subscriber:

informing the communications gateway of the quality of service requested by the at least one subscriber; and

providing the subscriber with the quality of service requested by the at least one subscriber.

9. The method of claim 8, further comprising:

responsive to the quality of service level being unable to meet the quality of

service requested by the at least one subscriber, notifying the at least one subscriber that the quality of service requested by the at least one subscriber cannot be provided by the at least one communications gateway.

10. The method of claim 8, wherein notifying the at least one subscriber further comprises offering the at least one subscriber an option of switching to a second communications gateway providing a quality of service level that is sufficient to meet the requested QOS.

11. The method of claim 8, wherein providing the at least one subscriber with the quality of service requested by the at least one subscriber comprises:

responsive to a communications medium being unable to support the quality of service requested by the at least one subscriber, switching to an alternate communications medium that is able to support the quality of service requested by the at least one subscriber.

12. A computer implemented method for managing quality of service requested by subscribers, and quality of service levels provided by communications gateways, wherein the communications gateways provide real time data for distributed devices that control or monitor physical or logical entities, the devices having attributes representative of states of the entities, the method comprising:

receiving, from a communications gateway, a quality of service level that the communications gateway can provide;

receiving, from a first subscriber, a quality of service requested by the first subscriber;

receiving, from a second subscriber, a quality of service requested by the second subscriber; and

responsive to the quality of service level being sufficient to meet the quality of

service requested by the first subscriber, but being insufficient to meet the quality of service requested by the second subscriber:

informing the communications gateway of the quality of service requested by the first subscriber;

providing the first subscriber with the quality of service requested by the first subscriber; and

notifying the second subscriber that the quality of service requested by the second subscriber cannot be provided by the communications gateway.

13. The method of claim 12, further comprising:

responsive to the quality of service level supported by the communications

gateway being sufficient to meet the quality of service requested by each of the first and the second subscribers:

informing the communications gateway of the greater of the quality of service requested by the first subscriber and the second subscriber;

providing the first subscriber with the quality of service requested by the first subscriber; and

providing the second subscriber with the quality of service requested by the second subscriber.

14. The method of claim 12, further comprising:

responsive to the quality of service level being insufficient to meet the quality of



service requested by both the first and the second subscribers, notifying each of the first and the second subscribers that the quality of service requested by each subscriber cannot be provided by the communications gateway.

15. A computer implemented system for managing real-time data from distributed devices that control or monitor physical or logical entities, the devices having attributes representative of states of the entities, comprising:

a communications gateway communicatively coupled to selected ones of the devices to receive real time data from the devices, the real time data formatted according to a communications protocol associated with the devices, the communications gateway converting the received real time data to standardized real time data in a standard data format independent of the devices that specifies for each item of real time data a content and source of the real time data;

an object server communicatively coupled to the communications gateway to receive information regarding the standardized real time data, and to publish a list of the devices and their attributes; and

a subscriber communicatively coupled to the object server, to subscribe to at least one particular attribute of a specific device from the list published by the object server, and in response to which the object server creates at least one data object corresponding to the specific device, the at least one data object having attributes corresponding to attributes of the specific device, the subscriber comprising:

at least one service agent communicatively coupled to the object server  
to receive standardized real time data of the specific data object.

16. The system of claim 15, the subscriber being a personal agent, further comprising:

at least one presentation cell, each presentation cell providing a representation of a device that is dynamically responsive to real time changes in the attributes of the device, each presentation cell communicatively coupled to the at least one service agent to receive from the at least one service agent the standardized real time data, and mapping the standardized real time data to an output representation.

17. A computer implemented method for managing real-time data from distributed devices that control or monitor physical or logical entities, the devices having attributes representative of states of the entities, the method comprising:

on a first host system:

identifying the devices communicatively coupled to a communications gateway;

publishing a list of the identified devices and their attributes;

on a second host system:

from the published list, requesting at least one attribute of at least one device;

on the first host system:

responsive to receiving, from a subscriber, a request for at least one attribute of at

least one device:

creating at least one data object corresponding to the requested device in

an object server communicatively coupled to the communications gateway; and

establishing a link from the subscriber to the at least one data object; and

transmitting the real time data for the at least one requested attribute of the at least

one data object to a service agent on the subscriber, wherein the service agent is communicatively coupled to the object server;

on the second host system:

republishing the transmitted data;

on a client device:

subscribing to the republished data;

representing the subscribed-to data on at least one presentation cell.

18. A computer program product stored in a computer readable medium for controlling a client device to perform a method for managing real-time data from distributed devices that control or monitor physical or logical entities, the devices having attributes representative of states of the entities, the method comprising:

identifying the devices communicatively coupled to a communications gateway;

publishing a list of the identified devices and their attributes;  
responsive to receiving, from a subscriber, a request for at least one attribute of  
at least

one device:

creating at least one data object corresponding to the requested device in  
an

object server communicatively coupled to the communications  
gateway; and

establishing a link from the subscriber to the at least one data object; and  
transmitting the real time data for the at least one requested attribute of the at  
least one

data object to a service agent on the subscriber, wherein the service agent  
is communicatively coupled to the object server.

19. A computer program product stored in a computer readable medium for  
controlling a client device to perform a method for managing quality of service  
requirements of subscribers, with quality of service capabilities of communications  
gateways, wherein the communications gateways provide real time data for distributed  
devices that control or monitor physical or logical entities, the devices having attributes  
representative of states of the entities, the method comprising:

receiving, from at least one communications gateway, a quality of service level  
that the at least one communications gateway can provide;

receiving, from at least one subscriber, a quality of service requested by the at  
least one subscriber; and

responsive to the quality of service level being sufficient to meet the quality of service requested by the at least one subscriber:

informing the communications gateway of the quality of service requested by the at least one subscriber; and

providing the subscriber with the quality of service requested by the at least one subscriber.

20. A set of computer program products stored on computer readable mediums for controlling a client device to perform a method for managing real-time data from distributed devices that control or monitor physical or logical entities, the devices having attributes representative of states of the entities, the method comprising:

on a first host system:

identifying the devices communicatively coupled to a communications gateway;

publishing a list of the identified devices and their attributes;

on a second host system:

from the published list, requesting at least one attribute of at least one device;

on the first host system:

responsive to receiving, from a subscriber, a request for at least one attribute of at

least one device:

creating at least one data object corresponding to the requested device in

an object server communicatively coupled to the communications gateway; and

establishing a link from the subscriber to the at least one data object; and

transmitting the real time data for the at least one requested attribute of the at least

one data object to a service agent on the subscriber, wherein the service agent is communicatively coupled to the object server;

on the second host system:

republishing the transmitted data;

on a client device:

subscribing to the republished data;

representing the subscribed-to data on at least one presentation cell.

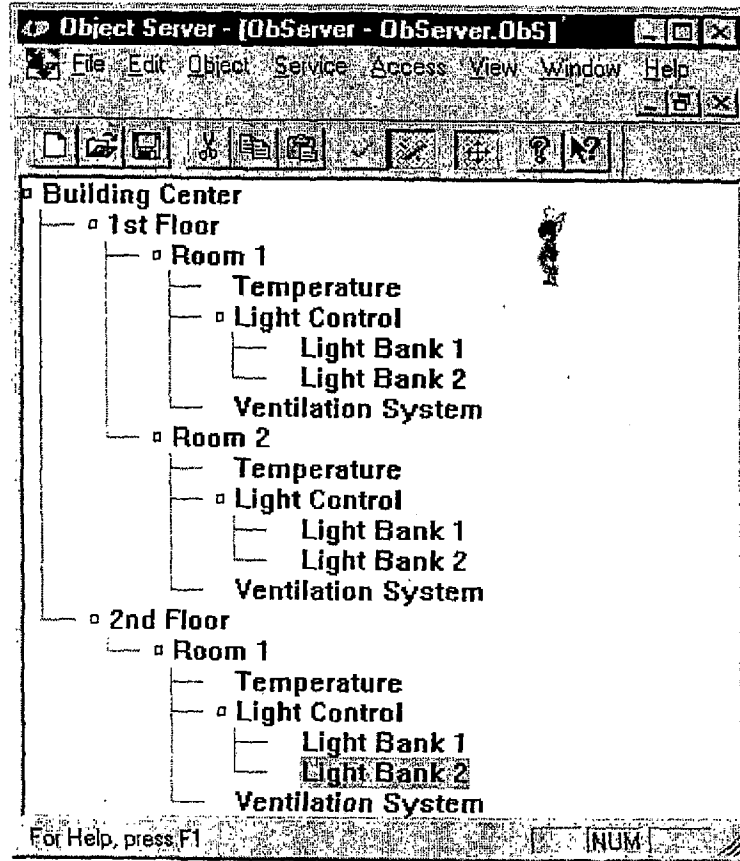


FIG. 1A

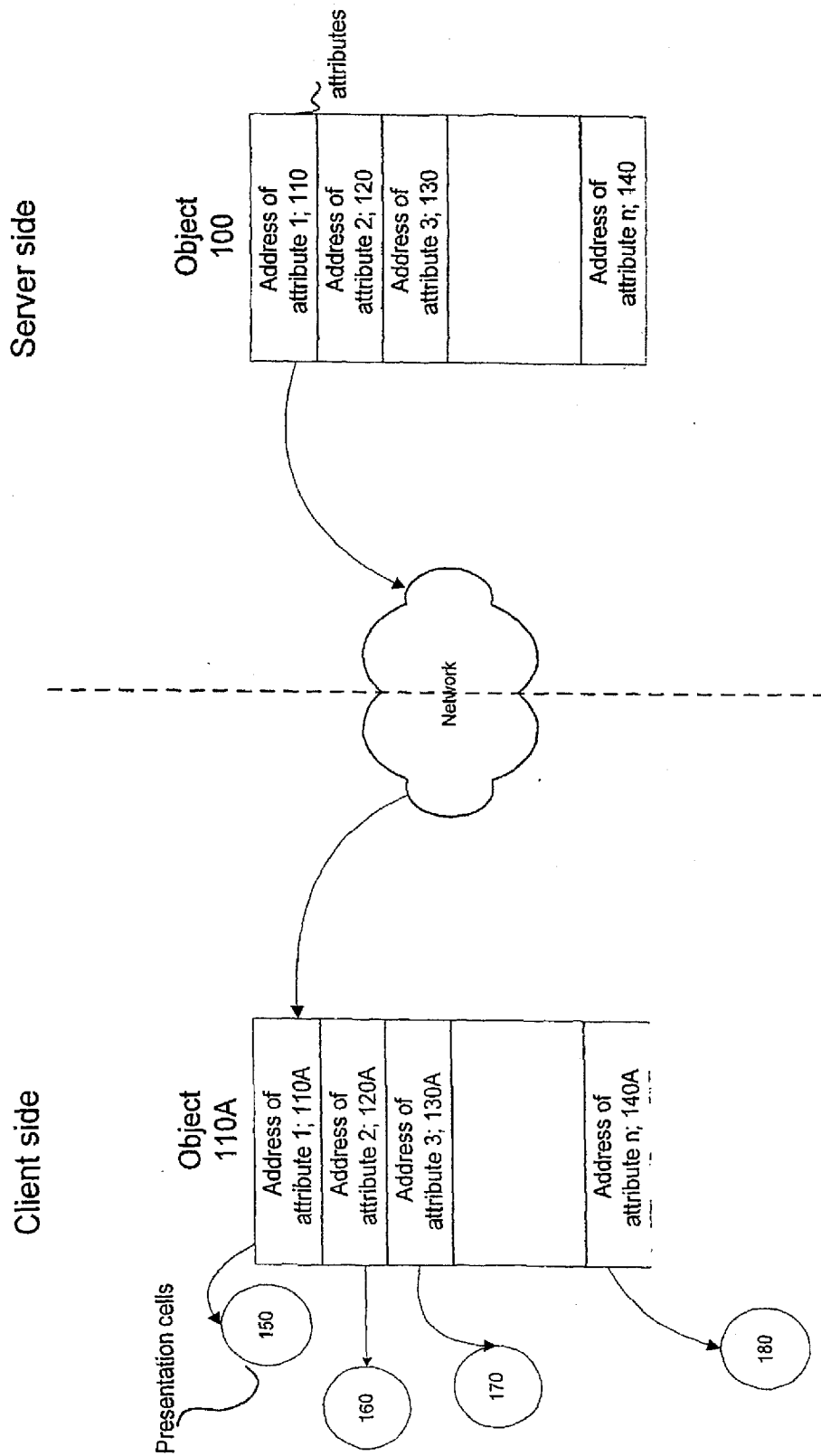


Figure 1B



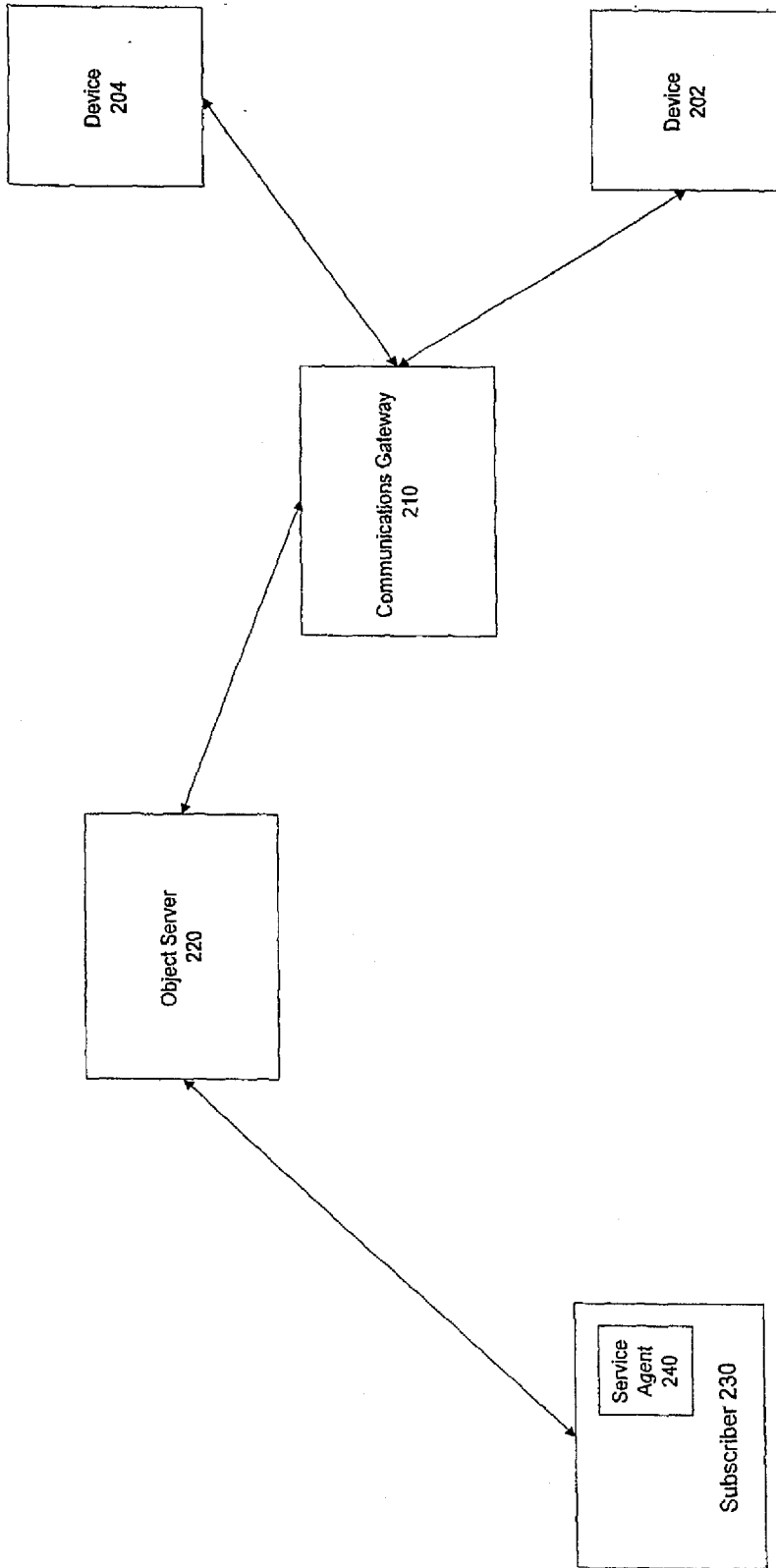


Figure 2

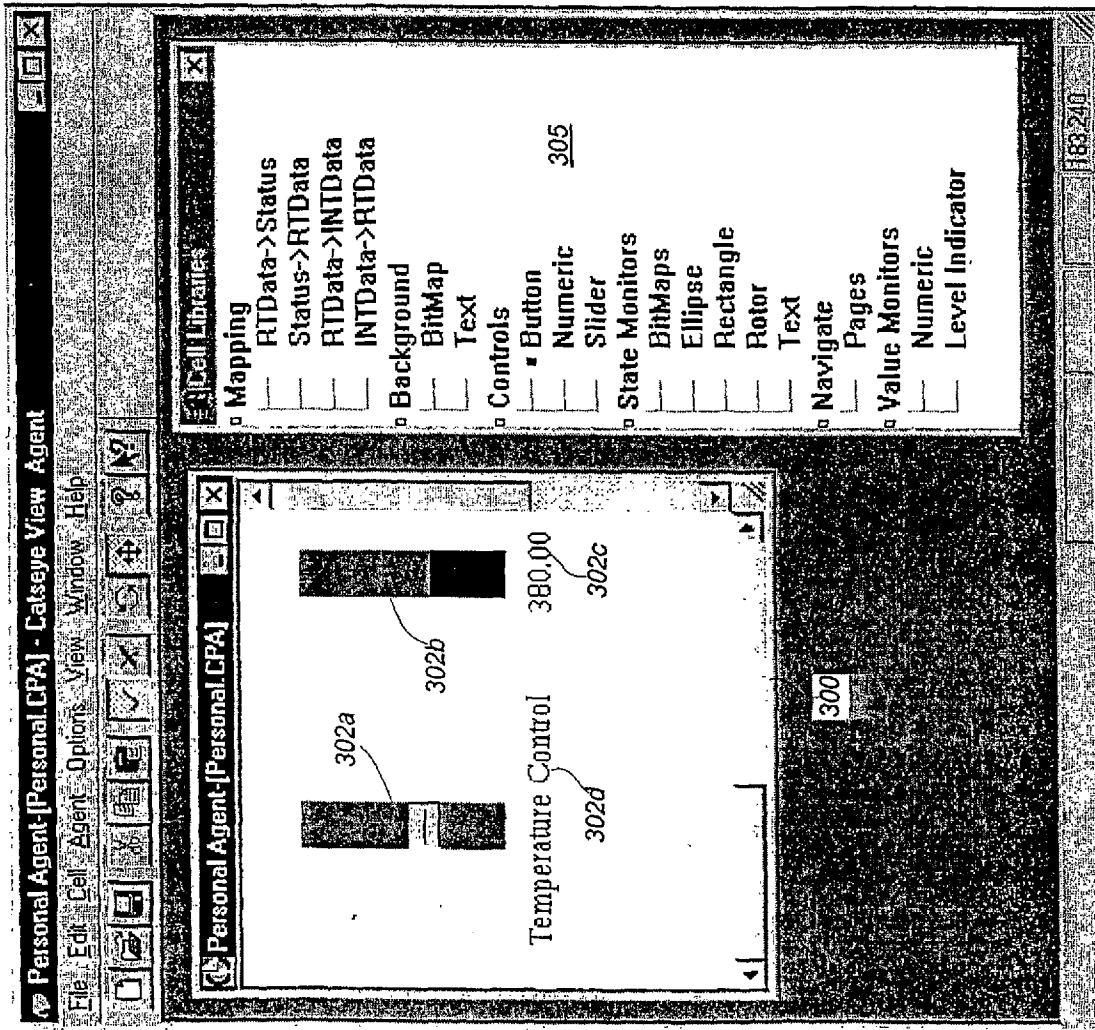


FIG. 3

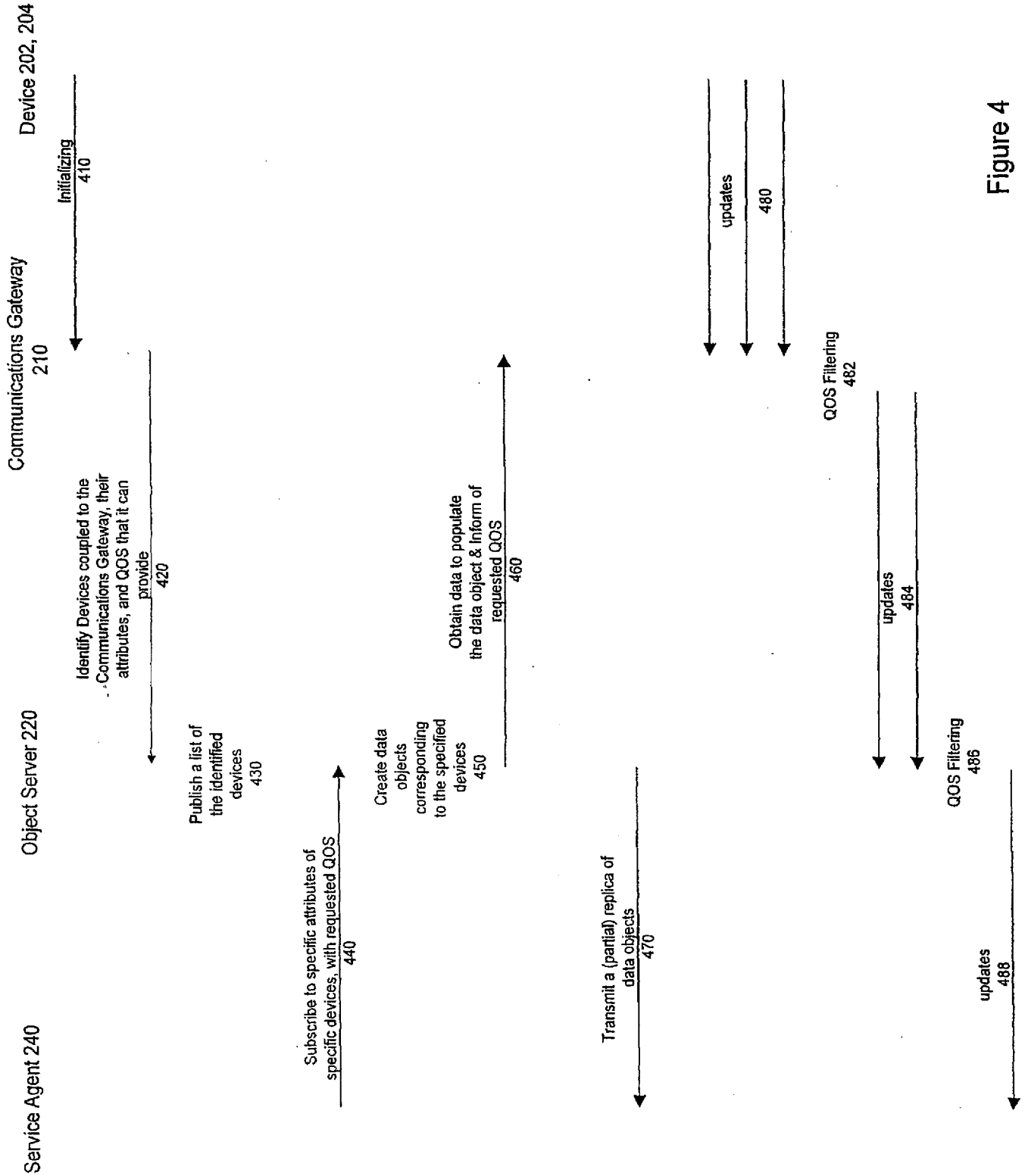


Figure 4

Server side 502

Client side 504

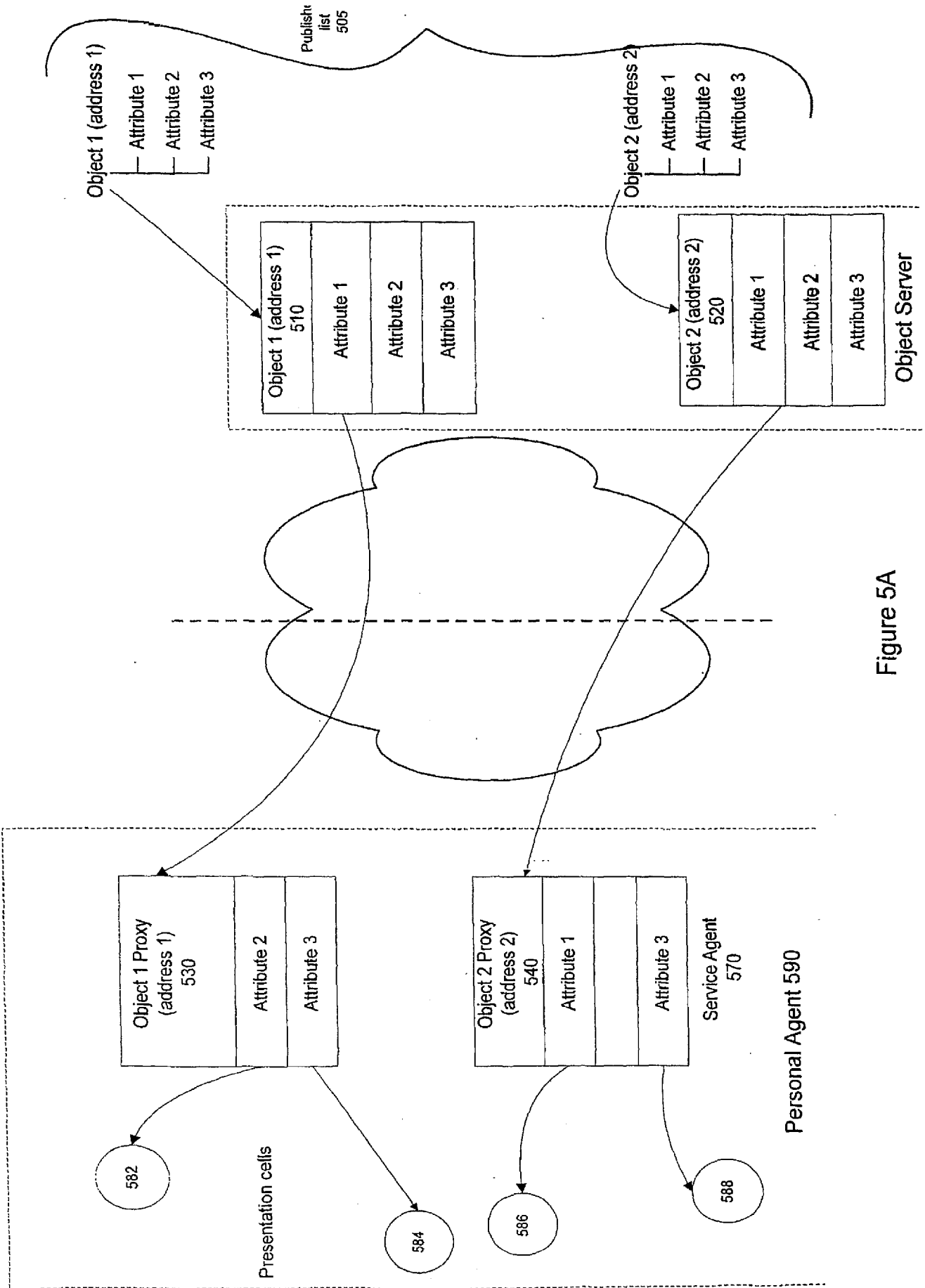


Figure 5A

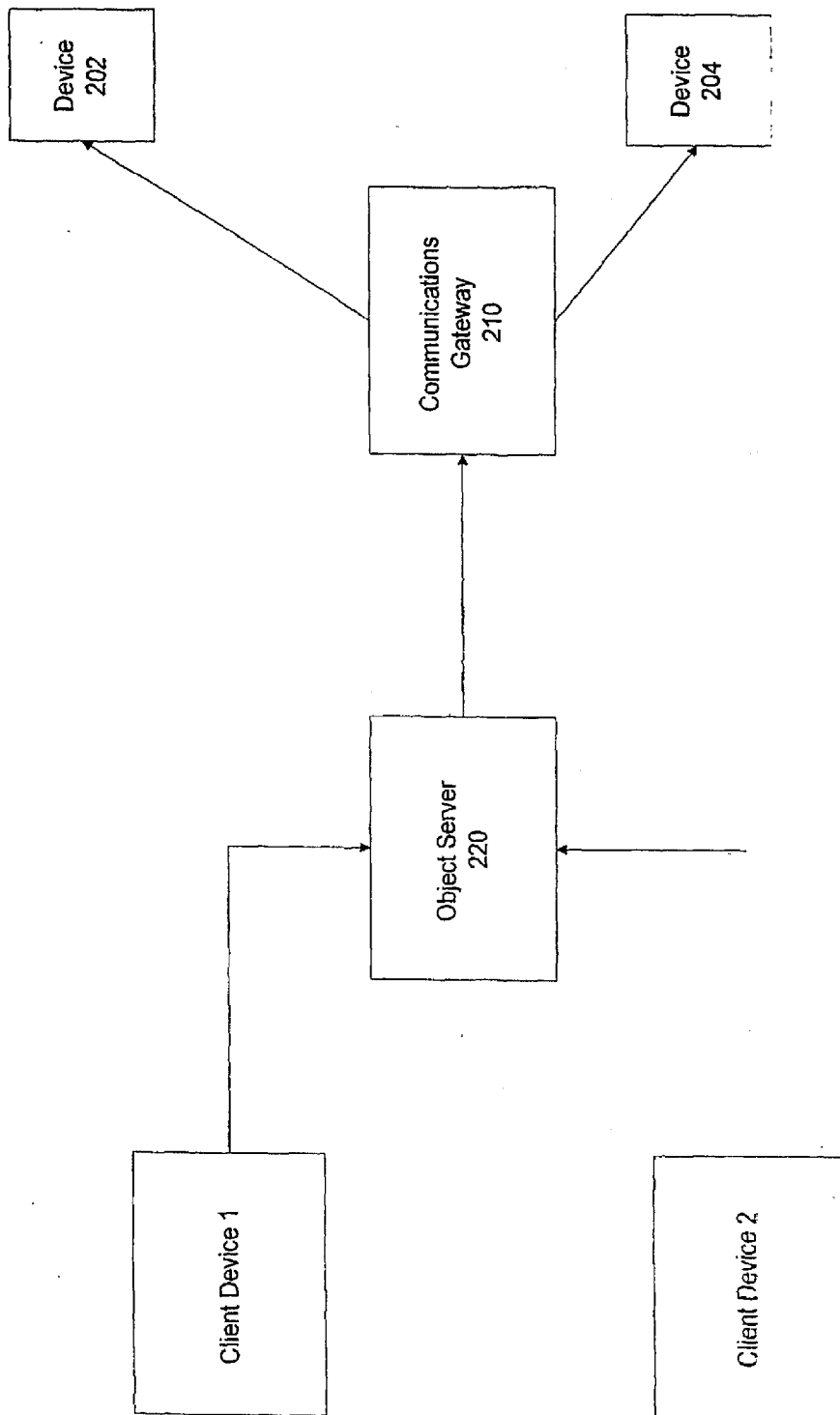


Figure 5B

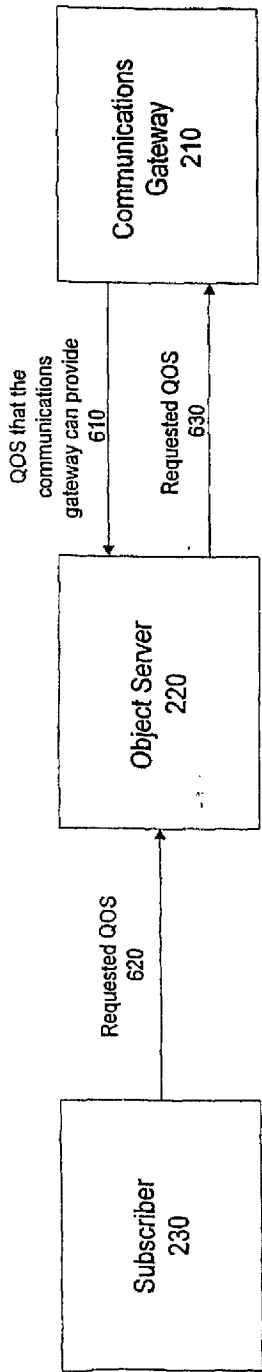


Figure 6A

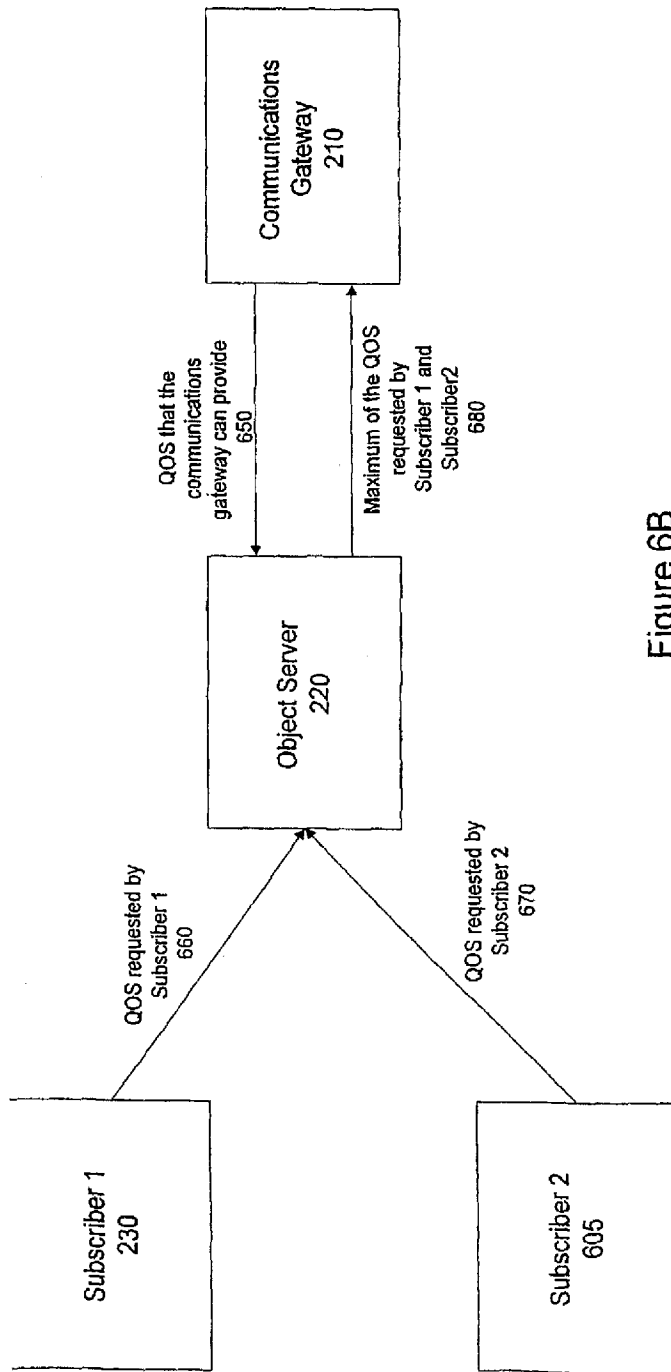


Figure 6B

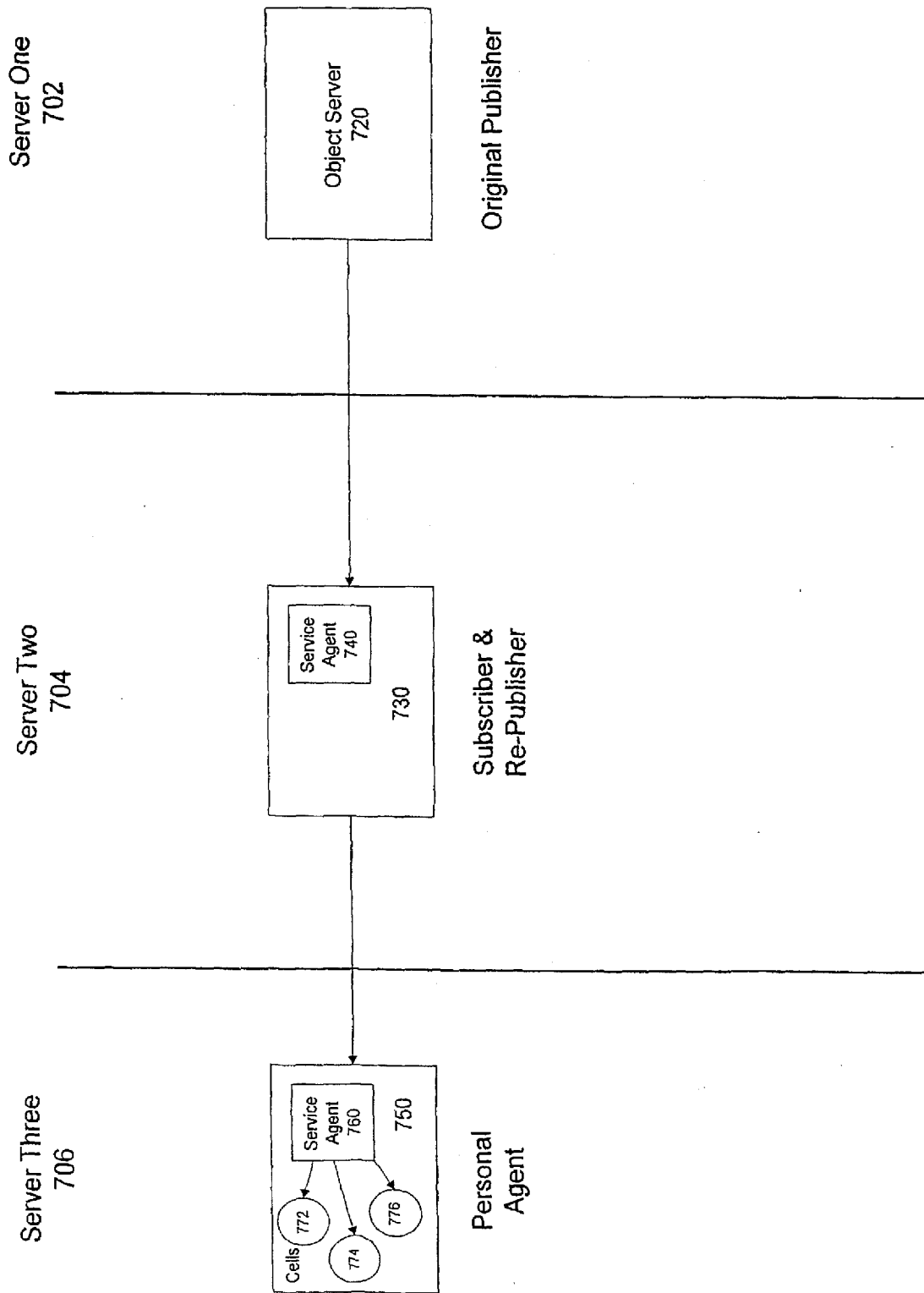


Figure 7

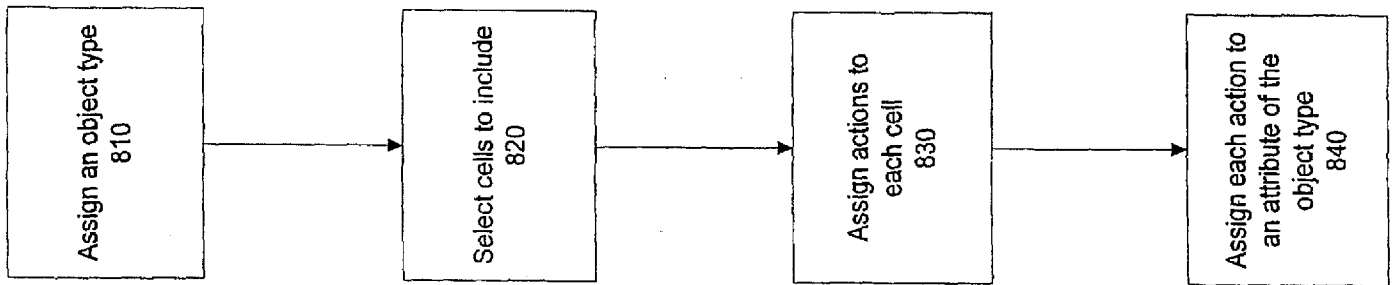


Figure 8A



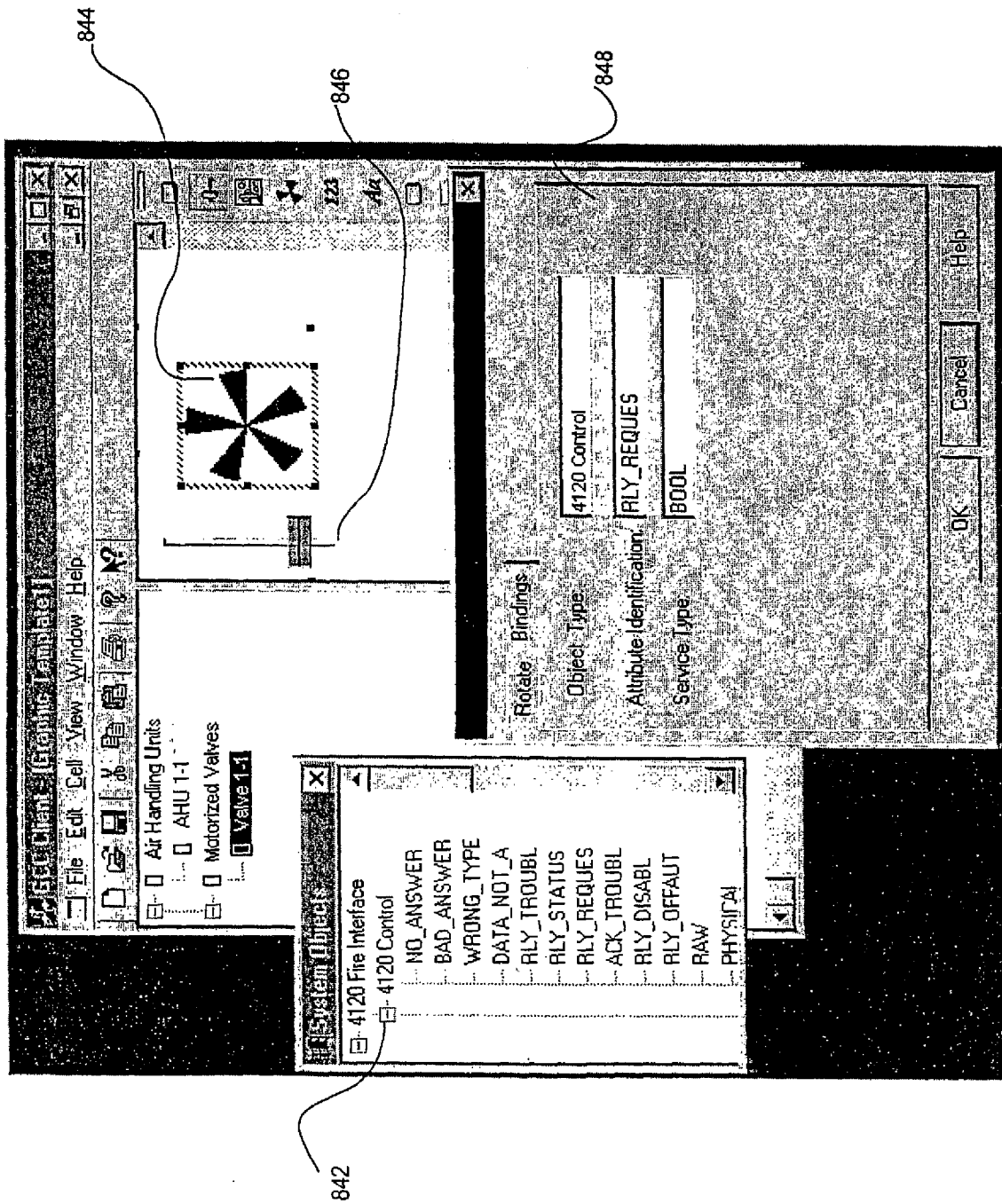


Figure 8B

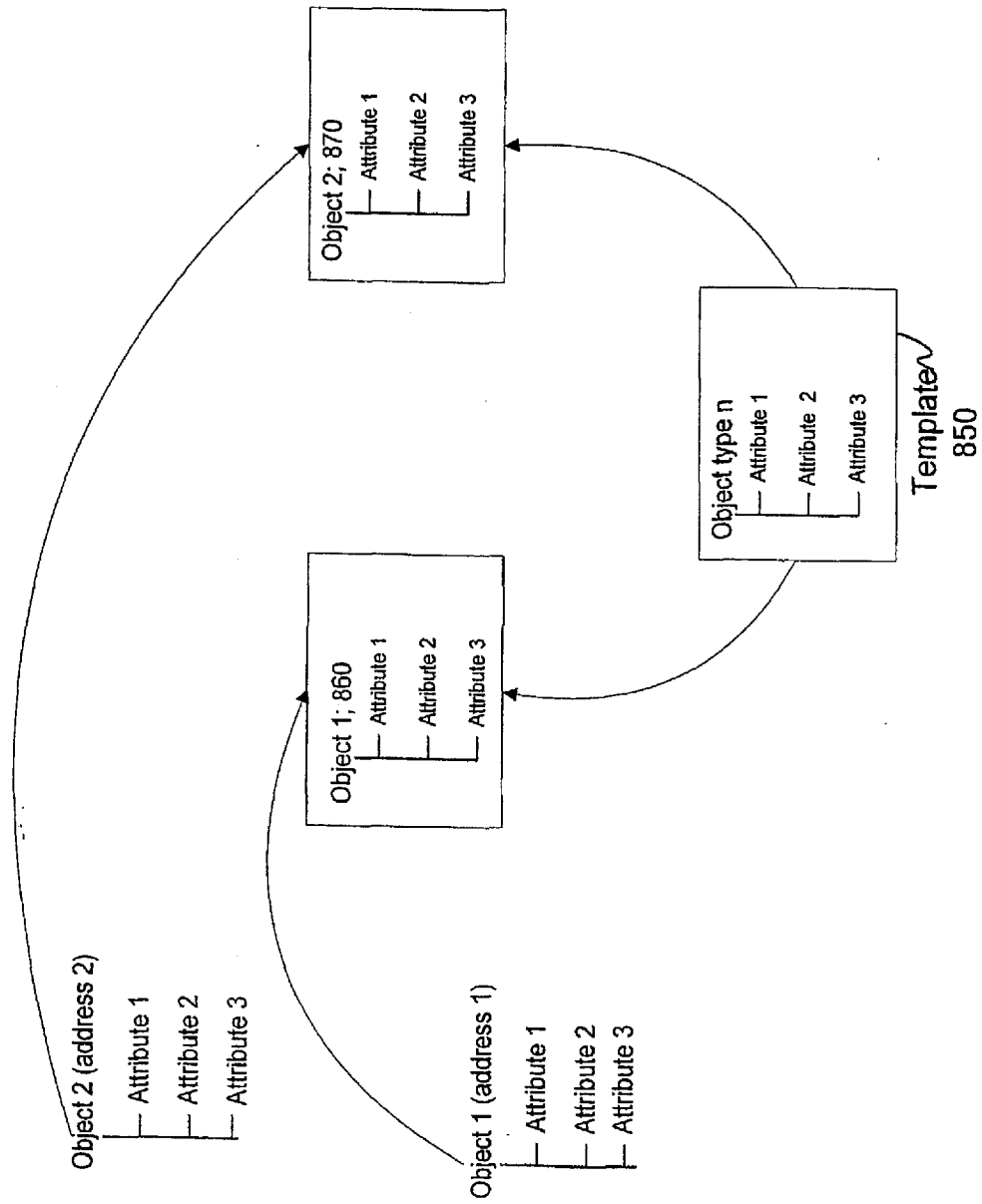


Figure 8C

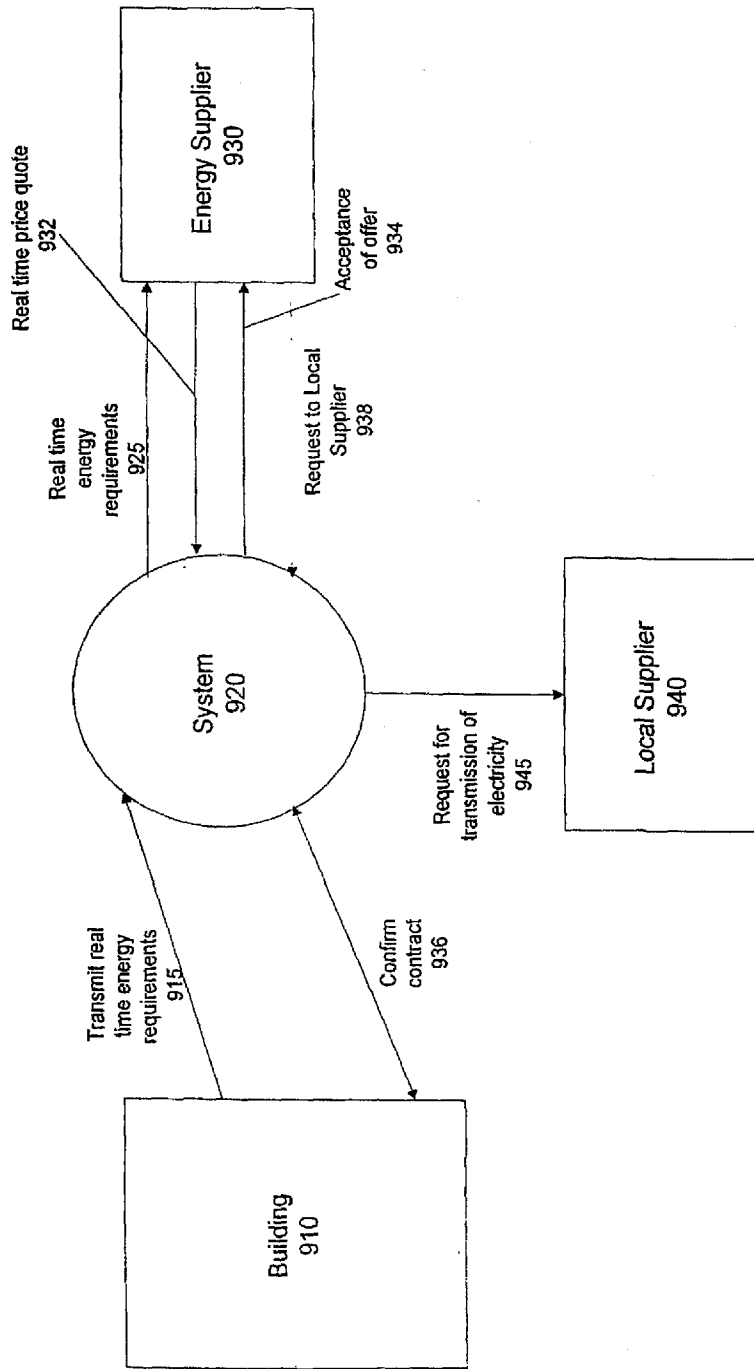


Figure 9

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
9 December 2004 (09.12.2004)

PCT

(10) International Publication Number  
WO 2004/107710 A1

(51) International Patent Classification<sup>7</sup>: H04L 29/06

(21) International Application Number:  
PCT/KR2004/001261

(22) International Filing Date: 28 May 2004 (28.05.2004)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:  
10-2003-0034962 30 May 2003 (30.05.2003) KR  
PCT/KR03/01345 7 July 2003 (07.07.2003) KR

(71) Applicant (for all designated States except US): LG ELECTRONICS, INC. [KR/KR]; 20, Yoido-Dong, Yongdungpo-Ku, Seoul 150-010 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): BAEK, Seung-Myun [KR/KR]; Lucky Apt. 12-403, Banlim-Dong,

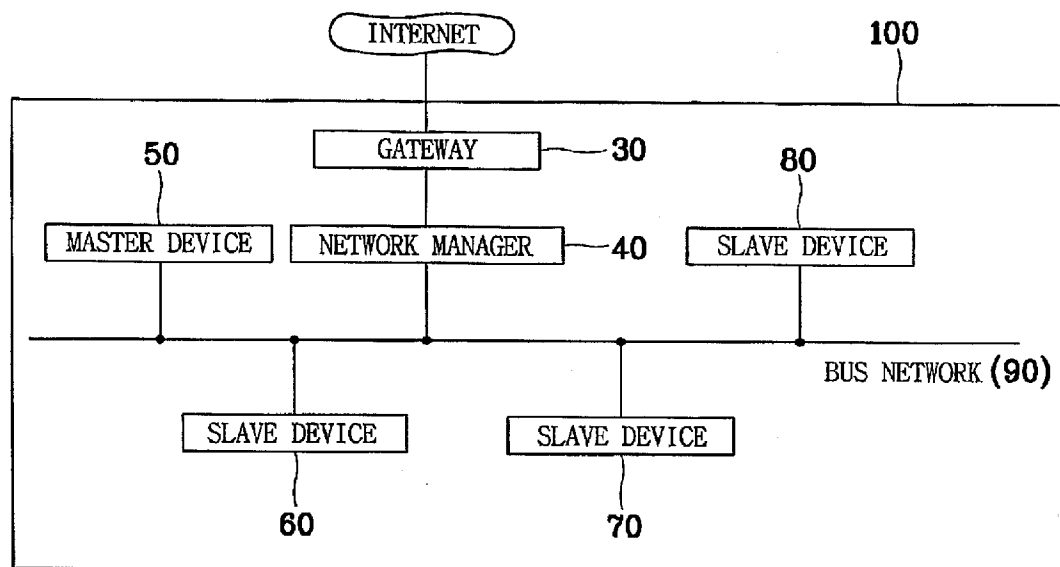
Changwon-Shi, Kyungsangnam-Do 641-764 (KR). LEE, Koon-Seok [KR/KR]; Sungwon Apt. 102-1406, 45-1 Sangnam-Dong, Changwon-Shi, Kyungsangnam-Do 641-778 (KR). CHOI, Hwan-Jong [KR/KR]; 909-13, Mandeuk 3-Dong, Buk-Ku, Busan 616-829 (KR). KIM, Yong-Tae [KR/KR]; Daedong Apt. 1006-1504, Mukea-Ri, Jangyou-Myun, Gimhae-Shi, Kyungsangnam-Do 621-833 (KR). KOO, Feel-Young [KR/KR]; Keukdong-Villa No. 407, 542 Minrak-Dong, Suyoung-Ku, Busan 613-829 (KR). KOO, Ja-In [KR/KR]; 336-28, Hadae-Dong, Jinju-Shi, Kyungsangnam-Do 660-997 (KR). KANG, Seong-Hwan [KR/KR]; 1128, Keumeum-Ri, Seolcheon-Myun, Namhae-Kun, Kyungsangnam-Do 668-891 (KR).

(74) Agent: LEE, Kwang-Yeon; Lee & Kim, 5th Floor, New-Seoul Bldg., 828-8 Yoksam 1-Dong, Kangnam-Ku, Seoul 135-935 (KR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,

[Continued on next page]

(54) Title: HOME NETWORK SYSTEM



(57) Abstract: The present invention discloses a home network system (100) which uses a message structure for efficient communication between a plurality of home appliances. The home network system (100) includes at least one slave device (60, 70, 80), and at least one master device (50) connected to the slave device (60, 70, 80) through a network (90), for transmitting a request message to the slave device (60, 70, 80), wherein the request message is transmitted from an upper layer of the master device (50) to a lower layer thereof and from a lower layer of the slave device (60, 70, 80) to an upper layer thereof, and has a command code implying an operation which will be executed by the slave device (60, 70, 80), and a related argument for executing the operation.

WO 2004/107710 A1



KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

## HOME NETWORK SYSTEM

### TECHNICAL FIELD

The present invention relates to a home network system, and more particularly to, a home network system which uses a message structure for efficient communication between a plurality of home appliances.

### BACKGROUND ART

Home automation for automatically controlling home appliances at home or remotely has almost reached a commercial use stage. At its early stage, the home automation separately controlled each home appliance by using a telephone or infrared rays, and did not connect the home appliances one another. However, there has been suggested a method for building a network of home appliances by using a communication means, and collectively managing the network by using a controller.

Fig. 1 is a structure view illustrating a general home network system. Referring to Fig. 1, a home network connects various digital home appliances so that a user can always enjoy convenient, safe and economic life services inside or outside the house.

As factors of the advent of the home network, refrigerators or washing machines called white home appliances have been gradually digitalized due to development of digital signal processing techniques, and new information home appliances have been made due to rapid development of home appliance operating system techniques and high speed multimedia communication techniques.

Here, an IT network is built to exchange data between a personal computer

and peripheral devices or provide internet services, and an AV network is built between home appliances using audio or video information. In addition, a living network is built to simply control home appliances, such as home automation or remote meter reading, and may be comprised of a refrigerator, washing machine, microwave oven, electric lamp, gas alarm, air conditioner and telephone.

The home network system includes a master device which is a home appliance for controlling an operation of the other home appliances or monitoring a status thereof, and a slave device which is a home appliance having a function of responding to the request of the master device and a function of notifying a status change according to properties of the home appliances or other factors. Here, the home appliances (or new devices) include home appliances for the living network service such as a washing machine and a refrigerator as well as home appliances for the IT network service and the AV network service.

In the conventional home network system, there are increasing demands for a message structure for precisely transmitting information between a plurality of home appliances (master devices and slave devices) connected to the home network system.

#### DISCLOSURE OF THE INVENTION

An object of the present invention is to provide a home network system which can efficiently transmit a control command, by transmitting a request message having a predetermined structure from a master device to a slave device by using layers between home appliances (master device and slave device).

Another object of the present invention is to provide a home network system which can efficiently transmit a response, control a network traffic and implement optimum performance of home appliances (master device and slave

device), by transmitting a response message having a predetermined structure from a slave device to a master device in response to a predetermined request message by using layers between the home appliances.

Yet another object of the present invention is to provide a home network  
5 system which can efficiently notify an event, by transmitting an event message having a predetermined structure from one home appliance to another home appliance by using layers between the home appliances.

In order to achieve the above-described objects of the invention, there is provided a home network system including: at least one slave device; and at least  
10 one master device connected to the slave device through a network, for transmitting a request message to the slave device, wherein the request message is transmitted from an upper layer of the master device to a lower layer thereof and from a lower layer of the slave device to an upper layer thereof, and has a command code implying an operation which will be executed by the slave device,  
15 and a related argument for executing the operation.

According to another aspect of the invention, a home network system includes: at least one master device; and a slave device connected to the master device through a network, for receiving a request message from the master device and transmitting a response message to the master device, wherein the response  
20 message is transmitted from an upper layer of the slave device to a lower layer thereof and from a lower layer of the master device to an upper layer thereof, and has a command code included in the request message for implying an operation which will be executed by the slave device, and a field for executing the request.

Preferably, when the request message has been normally executed, the  
25 field includes an ACK code.

Preferably, the response message further includes a field for notifying an



execution result of the request message.

Preferably, when the request message has not been normally executed, the field includes an NAK code.

Preferably, the command code includes an instantaneous command for  
5 allowing the slave device to receive the request message, directly execute the request message, and then transmit the response message.

Preferably, the command code includes a program command for allowing the slave device to receive the request message, transmit the response message to the master device, and then execute the request message.

10 Preferably, the related argument is an argument independent from the command code.

Preferably, the related argument is an argument dependent upon the command code.

According to another aspect of the invention, a home network system  
15 includes at least two devices, wherein, when a status of one device is changed, one device generates an event message and transmits the event message to the other device, and the event message is transmitted from an upper layer of one device to a lower layer thereof and from a lower layer of the other device to an upper layer thereof, and has a command code, an event code and a status value.

20 Preferably, the command code is '0x11'.

According to another aspect of the invention, a storage medium records a message structure in a home network system including at least one master device and slave device, wherein a request message from the master device to the slave device is transmitted from an upper layer of the master device to a lower layer  
25 thereof and from a lower layer of the slave device to an upper layer thereof, and has a command code implying an operation which will be executed by the slave

device, and a related argument for executing the operation.

According to another aspect of the invention, a storage medium records a message structure in a home network system including at least one master device and slave device, wherein a response message to a request message from the master device to the slave device is transmitted from an upper layer of the slave device to a lower layer thereof and from a lower layer of the master device to an upper layer thereof, and has a command code included in the request message for implying an operation which will be executed by the slave device, and a field for executing the request.

10 Preferably, when the request message has been normally executed, the field includes an ACK code.

Preferably, the message structure further includes a field for notifying an execution result of the request message.

15 Preferably, when the request message has not been normally executed, the field includes an NAK code.

Preferably, the command code includes an instantaneous command for allowing the slave device to receive the request message, directly execute the request message, and transmit the response message.

20 Preferably, the command code includes a program command for allowing the slave device to receive the request message, transmit the response message to the master device, and execute the request message.

Preferably, the related argument is an argument independent from the command code.

25 Preferably, the related argument is an argument dependent upon the command code.

According to another aspect of the invention, a storage medium records a

message structure in a home network system including at least two devices, wherein an event message generated due to status change of one device is transmitted from an upper layer of one device to a lower layer thereof and from a lower layer of the other device to an upper layer thereof, and has a command code,  
5 an event code and a status value.

Preferably, the command code is '0x11'.

### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a structure view illustrating a general home network system;  
10 Fig. 2 is a structure view illustrating a home network system in accordance with the present invention;  
Fig. 3A is a structure view illustrating a request message in accordance with the present invention;  
Fig. 3B is a structure view illustrating a first example of a response  
15 message in accordance with the present invention;  
Fig. 3C is a structure view illustrating a second example of the response message in accordance with the present invention; and  
Fig. 3D is a structure view illustrating an event message in accordance with the present invention.

20

### BEST MODE FOR CARRYING OUT THE INVENTION

A home network system in accordance with the present invention will now be described in detail with reference to the accompanying drawings.

Fig. 2 is a structure view illustrating the home network system in  
25 accordance with the present invention. Referring to Fig. 2, the home network system 100 includes at least one master device 50 and slave devices 60, 70 and

80 connected through a bus network 90. In addition, the home network system 100 further includes a gateway 30 for access to an external network (for example, internet), and a network manager 40 connected to the gateway 30, for providing an internet service and performing environment setting and resetting functions of home appliances of the home network system 100.

Here, the master device 50 performs the same functions as the general master device, and the network manager 40 performs similar functions to the master device 50 except for the internet service. For conveniences' shake, there are presumed that the network manager 40 performs functions such as a bridge for the internet service, and that only one master device 50 exists in the home network system 100.

The bus network 90 can be a wire medium such as a specially-installed line, or a previously-installed power line or telephone line, or a wireless transmission medium. However, still referring to Fig. 2, the home network system 100 composes a closed network for connecting home appliances of one house through a wire or wireless transmission medium. At this time, the closed network includes a physically-connected but logically-divided network. In addition, the bus network 90 of the home network system 100 pursues to a different protocol from the external network. It is thus impossible to access the home appliances merely through the external network.

Fig. 3A is a structure view illustrating a request message in accordance with the present invention. As shown in Fig. 3A, the request message is transmitted from the master device 50 to the slave devices 60, 70 and 80, and has a command code for allowing the slave devices 60, 70 and 80 to execute a predetermined operation, and a related argument for executing the operation.

The related argument included in the request message is a data necessary

to execute a control command according to the command code. The related argument is classified into an independent argument independent from the command code, and a dependent argument dependent upon the command code. For example, the independent argument is a voice data or an image data. When the command code implies transmission of a predetermined data, the independent argument is included in the request message. The independent argument itself has inherent characteristics, and such characteristics are not changed by the command code. On the other hand, for example, the dependent argument is a predetermined constant. When the command code implies temperature setting of a refrigerator, the dependent argument is regarded as a set temperature value, and when the command code implies operation start of a microwave oven, the dependent argument is regarded as an operation time value. That is, the dependent argument does not have inherent characteristics, but characteristics thereof are determined by the command code.

The related argument can be used as the independent argument or the dependent argument according to intentions of the designer designing the home network system 100, or properties of each home appliance.

The request message is transmitted from an upper layer of the master device 50 to a lower layer thereof under a predetermined control protocol of the home network system 100, and transmitted from lower layers of the slave devices 60, 70 and 80 to upper layers thereof through the bus network 90. Accordingly, control means (not shown) of the slave devices 60, 70 and 80 receive the request message and perform a predetermined operation.

Fig. 3B is a structure view illustrating a first example of a response message in accordance with the present invention. As depicted in Fig. 3B, the response message is a response to the request message of Fig. 3A, and has a

command code included in the request message, an ACK (acknowledgement) and a return value.

The command code is a previously-inputted command code from the master device 50, which has been processed or will be processed in the slave devices 60, 70 and 80, the ACK implies that the request message has been normally executed, and the return value implies an execution result of the request message.

Fig. 3C is a structure view illustrating a second example of the response message in accordance with the present invention. As illustrated in Fig. 3C, the response message is a response to the request message of Fig. 3A, and has a command code included in the request message, an NAK (no acknowledgement) and an NAK code (or error code).

The command code is a previously-inputted command code from the master device 50, which has been processed or will be processed in the slave devices 60, 70 and 80, the NAK implies that the request message has not been normally executed, and the NAK code implies a non-execution reason. Here, the NAK code does not include transmission errors resulting from communication failure by message transmission.

Such response messages are transmitted from the upper layers of the slave devices 60, 70 and 80 to the lower layers thereof under a predetermined control protocol of the home network system 100, and transmitted from the lower layer of the master device 50 to the upper layer thereof through the bus network 90. Accordingly, a control means (not shown) of the master device 50 receives and processes the response messages.

The command codes of Figs. 3A to 3C are divided into an instantaneous command code and a program command code. The instantaneous command code

can be executed by the slave devices 60, 70 and 80 directly after reception. When the slave devices 60, 70 and 80 receive the request message containing the instantaneous command code, the slave devices 60, 70 and 80 must transmit the response message after executing the command. The program command code  
5 requires a sequence for execution. When the slave devices 60, 70 and 80 receive the request message containing the program command code, the slave devices 60, 70 and 80 must execute the command after transmitting the response message.

Here, characteristics of the instantaneous or program command code are determined by estimating a traffic of the whole network including the bus network  
10 90 not to generate an excessive traffic, or determined in consideration of properties of each home appliance to process data with optimum performance.

Fig. 3D is a structure view illustrating an event message in accordance with the present invention. Referring to Fig. 3D, the event message has a command code for notifying the event message, an event code and a status value.

15 The event message is generated because of status changes of the home appliances (master device 50 and slave devices 60, 70 and 80). According to generation reasons, event messages are classified into a user event generated due to a command directly from the user, a periodical event automatically generated at an interval of a predetermined time, a status event generated due to  
20 spontaneous status change during monitoring of the status of the home appliance, an error event generated due to an error relating to the operation of the home appliance, and an external event generated due to a request from the outside of the home network system 100.

In the case that the user (or master device 50) monitors the status of the  
25 home appliance, it is inefficient for the user to request the status value whenever he/she intends to know the status of the home appliance. That is, when the status

value of the home appliance is changed, the home appliance can efficiently notify the status change by using the event message. In addition, a process for directly notifying the status change when the event is generated is necessary in order to directly notify a defect or error of the home appliance.

5           The event message uses the command code of 0x11, the event code contains a product code implying the home appliance relating to the event and an event type, and the return value contains information of a value changed due to the event.

10           The message structures can be stored in a predetermined storage means of the master device and the slave device of the home network system, or transmitted through the bus network.

15           Although the preferred embodiments of the present invention have been described, it is understood that the present invention should not be limited to these preferred embodiments but various changes and modifications can be made by one skilled in the art within the spirit and scope of the present invention as hereinafter claimed.



What is claimed is:

1. A home network system, comprising:

at least one slave device; and

5 at least one master device connected to the slave device through a network,  
for transmitting a request message to the slave device,

wherein the request message is transmitted from an upper layer of the  
master device to a lower layer thereof and from a lower layer of the slave device to  
an upper layer thereof, and has a command code implying an operation which will  
10 be executed by the slave device, and a related argument for executing the  
operation.

2. A home network system, comprising:

at least one master device; and

15 a slave device connected to the master device through a network, for  
receiving a request message from the master device and transmitting a response  
message to the master device,

wherein the response message is transmitted from an upper layer of the  
slave device to a lower layer thereof and from a lower layer of the master device to  
20 an upper layer thereof, and has a command code included in the request message  
for implying an operation which will be executed by the slave device, and a field for  
executing the request.

3. The system of claim 2, wherein, when the request message has been

25 normally executed, the field comprises an ACK code.

4. The system of claim 3, wherein the response message further comprises a field for notifying an execution result of the request message.

5. The system of claim 2, wherein, when the request message has not been normally executed, the field comprises an NAK code.

6. The system of claim 1 or 2, wherein the command code comprises an instantaneous command for allowing the slave device to receive the request message, directly execute the request message, and then transmit the response message.

7. The system of claim 1 or 2, wherein the command code comprises a program command for allowing the slave device to receive the request message, transmit the response message to the master device, and then execute the request message.

8. The system of claim 1, wherein the related argument is an argument independent from the command code.

9. The system of claim 1, wherein the related argument is an argument dependent upon the command code.

10. A home network system, comprising at least two devices, wherein, when a status of one device is changed, one device generates an event message and transmits the event message to the other device, and the event message is transmitted from an upper layer of one device to a lower layer

thereof and from a lower layer of the other device to an upper layer thereof, and has a command code, an event code and a status value.

11. The system of claim 10, wherein the command code is '0x11'.

5

12. A storage medium for recording a message structure in a home network system including at least one master device and slave device,

wherein a request message from the master device to the slave device is transmitted from an upper layer of the master device to a lower layer thereof and from a lower layer of the slave device to an upper layer thereof, and has a command code implying an operation which will be executed by the slave device, and a related argument for executing the operation.

10

13. A storage medium for recording a message structure in a home network system including at least one master device and slave device,

15

wherein a response message to a request message from the master device to the slave device is transmitted from an upper layer of the slave device to a lower layer thereof and from a lower layer of the master device to an upper layer thereof, and has a command code included in the request message for implying an operation which will be executed by the slave device, and a field for executing the request.

20

14. The medium of claim 13, wherein, when the request message has been normally executed, the field comprises an ACK code.

25

15. The medium of claim 14, wherein the message structure further

comprises a field for notifying an execution result of the request message.

16. The medium of claim 13, wherein, when the request message has not been normally executed, the field comprises an NAK code.

5

17. The medium of claim 12 or 13, wherein the command code comprises an instantaneous command for allowing the slave device to receive the request message, directly execute the request message, and transmit the response message.

10

18. The medium of claim 12 or 13, wherein the command code comprises a program command for allowing the slave device to receive the request message, transmit the response message to the master device, and execute the request message.

15

19. The medium of claim 12, wherein the related argument is an argument independent from the command code.

20. The medium of claim 12, wherein the related argument is an argument dependent upon the command code.

20

21. A storage medium for recording a message structure in a home network system including at least two devices,

wherein an event message generated due to status change of one device is transmitted from an upper layer of one device to a lower layer thereof and from a lower layer of the other device to an upper layer thereof, and has a command code,

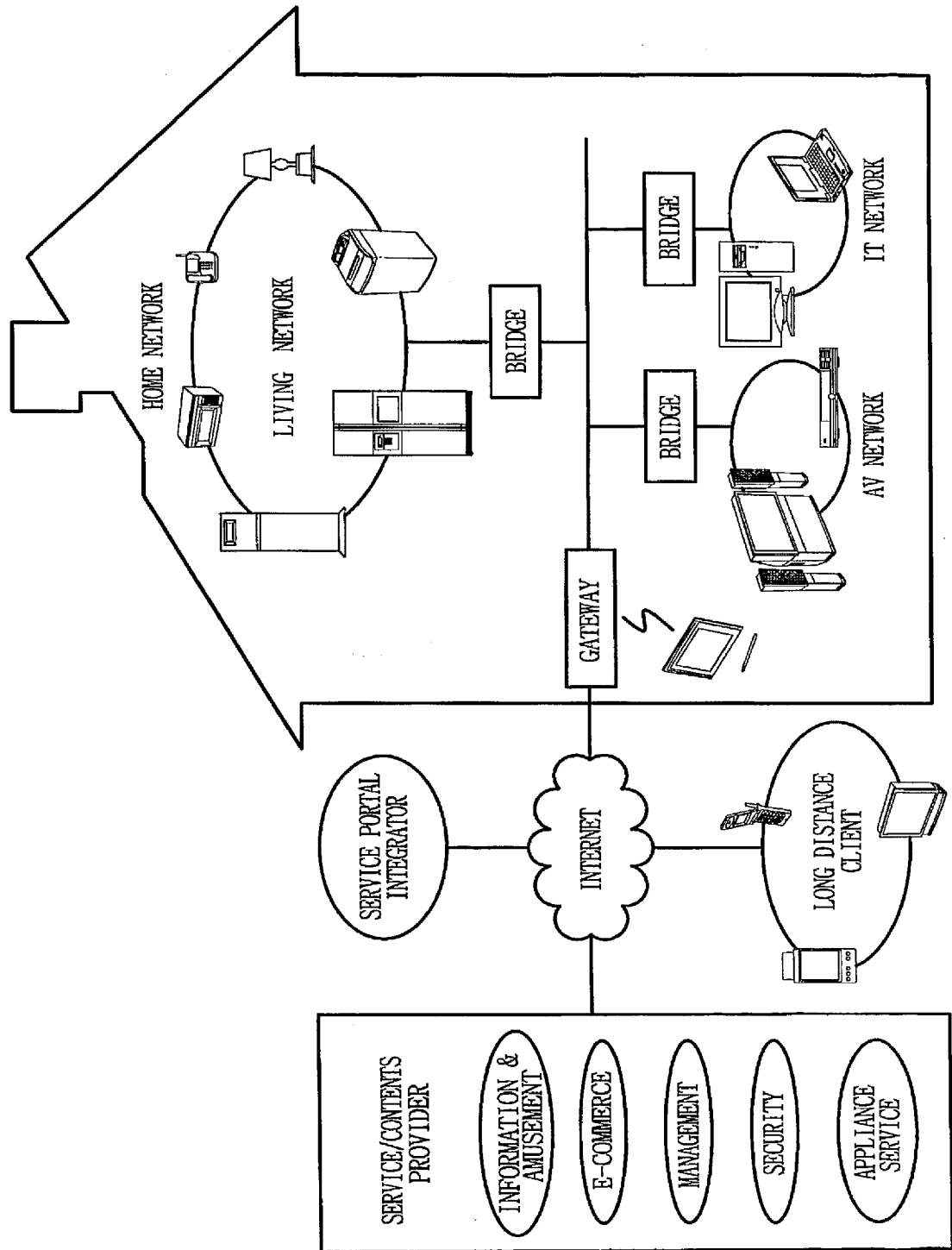
25

an event code and a status value.

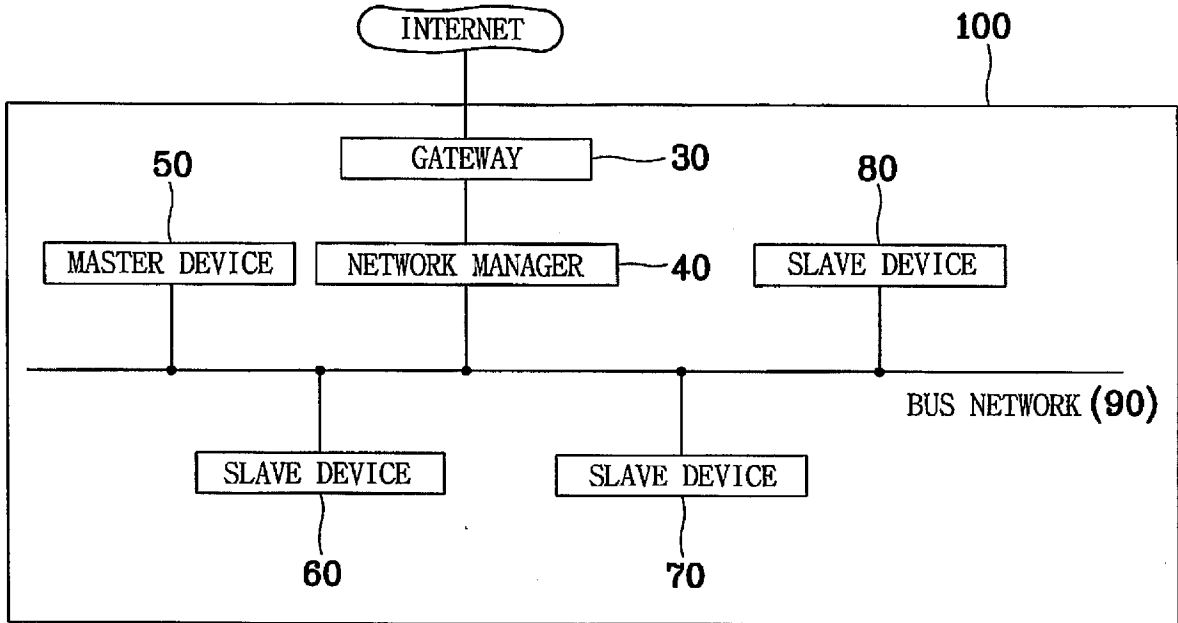
22. The medium of claim 21, wherein the command code is '0x11'.

1/3

FIG. 1



2/3  
FIG. 2



3/3  
FIG.3A

COMMAND CODE	INPUT ARGUMENT
--------------	----------------

FIG.3B

COMMAND CODE	ACK	RETURN VALUE
--------------	-----	--------------

FIG.3C

COMMAND CODE	NAK	NAK-CODE
--------------	-----	----------

FIG.3D

COMMAND CODE	EVENT CODE	STATUS VALUE
--------------	------------	--------------



## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/KR 2004/001261

A. CLASSIFICATION OF SUBJECT MATTER IPC <sup>7</sup> : H04L 29/06 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) IPC <sup>7</sup> : H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPI, PAJ, EPODOC, Elsevier, IEE, I3E, IEEEExplore		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Koon-Seok Lee, Hoan-Jong Choi, Chang-Ho Kim, Seung-Myun Baek, 'A new control protocol for home appliances-LnCP.' In: International Symposium on Industrial Electronics, 2001. Proceedings. ISIE 2001. 12-16 June 2001 pages: 286 - 291 volume 1	1-22
X	US 2003/0088703 A1 (KIM) 8 May 2003 (08.05.2003) <i>figures; abstract; sections 4, 9-13</i>	1, 8-13, 19-22
A		2-7, 14-18
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>		
Date of the actual completion of the international search 28 September 2004 (28.09.2004)		Date of mailing of the international search report 1 October 2004 (01.10.2004)
Name and mailing address of the ISA/ AT <b>Austrian Patent Office</b> Dresdner Straße 87, A-1200 Vienna Facsimile No. +43 / 1 / 534 24 / 535		Authorized officer <b>MESA PASCASIO J.</b> Telephone No. +43 / 1 / 534 24 / 327

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
PCT/KR 2004/001261

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
	A		none	
US	A	20030088 703	none	

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
8 January 2004 (08.01.2004)

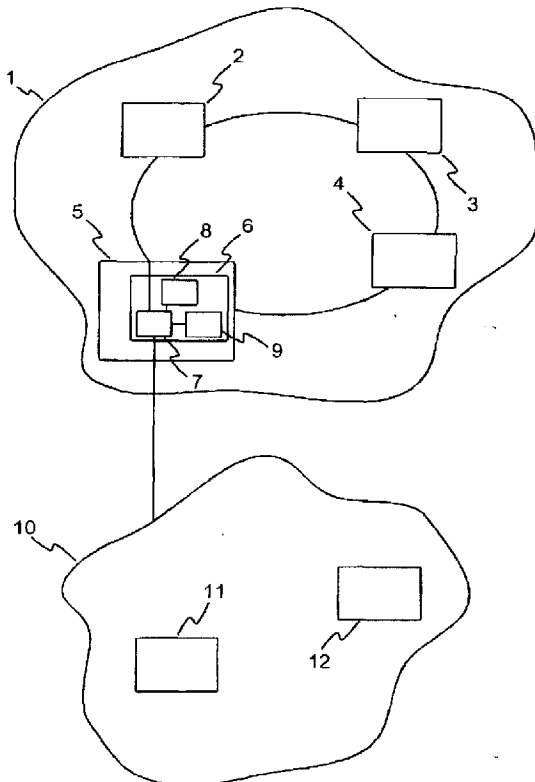
PCT

(10) International Publication Number  
WO 2004/004222 A1

- (51) International Patent Classification<sup>7</sup>: **H04L 12/28**
- (21) International Application Number: PCT/EP2003/006233
- (22) International Filing Date: 13 June 2003 (13.06.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 102 28 605.1 26 June 2002 (26.06.2002) DE
- (71) Applicant (for all designated States except US): **THOMSON LICENSING S.A.** [FR/FR]; 46 Quai A. le Gallo, F-92100 Boulogne-Billancourt (FR).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): **KÖHLER, Ralf** [DE/DE]; Froebeniusweg 7, 30455 Hannover (DE).
- (74) Agent: **THIES, Stephan**; European Patent Operations, Karl-Wiechert-Allee 74, 30625 Hannover (DE).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: MODULE FOR INTEGRATION IN A HOME NETWORK



(57) Abstract: In a home network (1), a wide variety of devices (2, 3, 4, 5) are interlinked so that they can exchange data among one another. Such home networks (1) also often have a connection to an external network (10). If an individual device of the home network wishes to obtain data from the external network (10), it requires comprehensive hardware and software for searching for and processing the data. The hardware and software must be able to read the different data formats and formats for describing the data contents which are used by providers (11, 12) in the external network (10). According to the invention, it is provided that a module (6) of the home network (1) performs this search task for the other devices (2, 3, 4) and establishes connection with the external network (10) via a connecting device (5). After finding data sought, it makes the data available to the inquiring device (2, 3, 4) in a format that can be read by the latter.

WO 2004/004222 A1



**Published:**

— with international search report

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Module for integration in a home network**

The invention relates to a module for integration in a home network with individual devices which are  
5 connected to one another and communicate among one another via one or more protocols, the home network having at least one connecting device which allows communication with an external network.

10 A home network is understood to be the amalgamation of a plurality of functionally quite different devices e.g. in a residence or a small office. The devices are e.g. communications devices, such as telephone and fax, entertainment devices, such as television, DVD player,  
15 etc., and work devices, such as computer and the like. In some instances, domestic appliances and household equipment, such as refrigerator and heating, are also connected to such a network. The devices are set up to communicate with one another by means of defined  
20 protocols (e.g. HAVi, Home Audio/Video Interoperability, or UPnP, Universal Plug and Play) and to exchange digital or alternatively analog data among one another. This opens up the possibility of data which are present in a specific device of the home  
25 network also being made available to the other devices that are integrated in the home network. Thus, it is conceivable, by way of example, for music which is present in the form of a file in a computer in the  
30 living room. At the same time, it is possible, under certain circumstances, for the stereo system to be controlled by means of a menu displayed on a television that is integrated in the home network.

35 In addition to the possibility of the internal exchange of data, however, some devices furthermore also have connections to external networks: the telephone is connected to a telephone network (analog, ISDN) and the

- 2 -

television is connected to a cable network which serves to transmit video and audio signals, but is also increasingly used for the transmission of data for a computer. The computer is connected by a modem to the  
5 Internet with its diverse services (World Wide Web, Usenet etc.) or to comparable networks. In this case, each device independently produces a connection to the associated network and is then able to localize and to retrieve the required data there and subsequently to  
10 process them. However, this presupposes that, in the residence, in the house or in the office, the various external networks are routed through to the respective device, which is associated with a considerable installation outlay.

15 Therefore, it has already been proposed to centralize the network accesses. Thus, US-A 5,886,732 shows the possibility of combining a plurality of network accesses (NIU: Network Interface Units) of different  
20 providers in a central station which interacts with a plurality of home networks via a switched node (switch hub), such a network comprising e.g. a set-top electronic unit STE without the otherwise customary network access means. A plurality of devices (CVCR,  
25 DCAM, DTV1) that process video and audio signals are connected to the STE via a data bus. Accordingly, the set-top electronic unit STE no longer performs the function of realizing the network access, but still has the task of conditioning the received data for the  
30 connected devices.

The system in accordance with WO 01/56233 is also based on this principle: a central telephone access system which can utilize the various services offered, such as  
35 analog, ISDN, DSL, serves as access to the telephone network and to the Internet for connected computers and other devices: here, too, the central station only has the task of producing the network access.

- 3 -

The situation is similar in accordance with  
EP 1 017 206 A2: the individual devices of the home  
network are connected to the Internet via a central  
5 network access (home gateway) located outside the home  
network. Each device thus sets up its access to the  
Internet independently of the other devices of the  
network. The system makes it possible to access the  
various devices in the home network from the Internet  
10 via a single address.

In the case of the previously known systems, although  
the individual devices no longer have to establish the  
network access, they continue to be responsible for  
15 finding or filtering out the desired data in the  
external network and converting them into formats  
suitable for reproduction. This task is associated with  
a considerable outlay, however, since video and audio  
data, in particular, are likely to be present in  
20 different formats which, under certain circumstances,  
cannot be processed by the devices, and even the  
formats of data which describe the respective data  
contents (metadata) vary. Moreover, the transmission  
protocols (e.g. IP (Internet Protocol), UDP (User  
25 Datagram Protocol) or RTP (Real-Time Transport  
Protocol)) used in the external network are also not  
necessarily compatible with the transmission protocols  
of the home network. Although UPnP, for example, is  
based on the Internet Protocol IP, that still does not  
30 mean, however, that a terminal communicating by means  
of UPnP can process specific audio/video data by means  
of IP. Therefore, a search unit must know all or at  
least the predominant formats and protocols in order to  
be able to receive and process the data that are stored  
35 in the external network with a corresponding format.  
Furthermore, a search unit must be able to establish  
connection with various providers of data in order to  
be able to find the stored data. The abovementioned

- 4 -

tasks of a search unit require a high outlay on software and associated hardware, which causes high costs.

5 Consequently, the invention is based on the problem of reducing the outlay on software and hardware required for the search units of devices in a home network, so that the connected devices are simpler in their construction and hence more cost-effective.

10

In order to solve the problem, the invention provides a module for integration in a home network having the further features that the module has one or more search units in particular for finding data available at  
15 providers in the external network and is able to receive the data and/or the metadata describing their content and can make them available to the devices of the home network. In this way, the search function is performed by a central module so that the connected  
20 devices no longer have to provide this function themselves. As a result, said devices can be produced more cost-effectively. The module may be realized both in the form of a computer program which uses available electronics in the home network, for example in the  
25 computer or in the connecting device, and as an autonomous device with electronics and programming. The search unit must on the one hand know the addresses of providers via which it can obtain data, and on the other hand it must be able to communicate with said  
30 providers and evaluate the received data. The search unit therefore has to know what details in what form it must give the various providers in order to acquire the desired data. In this case, providers are not only to be understood as commercial providers of data which  
35 make available "video/music on demand" or live TV or radio programs, for example, the operators of private pages on the Internet or the known search engines on the Internet also constitute providers. In principle, a



- 5 -

provider is anyone who makes data available to others free of charge or for payment via a network.

5 The term data is to be understood both as files and as data streams which in the actual sense do not constitute files. By way of example, live TV programs are received by an IP-TV server directly from a satellite and converted in real time into an IP data stream to which devices in the home network can be  
10 connected. In this case, no audio/video files are stored, rather only data are forwarded to the terminal.

The module can be improved further by having a format converter, which converts the data of the external  
15 network into a format which corresponds to one of the formats which are defined for the exchange of data in the home network and are readable for the devices in the home network. In this way, a possibly required format conversion of the data requested from the  
20 external network is also shifted from the individual devices of the home network to the module, so that the individual devices of the home network are simplified further.

25 In an advantageous manner, the format converter is able, moreover, to convert data in a format which corresponds to one of the formats which are defined for the exchange of data in the home network and are readable for the devices in the home network into a  
30 format used in the external network. In this way, data which are requested from the home network by the external network can also be made available without any further outlay.

35 According to the invention, the search unit and/or the format converter can be updated. This has the advantage, inter alia, that, in the event of newly emerging formats or in the event of changes to the

- 6 -

addresses or communication methods of providers in the external network, only the module or the format converter and the search unit have to be set to these new formats or the new addresses and methods, while the other devices in the network can still have recourse to a form that is readable for them. Thus, these devices do not need to be exchanged or updated. The updating may be effected, for example, by means of information from the external network made available by the providers. However, it is equally conceivable for a service provider to collate this information and make it available as a chargeable service, whether by direct dispatch via the network or by the provision of a storage medium holding the information.

In an advantageous manner, the module communicates with the other devices of the home network by means of one of the protocols defined for the home network. In this way, the programming of the individual devices of the home network is very simple: the devices only have to communicate with the module in the formats defined for the home network. For the inquiring device, the situation is as if the connecting device had the data inquired about in an appropriate format for the inquiring device. The fact that the connecting device first of all itself obtains the respective data from the external network and, if appropriate, subjects them to a format conversion remains hidden from the inquiring device. The module could thus be manifested as a standard device in the home network, for example as a central media store.

According to the invention, the module converts control data from a protocol defined for the home network into a protocol used by the external network or by a provider of data. This is of interest in particular for the case where the transmitted data are data streams, as occur for example with "video/audio on demand" or

- 7 -

live TV programs. The conversion of the control data allows the devices in the home network to control the source of the data without knowing the corresponding protocols. Control data may be, for example, commands  
5 such as START, STOP, PAUSE, FAST FORWARD etc.

In order to be able to adapt the data transmission into the home network, if appropriate, to the transmission speed of the external network, or in order to provide a  
10 buffer for a format conversion, the module has a memory, which stores the received data and, if appropriate, the data converted into the format defined for the home network.

15 The invention is particularly beneficial if the external network is the Internet. It is precisely in this network that numerous data are available which, however, first have to be found in order to be able to be used by the respective end user device. On the  
20 Internet, it has also been possible to establish different protocols for data transmission and formats in which data are stored or made available in files or data streams, so that the search units must be able to understand and interpret a plurality of protocols and  
25 formats. In this case, the searching through the external network is performed by programs referred to as agents. The content descriptions of the providers in the external network are gradually evaluated and compared with the inquiry from the home network. If a  
30 match is found, the corresponding data are downloaded via the connecting device.

The data from the external network are typically text, audio and/or video data. Since, as a general rule, home  
35 networks are primarily used for exchanging multimedia data, these types of data are those which are requested the most often. However, the data may, of course, also involve other types of data for the connected devices,

- 8 -

for example updates for the software on a computer, program updates for a washing machine, weather data or forecasts for a heating system, present energy costs for storage heating, and much more.

5

According to the invention, the module communicates with the devices of the home network via a data bus. Via the data bus, information about the type and setting of the respective device is exchanged, so that the various devices can identify themselves and adapt themselves to one another, that is to say communicate their respective type and settings, and, moreover, data are exchanged and forwarded, which data are then used for reproduction and/or recording in the respective device. In this case, the communication between the devices can be effected both in a wire-based manner and in a wire-free manner (e.g. Bluetooth, etc.).

In an advantageous manner, the module is integrated in the connecting device. In this way, a single device performs all the tasks necessary for communication with the external network, that is to say both the connection to the external network and the search for data and the conversion of the data into suitable formats. It goes without saying, however, that the module may also be an autonomous device which can be integrated without difficulty into an already existing home network.

In accordance with a further improvement the module is able to receive and process inquiries from the external network and send data from the home network into the external network. This makes it possible, by way of example, for a user, even from outside the home network, via the external network, to establish contact with the devices in the home network and to retrieve the data which can be made available by them, without having to rely on a special protocol for this purpose.

- 9 -

Furthermore, in this way, one's own data can also be made available to other persons. For this purpose, it is advantageous to provide a method for the monitoring and control of the access rights and for  
5 identification.

It goes without saying that combinations of advantageous features likewise lie within the scope of validity of the invention.  
10

In order to provide a better understanding, the invention will be explained in more detail below using an exemplary embodiment. For this purpose:

15 figure 1 shows a diagrammatic illustration of a module according to the invention in a home network which communicates with an external network via a connecting device.

20 A home network is designated by 1. A plurality of devices 2, 3, 4, 5 are connected to one another in this local network. Said devices are typically one or a plurality of computers, and also reproduction devices for sound and picture information, such as e.g. video  
25 devices, DVD or CD players. The devices communicate among one another in accordance with specific protocols, which makes it possible for one device to be controlled by another or for the data available in one device to be made available to other devices as well.

30 Moreover, the devices inform one another of their settings, so that an adaptation that normally has to be performed manually is effected automatically. Various protocols, such as HAVi or UPnP, geared specifically to such local amalgamations of devices have become  
35 established for this.

The communication with an external network, e.g. the Internet, which is marked by the reference symbol 10,

- 10 -

poses certain problems, however, since dedicated protocols, e.g. TCP/IP, are defined for this, which are generally not understood except by computers. In the external network 10, however, providers 11, 12 hold  
5 data which could actually be reproduced and/or recorded by the devices 2, 3, 4 of the home network 1. Said data involves e.g. pieces of music or else cinema films or texts. For access to the corresponding data, the home network 1 has a connecting device 5, which produces the  
10 connection to the external network 10, and also a module 6, in which a search unit 7 is integrated. The search unit 7 establishes contact with the providers 11, 12 and serves for finding the desired data in the external network 10.

15

The module 6 controls the data exchange protocols of the external network 10 and is able to understand and evaluate the formats used by the various providers 11, 12 for describing the content of data. For this  
20 purpose, said module contains, under certain circumstances, a plurality of submodules (not illustrated) which are set to the most important formats for describing data contents. For all the other devices 2, 3, 4 of the home network 1, insofar as they  
25 wish to access such data, the module 6 performs the task of finding corresponding data in the external network 10.

Insofar as the devices 2, 3, 4 can process the data  
30 directly, they are transferred directly. However, the module 6 also contains a format converter 8 which possibly performs a format conversion. The module 6 communicates with the devices 2, 3, 4 of the home network 1 in accordance with one of the protocols  
35 defined for the home network. It accepts e.g. the inquiries of the other devices 2, 3, 4 for specific contents and issues a corresponding search job to the search unit 7. Consequently, to the inquiring devices

- 11 -

2, 3, 4, the module 6 appears as a carrier of the  
desired data, as if it were a central media server, for  
example, on which the desired data are stored. In order  
to adapt the module 6 to the transmission speed of the  
5 external network 10 a memory 9 is provided for the  
module 6, the data from the external network 10 being  
stored in said memory.

- 12 -

**Patent Claims**

1. A module (6) for integration in a home network (1) with individual devices which are connected to one another and communicate among one another via one or more protocols defined for the home network (1), the home network (1) having at least one connecting device (5) which allows communication with an external network (10), **wherein** the module (6) has one or more search units (7) in particular for finding data available at providers (11, 12) in the external network (10) and is able to receive the data and/or the metadata describing their content and can make them available to the devices (2, 3, 4) of the home network (1).

15

2. The module (6) as claimed in claim 1, **wherein** it has a format converter (8), which converts the data of the external network (10) into a format which corresponds to one of the formats which are defined for the exchange of data in the home network (1) and are readable for the devices (2, 3, 4) in the home network (1).

20

3. The module (6) as claimed in claim 2, **wherein** the format converter (8) converts data in a format which corresponds to one of the formats which are defined for the exchange of data in the home network (1) and are readable for the devices (2, 3, 4) in the home network (1) into a format used in the external network (10).

30

4. The module (6) as claimed in one of claims 1-3, **wherein** the search unit (7) and/or the format converter (8) can be updated.

35

5. The module (6) as claimed in one of the preceding claims, **wherein** the module (6) communicates with the other devices (2, 3, 4) of the home network (1) by



- 13 -

means of one of the protocols defined for the home network (1).

6. The module (6) as claimed in one of the preceding  
5 claims, **wherein** it converts control data from a protocol defined for the home network (1) into a protocol used by the external network (10) or by a provider (11, 12) of data.

10 7. The module (6) as claimed in one of the preceding claims, **wherein** it has a memory (9), which stores the received data and/or the data converted into the format defined for the home network (1).

15 8. The module (6) as claimed in one of the preceding claims, **wherein** the external network (10) is the Internet.

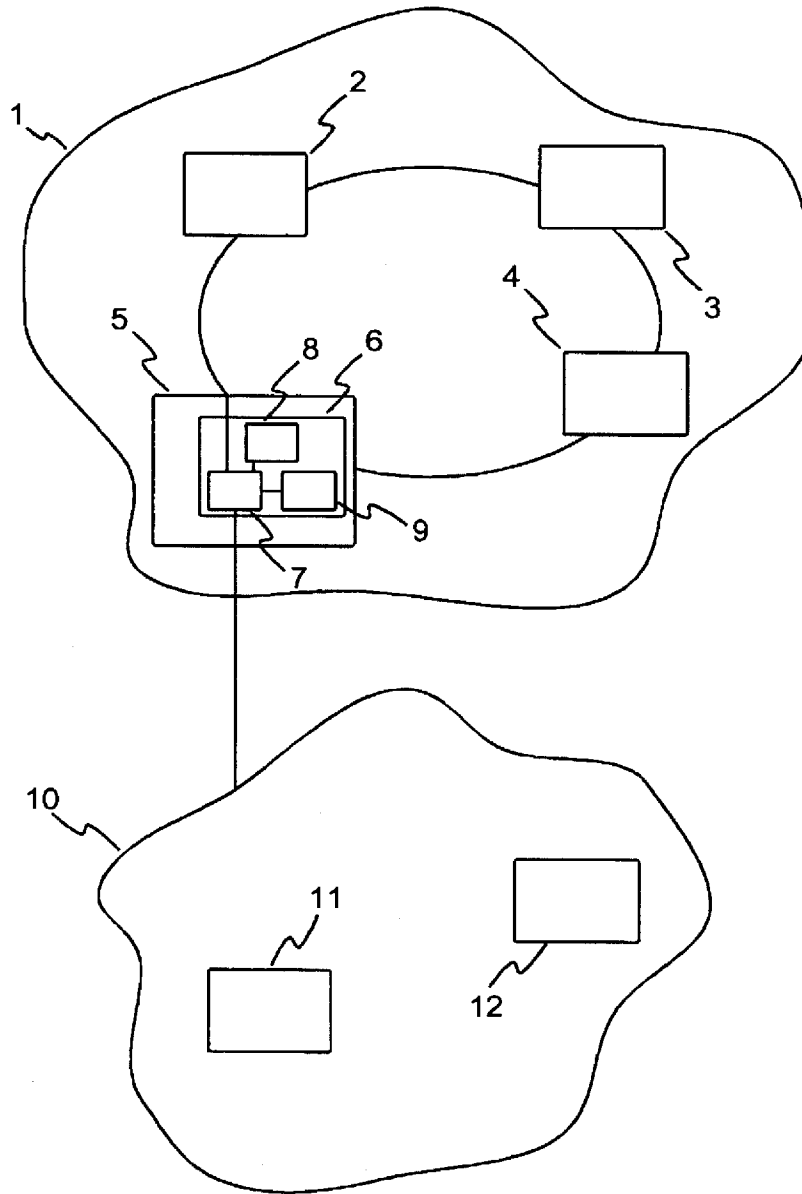
20 9. The module (6) as claimed in one of the preceding claims, **wherein** the data from the external network (10) are text, audio and/or video data.

25 10. The module (6) as claimed in one of the preceding claims, **wherein** it communicates with the devices (2, 3, 4) of the home network (1) via a data bus.

30 11. The module (6) as claimed in one of the preceding claims, **wherein** it is integrated into the connecting device (5).

35 12. The module (6) as claimed in one of the preceding claims, **wherein** it is able to receive and process inquiries from the external network (10) and send data from the home network (1) into the external network (10).

Fig. 1



**INTERNATIONAL SEARCH REPORT**

International Application No  
PCT/EP 03/06233

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**  
Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 86948 A (KONINKL PHILIPS ELECTRONICS NV) 15 November 2001 (2001-11-15) page 3, line 26 -page 3, line 33; figure 1 page 6, line 28 -page 6, line 34 figure 1	1-12
X	WO 01 86914 A (FISCHER MATTHEW J ;BROADCOM CORP (US); LUCAS BOB (US); RABENKO THE) 15 November 2001 (2001-11-15) page 1, line 16 -page 4, line 20 page 29, line 18 -page 30, line 29 figures 1A,2,5H	1-12

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*&\* document member of the same patent family

Date of the actual completion of the international search  
  
25 September 2003

Date of mailing of the international search report  
  
06/10/2003

Name and mailing address of the ISA  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer  
  
Oteo Mayayo, C

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 03/06233

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>EP 1 117 214 A (TERAYON COMM SYSTEMS INC)                      18 July 2001 (2001-07-18)                      page 4, left-hand column, line 50 -page 5,                      left-hand column, line 52                      page 5, right-hand column, line 4 -page 5,                      right-hand column, line 26                      page 6, left-hand column, line 29 -page 8,                      right-hand column, line 43                      figures 3,7,8</p> <p style="text-align: center;">---</p>	1-12
Y	<p>CORCORAN P M: "MAPPING HOME-NETWORK                      APPLIANCES TO TCP/IP SOCKETS USING A                      THREE-TIERED HOME GATEWAY ARCHITECTURE"                      IEEE TRANSACTIONS ON CONSUMER ELECTRONICS,                      IEEE INC. NEW YORK, US,                      vol. 44, no. 3, August 1998 (1998-08),                      pages 729-736, XP000851577                      ISSN: 0098-3063                      the whole document</p> <p style="text-align: center;">---</p>	1-12
A	<p>WO 00 62505 A (THOMSON MULTIMEDIA SA                      ;FURON TEDDY (FR); QUES FLORENCE (FR);                      ANDRE) 19 October 2000 (2000-10-19)                      the whole document</p> <p style="text-align: center;">-----</p>	1-12

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International Application No

PCT/EP 03/06233

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0186948	A	15-11-2001	CN 1386367 T	18-12-2002
			WO 0186948 A2	15-11-2001
			EP 1282981 A2	12-02-2003
WO 0186914	A	15-11-2001	AU 5967401 A	20-11-2001
			EP 1281264 A2	05-02-2003
			WO 0186914 A2	15-11-2001
			US 2002006137 A1	17-01-2002
EP 1117214	A	18-07-2001	EP 1117214 A2	18-07-2001
			US 2002044225 A1	18-04-2002
			US 2002059637 A1	16-05-2002
			US 2002019984 A1	14-02-2002
			US 2002031120 A1	14-03-2002
WO 0062505	A	19-10-2000	FR 2792482 A1	20-10-2000
			AU 3658900 A	14-11-2000
			CN 1354946 T	19-06-2002
			WO 0062505 A1	19-10-2000
			EP 1169831 A1	09-01-2002
			JP 2002542672 T	10-12-2002
			TW 502513 B	11-09-2002

(19) World Intellectual Property  
Organization  
International Bureau



(43) International Publication Date  
29 September 2005 (29.09.2005)

PCT

(10) International Publication Number  
WO 2005/091218 A2

(51) International Patent Classification<sup>7</sup>: G06T 5/00

(21) International Application Number:  
PCT/US2005/008766

(22) International Filing Date: 16 March 2005 (16.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/553,934 16 March 2004 (16.03.2004) US  
60/553,932 16 March 2004 (16.03.2004) US  
60/652,475 11 February 2005 (11.02.2005) US

(71) Applicant (for all designated States except US): **ICON-  
TROL NETWORKS, INC** [US/US]; 502 Waverly Street,  
Suite 302, Palo Alto, CA 94301 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **RAJI, Reza**  
[US/US]; 1921 Oakdell Drive, Menlo Park, CA 94025  
(US). **GUTT, Gerald** [US/US]; 11693 Tortoise Trail,  
Tucson, AZ 85743 (US). **STEVENS, Chris** [US/US]; 730  
Bryant Street, Palo Alto, CA 94301 (US).

(74) Agents: **WILLMAN, George, A.** et al.; Wilson Sonsini  
Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA  
94306-1050 (US).

(81) Designated States (unless otherwise indicated, for every  
kind of national protection available): AE, AG, AL, AM,  
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,  
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,  
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,  
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,  
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,  
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ,  
TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA,  
ZM, ZW.

(84) Designated States (unless otherwise indicated, for every  
kind of regional protection available): ARIPO (BW, GH,  
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,  
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),  
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,  
FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,  
SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,  
GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— without international search report and to be republished  
upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guid-  
ance Notes on Codes and Abbreviations" appearing at the begin-  
ning of each regular issue of the PCT Gazette.

(54) Title: PREMISES MANAGEMENT SYSTEM

(57) Abstract: Some embodiments of a method for premises management networking include monitoring premises management devices connected to a gateway at a premises; controlling premises management devices connected to the gateway at the premises; receiving, at the premises, an uplink-initiation signal associated with a network operations center server; and in response to the uplink-initiation signal, initiating, from the gateway at the premises, communications between the gateway and the network operations center server; and communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices.

WO 2005/091218 A2

## PREMISES MANAGEMENT NETWORKING

### CROSS-REFERENCE

This application is related to and claims the benefit of the following United States patent applications:

5 U.S. provisional application number 60/553,934 for *Business Method for Premises Management*, invented by Reza Raji and Chris Stevens, filed March 16, 2004;

U.S. provisional application number 60/553,932 for *Premises Management Networking*, invented by Gerry Gutt and Reza Raji, filed March 16, 2004; and

10 U.S. provisional application number 60/652,475 for *Control Network*, invented by Gerry Gutt and Reza Raji, filed February 11, 2005.

Each of the foregoing applications is incorporated herein by reference in its entirety.

This application is also related to the following U.S. patent applications:

U.S. utility application number not yet assigned for *Premises Management Networking*, invented by Reza Raji and Gerald Gutt, filed March 16, 2005.

15 U.S. utility application number not yet assigned for *Business Method for Premises Management*, invented by Reza Raji and Chris Stevens, filed March 16, 2005.

Each of the foregoing applications is incorporated herein by reference in its entirety.

### BACKGROUND OF THE INVENTION

20 Vendors such as premises vendors, communication service vendors, and Internet portal vendors need a solution for extending their relationship with vendees beyond the immediate transaction. Additionally, vendees desire additional premises management services beyond the immediate transaction for premises, communication services, or Internet portals. There is a need for advanced premises management services.

### INCORPORATION BY REFERENCE

25 All publications and patent applications mentioned in this specification are herein incorporated by reference to the same extent as if each individual publication or patent application was specifically and individually indicated to be incorporated by reference.

### BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows an example of an overall network for premises management.

30 Figure 2 shows an example of a homebuilder-branded Internet portal for premises management.

Figures 3A-3C show examples of detailed screens of the portal interface for premises management.

Figure 3D shows a screen shot of a Internet Portal-branded portal for premises management according to an embodiment of the invention.

5 Figure 3E shows a screen shot of a main portal summary page according to an embodiment of the invention.

Figure 3F shows a screen shot of a portal showing details device information according to an embodiment of the invention.

10 Figure 3G shows an automation tab screen according to an embodiment of the invention.

Figure 3H shows a system tab screen according to an embodiment of the invention.

Figure 4 is a diagram of a business method for premises management.

Figure 5 is a diagram of a method for premises management networking.

Figure 6 illustrates an example of a control network environment.

15 Figure 7 is a block diagram of a control network with a gateway.

Figure 8 is a flow diagram showing data being transformed, physically and logically, by a gateway.

Figure 9 is a flow diagram showing the data conversion.

Figure 10 is a diagram showing a gateway binding mechanism.

20 Figure 11 is a diagram showing a camera snapshot scenario.

Figure 12 is a diagram showing a camera environment.

### **DETAILED DESCRIPTION OF THE INVENTION**

Figure 1 shows an example of an overall network for premises management. A premises 110 has premises management devices such as a smart thermostat 112. The premises management devices are connected to a premises network 114 which can be, for example, an RF and/or power line network. The premises network 114 is connected to a gateway 116 which in turn is connected to a broadband device 119 such as a DSL, cable, or T1 line. The gateway 116 can alternatively or also be connected to a dial up modem 118. The premises 110 is connected to the Internet 120. The Internet 120 is connected to system managers at the network operations center 150. The Internet 120 is also connected to customers of the system manager, for example vendors such as premises vendors, communication service vendors, or Internet portal vendors. The Internet 120 is also

25  
30



connected to vendees 140, such as premises vendees, communication service vendees, or Internet portal vendees.

Figure 2 shows an example of a homebuilder-branded Internet portal for premises management.

5           Figures 3A-3H show examples of detailed screens of the portal interface for premises management. Figure 3A shows a main screen summarizing premises management services. Figure 3B shows a screen summarizing security management services and safety management services. Figure 3C shows a screen summarizing energy management services.

10           Figure 3D is another example, illustrating how services offered by the system can be branded and incorporated into a third part web portal, for example, in a personal portal such as one provided by Yahoo. The screen includes the usual Yahoo portal content such as the stock pane on the left, the news pane on the top and the calendar pane on the right. The system-specific pane is included on the bottom where the user can access monitoring and control information on the home or business. The look and feel of the system pane can be  
15 tailored by the service provider.

          The system portal summary page in Figure 3E shows a snap-shot of the state of the various devices in the user premises. At the top left is a drop-down box that displays the name of the premises being shown on the screen. The user can change premises by clicking on this box and selecting a different premises. A series of tabs allow the user to switch to  
20 Details, Notifications, Automation, Schedules and Systems screens for performing other system functions. The various panes on this page highlight different features.

          The status pane lists the different devices in the user premises along with their actual states. The pending updates pane shows the time of the last communication between the premises and the server as well as any pending updates waiting to be sent downlink to the  
25 premises. The pictures pane shows the last several (e.g. last four) pictures taken by the camera in the user premises. The user can click on a thumbnail picture to look at a larger version of the photo as well as access archived images for that camera, look at live video, take new pictures or delete photos. The schedule pane shows the schedules activities for the premises. The alarm history shows an archive of the most recent event and activity in the  
30 user premises. The reminders pane provides a means for the system to remind the user to perform certain activities or functions related to their home or business. The mode drop down button on the blue navigation bar allows the user to switch between the systems modes. The QuikControl drop down allows the user to control any device that is controllable (e.g. camera, thermostat, lamps, etc.).

Figure 3F shows a details screen of the portal showing details device information. The details screen allows the user to show more detailed device data. The list on the left displays the system devices and their actual states/values. The pictures pane on the top right display the camera thumbnails (beyond the 4 displayed on the summary page). The thermostat pane on the bottom right shows the details of the thermostat data including the current temperature, cooling and heating set points as well as the thermostat mode.

Figure 3G shows an automation tab screen. This screen shows how the user may assign automation rules to devices such that an event caused by a device can trigger one or more actions by other devices. The left column shows all possible events that can occur based on the devices that belong to this premises network. The three columns, one per mode, identify the action for each event for that mode. For example, the figure shows that when hall motion sensor occupied event occurs in the away mode, the conference room camera takes a picture. The bottom portion of the screen shows that the wireless keychain remote control's buttons can also be programmed by the user to perform any action desired.

Figure 3H shows a system tab screen showing status of devices. The System screen shows a list of all the devices in the premises' network, including the gateway. Each device in the system is on a separate line. The first column shows the name of the device along with a status indicator which show different colors based on the status of the device (green for ok, yellow for offline, red for not found or problematic). There is also a "last update" column that displays the date and time of the last signal received from that device. The third column (device) describes the type and model number for that device. The user can get more detailed information about a device by clicking on the line corresponding to the respective device.

Figure 4 is a diagram of a business method for premises management. In 410, an Internet portal is available for access to a vendee, such as a premises vendee, communication service vendee, and/or an Internet portal vendee. In 420, at least after a transaction between the vendor and the vendee, such as a premises transaction, a communication services transaction, and/or Internet portal services transaction, premises management services are provided via the Internet portal to the vendee. In 430, the Internet portal is branded with the brand of the vendor. The shown steps can be added to, removed, rearranged, and/or modified.

Figure 5 shows a diagram of a method for premises management networking. In 510, premises management devices connected to a gateway at a premises are monitored. In 520, premises management devices connected to the gateway at the premises are controlled. In 530, an uplink-initiation signal associated with a network operations center server is received

at the premises. In 540, in response to the uplink-initiation signal, communications between the gateway and the network operations center server are initiated from the gateway at the premises. In 550, during the communications between the gateway and the network operations center server, information associated with the premises management devices is  
5 communicated.

Property developers and service providers can:

1. Differentiate their offering from their competitors'
2. Generate new recurring revenue through new, value-added services
3. Reduce their operating costs
- 10 4. Increase the value of their offering
5. Increase the effectiveness and reach of their brand
6. Make smarter, knowledge-based business decisions
7. Increase customer retention and satisfaction

Additional content leverages the broadband infrastructure, thereby increasing the  
15 effective value of the broadband pipe.

Property developers/managers and service providers are facing ever increasing competition and lack the expertise, time and resources to offer control and telemetry services to their customers. Connecting people to devices is the next evolutionary step for the Internet.

20 Some of the architectural/design goals for the system are low cost, ease of use, and scalability.

The architecture and products/service offering is flexible enough to cater to the needs of the homeowner while being scalable and intuitive enough to allow for easy installation and minimal support.

25 Three types of customers are envisioned for the system. Although the ultimate end user is the property owner, customers can be: home developers and commercial property, e.g. multiple tenant unit (MTU) owners and managers; service providers (telcos, cable companies, ISPs, etc.); and homeowners or commercial building tenants.

30 The actual user of the services resides in the premises where, for example, the gateway and devices are installed. The system can be intuitive enough that the "average" end user can perform the installation and configuration steps.

The installer can be the person or entity that installs the gateway and the devices in the home, configures the gateway, connects the gateway to the Internet and/or telephone line and/or performs any troubleshooting necessary. Depending on the actual customer, the

installer can be 1) the installation crew of the service provider or property developer, 2) an outsourced installation outfit hired by the service provider or property developer, 3) an outsourced installation outfit hired by the end user, or 4) the end user.

5 The premises gateway can be a low-cost and stand-alone unit that connects the in-  
premises devices to the server. The connectivity to the Internet can be accomplished via a  
broadband connection (T1, DSL or cable) and/or via the telephone line. Though broadband  
connectivity is preferred due to its persistence and throughput, telephone connectivity is  
recommended to be present as a back-up option in case the broadband connection is lost. For  
premises without a broadband connection (e.g., vacation homes) a telephone-only connection  
10 can be used.

The service portal provides an intuitive end user interface to the premises network as  
well as access to system and network configuration screens and user account information and  
settings.

15 Some embodiments of the overall system can be put in use through the following  
steps:

1. Customer need for telemetry services is established
2. Customer (via web or phone) orders a system
3. Customer acquires system (via service provider, builder, etc.)
4. A service account is established (by the service provider/builder  
20 or by the homeowner or system manager)
5. Gateway is registered (by the service provider/builder or by the  
homeowner)
6. Gateway sends network/device information to the server
7. Homeowner configures own home (alarms, notifications, binding, etc.)
- 25 8. Future devices are added to system either via pre-configuration by system  
manager or via the end user through configuration screens on portal

Each of these steps is described below:

**Customer need is established**

30 This can done through the property developer, the service provider sales channel or  
direct advertising by the system manager.

**Customer orders a system from system manager**

The customer specifies what kinds of devices are needed and where each one will  
reside in the premises (e.g., living room thermostat, lobby motion sensor, etc.). The user

account is then appended by system manager to include this information as well as the actual unique ID for each device shipped to the customer.

#### **Customer acquires system**

The gateway and devices can be acquired by the customer in several ways:

- 5 1. Pre-installed by the property builder/developer/manager or service provider
2. Directly purchased by the end user

The choice of devices can depend on the particular services and functionality desired by the customer.

10 Once the customer acquires the gateway and devices, the devices are physically installed in the premises. This task can be performed with the help of an installer, or for smaller premises, performed by the end user.

#### **A service account is established**

15 This is generally done by the end user as the process uses personal information (name, payment option, etc.). The account registration involves the user logging on to the system manager web site and establishing a new account by entering name, address, phone number, payment details and/or the gateway serial number printed on the gateway in the end user's possession.

20 In some cases the system manager service account may already be pre-established with the gateway serial number and the end user simply has to update the account with personal and payment information. This scenario eliminates the need for the end user to deal with any cumbersome serial numbers or keys and is really more of a personalization step.

Multiple gateways can also be handled per user account.

#### **Gateway is registered**

25 This step involves the association of the user account on the system manager server (established in the previous step) with an actual gateway in the user's home. The gateway is connected to a broadband network or the telephone line in the home.

30 For this step, the installer, for example, presses a SYNCH button on the gateway, and initiates an uplink communication from the gateway to the system manager server using a default (first-time) IP address or, in the case of a dial-up-only connection, a toll free number dial by the gateway.

Upon establishing a connection with the server and locating its corresponding user account (e.g., established in a prior step), the gateway acquires a system manager server IP address (to be used from that point on for all gateway to server communication), and changes its state from unregistered to registered.

In the case where the gateway is pre-installed by the developer or service provider, this step may have already been performed.

The gateway may not be able to perform any functions until it has gone through this registration process (as indicated by the state of the gateway).

5           **Gateway sends network/device information to the server**

This is done on a regular basis and can always be initiated by the gateway. The server dictates the interval for uplink communication initiation between the gateway and server.

**Homeowner configures home (alarms, notifications, binding, etc.)**

10          This is the normal use of the system manager portal whereby the user selects the various monitoring, logging and notification options.

**Future devices are added to system**

The end user obtains additional devices from the system manager, in which case they are added to the end user system by the system manager before being shipped to the customer.

15          Alternatively, the end user could purchase a device from a third party source in which case they could use the system manager portal interface to add (or replace) the device manually.

          In addition, the system manager gateway can have a provision for “discovering” devices by listening for RF messages (e.g., GE Interlogix) or service pin messages (e.g.,  
20          LonWorks devices).

**Overview**

Parts of the system as a whole are described, including the gateway, the server and the web portal interface.

**System overview**

25          At the highest level, the system provides its users with a hosted and managed service for premises device monitoring and control for a fee, such as a monthly subscription fee. The premises markets include residential homes, commercial MTUs as well as small businesses.

          The traditional complexity and expense of installing and maintaining such a system is delegated to the system manager platform. As a revenue-grade Application Service Provider  
30          (ASP) business, the system provides reliability, scalability, security, cost-effectiveness, ease-of-use, and flexibility.

          The term “system” can denote the portal, server, gateway and end devices.

**Reliability**

The system can provide a high degree of reliability. This includes 24-7 operation of the Network Operations Center (NOC) and the server software it contains, and the reliability and fault-tolerance of the gateway and the control devices.

5 **Scalability**

The system, specifically the NOC, can scale to accommodate large numbers (in one embodiment, millions) of gateways and devices (in one embodiment, tens of millions). Though this may not be used at the onset, necessary architectural provisions can be built into the system to allow for such expandability.

10 **Security**

As a revenue-grade service offering, the system provides security against intentional and unintentional interference with the normal operation of the system. The system can be reasonably immune to external unauthorized access (either over the Internet or device network media). The system can provide reasonable protection against spoofing (of NOC server, gateway or device).

15 **Cost-Effectiveness**

Similar systems in the past have suffered from a high cost of in-premises devices and gateway as well as high and/or unpredictable installation costs. The system installation process is simple in order to minimize, if not eliminate, the installation costs.

20 **Ease-of-use**

The gateway and device installation process as well as the various user configuration and normal use menus/screens presented by the portal are, according to an embodiment, intuitive and easy to use. This eases the adoption and continued use of the system by its users.

25 **Flexibility**

The system is flexible enough to easily handle different device networking protocols/technologies should the need arise in the future. In addition, the system, including the web interface, can be adapted to different markets and applications.

**Variable Logging**

30 The system can log any device variable specified by the user for up to, for example, 30 days. The user defines a logging interval for each variable at the time of configuration. The logging feature can be handled by the gateway on the local device side and the data can be transferred to the server at regular intervals. The overall variable log for all variables can be kept on the server side.

Logging of data for more than, for example, 30 days (but no more than, for example, 180 days) can be provided to the user, for example for a nominal fee.

The system can allow for the logging of at least, for example, 10 variables per gateway. The minimum logging interval for any variable can be, for example, 5 minutes.  
5 Logging intervals provided can be, for example, 5, 15, 30, 60, 180 minutes as well as 6, 12, 24 hours and weekly.

#### **Activity logging and tracking**

10 The system must be able to provide at least, for example, a 14-day history log of all user, system and device actions. An action includes a change to a device variable, system or network settings brought on by either the system or the user (e.g., variable changed, logging enabled, device added, user notified, etc.). The user can trace back system activities to their cause and to the date and time they occurred. Past activities can be searched by variable,  
15 device, category or date.

#### **System modes**

The system can support user-defined modes, such as "home", "away", "sleep", "vacation", etc. The mode the user network is in plays a factor in the determination of the actions taken (reporting, alarming, eventing, notification, etc.) by the system when variable changes occur.

20 System mode can be changed by the user via methods such as:

1. Via the portal interface
2. Through a schedule set by the user
3. Via a binding (a variable change tied to the mode change – e.g., RF remote control)

25 The system can provide a set of default modes based on the user profile (homeowner, business, vacation home, etc.). These default modes are a starting point that can be changed or added to by the user at any time.

#### **Alarming**

30 The user can specify alarm conditions for variables with discrete states (e.g., binary ON/OFF). These alarms can be reported in real-time (i.e., immediate uplink) by the gateway to the server. The server then in turn looks at the data and determines, based on user alarm settings, whether to notify the user or not.

Alarm conditions can be determined based on the value or state of a variable as well as the system mode.



### **Eventing**

For non-critical events, the system can notify the user in non-real-time fashion regarding the state of any variable specified by the user. The variables chosen for user eventing can be of any kind (discrete or continuous). The gateway updates the server with the change of variable state/value at a regularly scheduled upload. The server continuously looks at variable data and determines, based on user eventing settings, whether to notify the user or not.

Eventing conditions can be determined based on the value or state of a variable as well as the system mode.

### **User notification**

The system can support user alarming and eventing via the following methods: email, text messaging, pager, and/or voice telephone call (voice synthesis).

### **Device data monitoring and control**

The user can specify any device variable for monitoring and control via the server portal. For example, up to 255 devices can be supported by a single gateway. For example, up to 512 variables can be supported by a single gateway.

The user can schedule specific variable updates (e.g., turn off thermostat at 8am every Tuesday). Scheduled events can be canceled (gateway-server protocol can support this). A scheduled variable update is allowed, per time stamp and variable ID. If time stamp and variable ID match an existing scheduled variable change, then the value for that pending variable change is re-written with the new value. A given variable can have multiple scheduled values as long as each scheduled update has a different time stamp.

Any pending downlink variable change commands can be canceled that have not been relayed to the gateway at any time through the portal interface.

### **Device Network Support**

The system can support an open architecture where most, if not all device networking protocols can be supported. Examples of specific device protocols supported by the system include RF and powerline protocols, such as GE Interlogix RF and Echelon LonWorks power line (PL & FT), simplifying the installation burden by requiring no new wires to be installed in a premises.

The LonWorks free topology twisted pair medium (FT-10) can be supported as an option to better support commercial applications (e.g., office buildings).

All devices, regardless of the technology, can possess these attributes:

1. Unique ID (global)

2. Non-volatility. Must not lose any pertinent data or state.
3. Low-battery indication over the network (if battery-operated)
4. Tamper detection (if security-sensitive)

5           **RF**

This system includes a low-level, simple unidirectional protocol for multiple sensors to talk to a receiver head end. The protocol needs and footprint are relatively small and as such the RF devices are comparatively low-cost and small. They also can function for several years without the need for a battery change for simplified installation and  
10 maintenance of the system by the user.

A bi-directional RF transceiver can be supported by the system. This allows for control as well as monitoring of remote devices (e.g., thermostat) by the user.

The following RF devices can be supported by the system:

1. Door and windows sensor
- 15 2. Motion sensor
3. Smoke alarm
4. Water sensor
5. Freeze sensor
6. Contact closure sensor (e.g., ITI DWS with external connector pins)
- 20 7. CO alarm
8. Heat sensor
9. Thermostat
10. RF remote control

**PL**

25 The power line solution offers a robust and reliable mechanism for communicating over existing residential power line wiring.

The following PL devices can be supported by the system:

1. Thermostat (e.g., RCS)
2. Load controller (e.g., Halen Smart)
- 30 3. Relay actuator (e.g., Comap)
4. Photo camera, e.g., black & white, low-resolution (with motion sensor)

**FT**

The Free Topology solution offers a cost-effective medium for commercial applications. Many third party LonWorks devices use this medium for communications.

**Other Devices**

The following is a non-exhaustive list of a few other devices supported by the system.

1. Small data/message display – for text messages, news, weather, stock, photos, etc.
- 5 2. Door latch control
3. Pool/spa controller
4. Weather station
5. Lighting control
6. Elderly or disabled monitoring
- 10 7. Irrigation controller (Bibija)
8. VCR programming

**Cameras**

The system can support cameras. For example, standard off-the-shelf IP cameras (also referred to as web cameras) may be used, such as those available from vendors such as  
15 Axis, Panasonic, Veo, D-Link, and Linksys, or other cameras manufactured for remote surveillance and monitoring.

Surveillance cameras may contain a standalone web server and a unique IP address may be assigned to the camera. The user of such a camera would typically retrieve the camera image by accessing the camera's web page through a standard web browser, using the  
20 camera's IP address. In some cases the IP camera acquires a local IP address by using a DHCP client to negotiate an address from the local DHCP server (usually residing in the user's router/firewall).

According to an embodiment, the gateway treats camera images as it does other sensor or device data. User commands to "snap" a picture are sent from the system's  
25 portal/server to the local premises gateway during scheduled communications between the gateway and server (initiated by the gateway). Alternatively, a picture "snap" command for a local or remote camera can be initiated by a sensor (e.g., motion detector, remote control, etc.) on the local device network. The gateway then in turn talks to the camera over the IP network (wired or wireless) to retrieve the image and pass that image up to the system's  
30 backend server, effectively acting as a pass-through agent for the camera.

Since the data from the gateway (including the camera image) is pushed up from the gateway to the server using standard HTTP protocol (used by web browsers), additional configuration of the user network may be avoided. Also, adjusting of the user's firewall (port forwarding, DMZ, etc.) may be avoided (i.e., simpler installation and enhanced security).

Also, the push mechanism eliminates all the issues related to accessing the camera from the Internet, namely firewall and dynamic IP issues mentioned above, since the user gets the images from the system servers and not from the premises directly.

5 The system's user portal interface acts as a unified user interface for the user by displaying multiple images from different cameras in the same user interface page (e.g., web page).

The system's IP cameras can be physically located anywhere as long as they are connected to the Internet (if remote) or to the local IP network (if local).

10 Due to the fact that the images are served from the system's server (as opposed to the local camera or network) potential security exposure of accessing the home network directly from the outside may be avoided. Also, additional security measures can be put in place (e.g., SSL) to block an unauthorized user from accessing the images on the server.

#### **Device low-battery notification**

15 The system can notify the user via the web portal of any low-battery conditions for the devices that operate on battery (e.g., GE Interlogix devices).

#### **Server-side binding**

20 The system can send variable control information downlink based on variable information collected through the uplink connection. This rule-based exchange can take place within the same atomic uplink-downlink (request-response) exchange between the gateway and server. The user specifies the actual "rules" for such bindings (e.g., turn off the thermostat when there is no motion in the premises for 2 hours).

This implementation may impact scalability because of the atomic communication factor.

#### **Local binding**

25 Local binding can permit a more real-time interaction between devices. This functionality can take place without the server's involvement (other than the initial configuration of the local rules). The local binding, given the different technologies used at the device level, needs to be routed through the gateway.

#### **Gateway Shoulder Tap**

30 The server can "call" a gateway if the user requests that a variable change be propagated to a device in real-time (rather than waiting for the next gateway uplink connection).

### **Device sharing between different users**

The system can provide a means for a single device to be managed by multiple users. For example, a security gate or a pool temperature sensor in a property common area should be accessible by all residents in the complex.

5

### **Gateway**

The gateway is the central link between the premises device network and the backend server. It can be a thin, low-cost client of the server and use the least amount of hardware and software without compromising the basic functionality and objectives of the overall system.

10

### **Internet connectivity**

The gateway can provide both a connection to a broadband network (Ethernet DSL or cable modem) and telephone network. The telephone network connection provides a second, redundant route for accessing the server in case the broadband network access is down and there is a need for the gateway to report critical alarm information uplink to the server. The telephone connection also provides a means for the system to support premises that have no broadband connection available (e.g., as in many second or vacation homes).

15

The gateway can terminate any data call in process if a user picks up a telephone and provide a dial tone immediately. In addition, the gateway may not initiate a data call if the phone is in use by the user (off hook).

20

They gateway can dial out in the absence of external power to the gateway.

### **Communication with server**

The gateway can initiate all communications with the server. Gateway communication can either initiate based on a predetermined schedule (e.g., every 30 minutes) or due to a local premises alarm (selected by the user).

25

Gateways can contact a common server for their first uplink connection in order to obtain their assigned gateway server address, which they can use for all subsequent uplink connections (unless changed later by the system). In the event that the gateway cannot connect to its designated gateway server, it can fall back to contacting the default initial gateway in order to refresh its gateway server address.

30

The predetermined call initiation schedule can be programmable by the server and can provide different intervals for broadband and telephone intervals (e.g., every 30 minutes for broadband and every 90 minutes for telephone).

By assigning the gateway-server communication initiation to the gateway the system can enjoy the following benefits:

1. Most if not all issues generally attributed to routers, firewalls and NAT are eliminated, as the gateway is now simply an HTTP client (much like a web browser).

5 2. Security against outside hackers is greatly increased as access into the gateway can be disallowed. The gateway knows whom it can talk to (server) and it does so when it needs to.

A possible disadvantage of a push-only scheme can be an inability of the server to provide "real-time" device control. This can be a relatively minor disadvantage minimized  
10 through the shoulder-tap mechanism.

### **Gateway Shoulder Tap**

The gateway can have the provision of initiating an uplink communication based on a telephone ring signal detected on the phone line. This shoulder tap from the server allows the  
15 server to pass down a variable change to the gateway without having to wait for the next gateway uplink connection.

A drawback of a telephone line shoulder tap is the occasional ringing on the telephone line. It is difficult to detect an incoming ring reliably without the phone actually ringing. This is fairly benign when considering:

20 1. Most user variable change requests (control) may not have to be done in real-time and can occur at the next scheduled gateway uplink synch.

2. Most often the premises (e.g., home) being controlled in real-time is unoccupied.

25 3. The shoulder tap can at most ring the phone only once so the user can wait for the second ring before picking up the phone

4. The user can opt to provide a second phone line dedicated to the gateway.

Implementing shoulder tap over IP is another embodiment with a more complicated installation process (e.g., router/firewall configuration, opening ports, etc.). Keeping an IP connection alive between the gateway and server can be unreliable and could heavily burden  
30 the server.

### **Configuration**

The gateway can be installed without any special skills. The NOC server can handle the complexity of configuration.

Once plugged into a power outlet as well as a broadband and/or telephone network, the gateway can:

1. Determine if there is a broadband connection available
2. If so, obtain an address from the local DHCP server
- 5 3. Make sure the telephone connection is operational
4. Contact the server for the first time and check to see if there is a user account associated with it (this can be a secured inquiry to eliminate hacking)

5. If there is no associated user account found, notify the user (e.g., blinking LED on front panel)

#### 10 **Device Discovery**

The gateway can be put into a device discovery mode via, for example, a front panel push button. Devices can normally be introduced to the system and assigned to the user:

1. By system manager before shipping out to the user
2. By the user/installer via the portal device registration screens

15 The discovery mode is a third way of registering devices. The discovery mode allows the gateway to listen for and discover new devices added to the network – should there ever be a need for such functionality. Upon discovery of a new device the information is passed to the server for further processing and registration. The user can then finalize the device registration process through the system's portal (e.g., assigning names, alarming, etc.).

20 If the user can specify the adding of a device, it can be configured by the user immediately on the portal. Auto-configuration comes with set defaults. Another similar device to copy can be specified.

#### **Auto recovery**

The gateway can be self-sustaining and autonomous.

25 In the event of communication failure between the gateway and the server for an extended period of time the gateway can continue to do its tasks (e.g., variable monitoring, logging, etc.).

In the event of an extended power loss or a system reset, the gateway can resume normal operation after the appropriate "boot-up" period (i.e., no more than 2-3 minutes). A hardware buffer can receive, e.g., RF signals during bootup.

30 Any pending scheduled events that did not occur because of the power loss can be performed once the gateway has resumed normal operation and can occur in the original order defined by the user.

In the event that the gateway software “hangs,” the gateway can recover itself through a built-in watchdog-monitoring feature.

### **Rule-based “binding”**

#### **Gateway power interruption**

5 The gateway can operate for at least, e.g., 5 minutes after a power failure in order to report its latest status (including the power status) to the server (either via broadband or telephone). The gateway may not use a rechargeable battery in order to eliminate the need for gateway servicing when the battery reaches the need of its life (e.g., typically 2-3 years).

10 The gateway can withstand power interruptions without losing any pertinent data (e.g., device data, log data, date & time).

For applications where the gateway and devices are to operate in the absence of power, the user can obtain and use an uninterruptible power supply (UPS).

#### **Remote firmware upgrade**

15 The gateway can receive firmware upgrades over its WAN connection (Internet or PSTN). The gateway can have provision for recovery in case there is an interruption during a firmware download (e.g., network connection loss).

20 The gateway firmware upgrade is an automated process initiated by the gateway based on a schedule downloaded from the server during a gateway-server exchange. The upgrade process may not involve any user interaction or involvement and may take place when the user is least likely to be using the system (e.g., at night).

#### **Variable logging**

25 The gateway can provide enough storage for logging one day worth of data for, e.g., 10 variables logged every, e.g., 15 minutes. In the event that the local gateway log is filled up before the gateway has had a chance to upload the data to the gateway, the gateway can stop logging additional data and report a “log full” error to the server at the next uplink connection.

#### **Security**

30 Appropriate security measures can be provided by the gateway to ensure protection against:

1. Inadvertent communication with neighboring networks and devices not related to a gateway/user.
2. Intentional external hacking into the system from the WAN side (Internet and PSTN).



3. Intentional external hacking in to the device network side (PL or RF).

**Power consumption**

The gateway can use minimal operating power in order to reduce the cost associated with the power supply as well as the circuitry to keep the gateway alive immediately after a power failure.

**Form factor**

The gateway can be encased in a visually attractive enclosure that is generic enough for multiple markets including consumer applications and commercial building applications (schools, etc.).

**Ease of use**

The gateway can use the simplest possible installation procedure. The gateway can “figure out” how to communicate with the NOC (broadband and/or PSTN) once the power has been connected to it. No user involvement may be necessary for this to take place.

**User interface**

The gateway’s user interfaces include the following LEDs and switches:

POWER LED

COMM LED: communication happening between gateway and server

DEVICE LED: Device communication (PL or RF) happening. This LED can also be used for the device discovery feature.

ERROR LED: Displays different errors using different blink rates (log error, synch error, comm. error)

SYNCH switch: Initiates a gateway-server uplink communication

**Gateway local reset**

The gateway can provide a way for it to be reset locally by the user. Upon the execution of this gateway reset function, the gateway can be in the factory default state with no device, variable, user or configuration variables residing in it.

The reset operation for the gateway can be performed by, e.g., holding down the SYNCH switch for 20 seconds.

**Agency certifications**

The gateway can be designed to comply with both FCC Part 15 (Level B) and Part 68 certifications.

If an external Tamura power supply is not used, then gateway design can meet the standards for the appropriate regional safety agency certification (i.e., UL, CSA, CE, and TUV).

### **Error reporting**

5 The system can report error to the user and/or administrator when the following conditions occur:

1. Downlink variable update failed
2. Gateway synch delayed or missed
3. Missing variable poll value
- 10 4. Variable log full
5. Broadband or phone line connection down

### **Server**

The server provides a hosted, reliable and secure “server-in-the-sky” for the premises gateways to communicate to and for the users (customers) to access for accessing and  
15 controlling the various devices in one or more premises.

### **Reliability**

The NOC facility can be run by a managed hosting service and as such provisions for power failure and security (theft) can be in place via the vendor providing the hosting service.  
20 However, the NOC server software architecture can support certain backup features.

All user, system, network, gateway and device data contained by the NOC server can be backed up on a regular schedule (e.g., once a day).

When NOC server hardware malfunctions, that hardware can be quickly and easily replaced with minimum user downtime.

### 25 **Security**

The server can communicate to the gateway in a secure fashion.

The data can be encrypted when transferring between the gateway and server, as well as ID/password for authentication.

### **Scalability**

30 The server software can be scalable such that it can support a large number of gateways over time. The scalability sold also enables the server to have a small foot print at the beginning when the number of gateways may be relatively small.

**Platform**

The interfaces between the servers and modules can be in XML in order to provide maximum flexibility and scalability. No requirements may be imposed for the operating system or programming language platforms used.

5 **Server API**

The server can provide an API (via XML and SOAP) that permits third party applications to get full access to the functionality of the server.

**Portal**

10 The portal can support web, WAP and PDA access points. An important attribute of the portal is ease-of-use.

**Customization**

The portal can present an automatically-customized UI to the user based on the application (e.g., residential, commercial, etc.) and the devices used (e.g., security, energy, safety, etc.).

15 As a secondary feature the portal can also allow the user to easily customize their portal for their particular needs.

Lastly, system manager personnel or authorized agents can further customize a portal for a specific customer (e.g., a telecom) or class of customers (e.g., homeowners of a home builder). This process can put a specific "skin" on a customer portal.

20 **User account screens**

These screens allow the end user to open an account and register the end user's gateway(s). Screens can be included for obtaining billing/payment info and other user information (e.g., address, primary contact information, phone number, etc.).

25 In addition, this can be where the user enters their gateway ID(s) (on the gateways) so the system can make an association between the logical user account and the physical user network(s)/gateway(s).

User notification options (email, phone, page, text messaging, etc.), as well as time zone, uplink interval can also be selected here.

30 The option to customize the WAP portal interface can be provided so the user can select the variables and the functionalities that are presented on a WAP device accessing the service.

### **Device registration screen**

The user can register devices obtained from other sources— assuming they were not pre-registered already by the system manager. The user can enter the unique device ID and the device name, etc.

5 The ability to delete a device from the local user network can be provided. History related to the device being deleted (log data, action tracking, etc.) can be removed from the system, e.g., 30 days after the device deletion.

The gateway can know if something succeeds or not and report it back to the server. Similarly, each “command” the server performs on the gateway can be tracked back when the results of what the gateway did with it come back (e.g., success, fail, etc.).

10 The gateway can report the downlink changes like it reports uplink changes. The state change of the variable in question (e.g., Change thermostat setpoint) can appear in the log like any other variable, along with its time stamp.

The portal can set the change, then after the change occurs it can verify it is reported in the log. For example, if the portal is asked to turn the light on, it can be ensured that it happened “once and only once” and if it failed, that can be known.

The ability to replace a device in the local user network can also be provided. Old log data for the replaced device can be kept without a break in the device’s data (i.e., the log can start getting values from the new device. Also, since the downlink values are set on the new device, those initial settings can also appear in the log.

### **Network configuration screens**

This is where the user configures the device network and sets preferences and options (e.g., which variables to monitor, logging options, etc.).

25 Provisions for creating variable groupings are also provided here (i.e., defining a single variable that represents the collection of all similar type variables selected by the user – either ANY or ALL function (OR or AND)— e.g., all door/windows sensor states).

The user selection of which variables are monitored for eventing and alarming is performed here as well.

### **Normal usage screens**

30 These represent the main screens used most often by the user on a day-to-day basis. Typical functionality provided includes: network summary, variable monitoring, variable control, variable logging, system activity log, system status, alarms, etc.

### **WAP Interface**

The portal can also provide a simplified interface for supporting WAP devices. The functionality can be a limited subset of monitoring and control services offered by the web portal.

5 The customization of the WAP portal interface can be done through the normal Web interface screens

### **PDA interface**

The portal can also provide a simplified interface for supporting browsers running on PDAs. The functionality can be a limited subset of monitoring and control services offered  
10 by the web portal.

The customization of the PDA portal interface can be done through the normal Web interface screens (see above).

### **Permission Levels**

The portal, in association with the server, can provide configurable user access and  
15 permission levels for both inter-account (e.g., different premises) and intra-account (e.g., mom, dad & kid) isolation.

### **Other features**

1. A desktop application in the icon tray that reports alarms and events in the background.
- 20 2. Support for larger premises (single user with multiple gateways)
3. Support for multiple users/locations per gateway
4. Rule-based local binding
5. IPSec (e.g., via HiFn chips)
6. Support for LonWorks free topology (FT-10) devices by the gateway

### **Control Network**

25 An embodiment of a control network may comprise a collection of sensor and actuator devices that are networked together.

Sensor devices are devices that sense something about their surroundings and report what they sense on the network. Examples of sensor devices are door/window sensors,  
30 motion detectors, smoke detectors and remote controls.

Actuator devices are devices that receive commands over the network and then perform some physical action. Actuator devices may include light dimmers, appliance controllers, burglar alarm sirens and cameras. Some actuator devices also act as sensors, in that after they respond to a command, the result of that command is sent back over the

network. For example, a light dimmer may return the value that it was set to. A camera returns an image after has been commanded to snap a picture.

The core of an embodiment of a control network is an architecture where sensor devices are coupled to actuator devices. A light switch, for example, may turn on a lamp through a light dimmer actuator. A door/window sensor or smoke detector triggers an alarm. Other devices may also be controlled in various ways.

Figure 6 illustrates an example of a control network environment. Here three different networks with devices are depicted (GE security, LonWorks, IP). The LonWorks network includes a light switch and lamp, the GE network has some door sensors and an alarm controller, and the IP network has some IP cameras attached.

Note that the computer in the middle of the network may be used to bridge the various networks, essentially providing interoperability, but with available existing technologies that calls for a custom solution requiring expensive custom software. Otherwise, the three control networks are independent.

Figure 7 depicts one embodiment of an architecture that uses these described concepts.

Here we see the same three local networks on the premises (IP, LonWorks, GE Security). However, now they are all connected together by the system gateway. Furthermore, the system gateway is attached to the internet, through which it regularly contacts the system servers in order to send up new data and get back control and configuration information. Clients can monitor and control their premises using ordinary browsers on a wide variety of devices by accessing the system servers.

Note that, at the premises, use of a PC or custom programming to achieve interoperability between different device technologies, or to provide remote monitoring and control may be avoided. Instead, in an embodiment both functions are performed by the system gateway, which according to an embodiment is designed to interface to a variety of device technologies and provide an abstraction layer that helps the rest of the system (servers and clients) to be technology-neutral.

30

### **Sensor/Actuator Device Abstraction**

Sensor and actuator devices are abstracted at the gateway hardware level so that different devices from different manufacturers can be handled seamlessly. Embodiments may support devices from several different manufacturers (for example, GE Security, Axis

Communications, Axsys Systems) using three different communications technologies (unlicensed-band RF for GE devices, Internet Protocol for IP cameras, and powerline for LonWorks modules).

### **Gateway Device**

5 The gateway device performs the hardware abstraction function according to an embodiment of the invention. The gateway includes the hardware and software required to communicate with all supported device technologies. Software on the gateway converts the raw data received from the device to an indexed data point. Periodically the gateway sends the data to the server, with each datum tagged with its data point index and time stamp.

10 In an embodiment, the server performs substantial operations for data storage and user interface.

### **Gateway – Server Data Interface**

Between the server and the gateway, an embodiment of the system uses a device-property-value model. Each device supports some number of properties that expose its capabilities. For example, an embodiment of a door sensor has a state property (open or close) and a battery-level property (low or ok). Both the devices and their properties are given indexes when the gateway is configured, and all subsequent data exchange uses the indexes to identify the property involved. This indexed property ID may also be referred to as an “indexed data point.”

20 Figure 8 illustrates how data is transformed, physically and logically, by the gateway.

The door sensor has detected an open door, and sends the gateway a message with its hardware ID and raw value. The gateway interprets the data, converts it to an indexed data point value, and sends it to the server as device #1, property #0, set to 1 (true). Note that the device ID is converted to the configured device index (1), and the changed property is identified by its property index (0).

25 In the second case, the client wants to take a picture, so the server sends down the value (in this case, the desired picture name) indexed by the camera’s device index (2) and the camera’s picture property’s index (1). In this case, the gateway initiates a web service to the camera to access (and upload) the image, then sends back the result of that operation to the server, again as an indexed data point.

30 According to an embodiment, the camera and a door sensor are both handled identically by the server and in the server-gateway protocol, using the device+property model.

### **Common Device Definition Format**

In the server infrastructure, the device data is handled as indexed data point values. When the data is presented to the user, it is reinterpreted. The device definition file is the mechanism that permits the server software to handle this reinterpretation with a single,  
5 common code module, independent of device types or technologies.

Physical devices are defined using a common device definition file format which provides the information necessary to convert the device- and technology-specific view of a device to an abstracted, generalized view.

### **Function Types and Properties Abstraction**

10 In order to allow client inspection and manipulation of sensor/actuator devices in a device- and technology-independent manner, device capabilities are mapped to standard function types, each of which defines one or more standard properties. This permits client software to, for example, query the system for temperature measurements, without necessarily knowing what physical device type provided it or what networking technology it  
15 used.

### **Raw Data Types**

Each property in a device definition is tagged with its raw data type. This is the format of the raw data as received from the device and passed up by the gateway. Note that this is usually not the same format as the raw data that is passed from the device to the  
20 gateway.

For Boolean (digital) properties, this raw value is either the string "1" or the string "0." For analog properties, the format of the value can vary widely depending on the type of device. The gateway does not have to be responsible for handling the wide variety of formats possible, since the raw format type is stored in the device type definition, and is used by the  
25 server to make the conversion when necessary.

### **Standard Data Types**

Each property in the device definition file is further tagged with a standard data type. This is the type that is stored in the server database and, by default, reported to the client. (Note that the actual database field type is a string: the "standard type", as used here, refers to  
30 how that string is formatted, not to the database data type).

### **Formatter Conversion Classes**

The server has a set of formatter classes that convert between the raw and standard formats. These are selected and instantiated dynamically, as needed, based on the raw and



standard data type strings from the device definition. This way the server code that manages data is identical for all data types, and supporting a new data type includes creation of a new formatter conversion class. Similarly, there are a set of formatter classes that convert between different standard formats.

5           **Data Conversion Data Flow**

Figure 9 illustrates how the data conversion is handled. Raw data is sent up by the gateway. The server uses the device definition to determine which raw data converter to invoke, calls the converter, and stores the standard data in the database. Later, when the data is read, the server accesses the standard data from the database, optionally reformats it to the client's specifications, then returns the formatted value to the client.

10           **Associative Binding**

Binding is the process of "connecting" the output of one device (a sensor) to another device (actuator). An example is a switch that triggers a light to go on.

15           **Gateway Binding**

First, whether the devices in question use the same technology or not, associative binding uses the gateway itself as the "connection" mechanism. The gateway receives the signals from the sensor, interprets them, and relays the appropriate message to the actuator.

Gateway binding can be implemented without associative binding. That may, however, involve the gateway containing code to do the data conversion from the source device's data format to the destination device's data format. For example, if a switch is bound to a lamp controller, switching the switch to on causes the lamp to turn on.

20           **Associative Binding**

The gateway implements a form of associative binding, where a binding (connection) is triggered by the value of a source device property. Bindings are kept in a table that maps source device properties+values to destination device properties+values. For example, consider a remote control that sends out a numeric value (for example, 1 to 10). Binding entries can map the individual values to different target devices, so that each value can turn on a different lamp. Furthermore, the binding entries contain the specific values that need to be sent to the target device property.

30           Each associative binding defined on the gateway may include:

Index of the source device property

Index of the target device property

Source property value

Destination property value

When a sensor's bound data point reports a change, the gateway checks whether there are any bindings that match that data value. If there are, it sends the appropriate destination data to the destination device property, hence to the destination device hardware.

Figure 10 illustrates a gateway binding mechanism. The steps illustrated in the diagram are:

1. User presses on-1 button, remote sends "prop 2 = 1"
2. Gateway finds "prop2=1" in table, sends "prop 0=8fff" to Device 2 prop 0
3. User presses on-2 button, remote sends "prop 2 = 2"
4. Gateway finds "prop2=2" in table, sends "prop 0=8fff" to Device 3 prop 0
5. User presses off-1 button, remote sends "prop 1 = 1"
6. Gateway finds "prop1=1" in table, sends "prop 0=0000" to Device 2 prop 0

#### **Gateway Data Abstraction**

The source and destination data are specified in the table as untyped strings, so the gateway can do a string comparison, which may not involve knowledge of the data semantics. The gateway passes the destination string back to the destination device, again without necessarily using semantic knowledge.

#### **User Data Abstraction**

In an embodiment of the system, the user knows the semantics of the data, but may not know the raw data formats. So the user knows that "when I press the lamp on button on my remote, I want the lamp to go to full brightness." Because the data from both the sensor and the actuator involved in a binding is normalized to standard data units, the user can specify their desired bindings using those standard data formats, and the system receives these selections. (In the above case, Remote "lamp" button = "On" causes the Lamp to be set to "100%").

#### **Server Data Abstraction**

As in cases where the server handles sensor/actuator data, it does so in the case of bindings using the format conversion classes, driven by the device definition files. The server does not necessarily use semantic knowledge of the values being bound.

#### **Gateway Device Abstraction**

For a given user premises, in addition to the sensor and actuator data, there is system-level data that is managed. Some examples are error logs, usage logs, gateway error alerts, tracking changes to the system, etc. The gateway may be treated as a pseudo device.

In this design, system data are reported as properties belonging to the gateway pseudo device. Because the system properties are exposed this way, they can be transparently handled by the server infrastructure (logging, reporting, etc.) rather than requiring a separate logging/reporting mechanism. This enhances the resiliency of the server design, since new system properties can be added without changing the server code (simply adding the new system variables to the gateway device model suffices).

### **Camera Snapshot: Abstracting Images Through Properties**

The data from cameras (i.e., "camera" function types) is a relatively large binary file. An embodiment of this does not fit the simple property-value model, and in an embodiment the image is not represented by a string. An embodiment handles the cameras and camera properties like other devices where it is appropriate, yet still offers the camera features (still images and video) to the user. An embodiment does that by creating special properties for the camera.

Cameras contain a property named "snapshot" that is linked to the camera's images. This property performs: 1) writing to this property causes the camera to take a snapshot and upload it to the server, and 2) the property is logged when the property changes. The value of the property is the name of the snapshot image. That is used by the server to fetch an image given a name.

### **Taking a Snapshot**

Clients write a string value to the snapshot property that gets sent down to the gateway. That causes the camera code in the gateway to get the snapshot from the camera and upload it to the server. Finally, it reports (to the server) that the property was successfully updated. While the gateway does require special code to handle the camera interface, the device property data is handled exactly like any other device property. Figure 11 illustrates a camera snapshot scenario.

### **Logging Images**

By using a regular property to represent an image snapshot, the times, names, etc. of the snapshots can be logged using the ordinary property logging mechanisms used for other properties. The client software uses this history log to display thumbnails of the saved images. As in the case of the server, the client software does not need special code to get the list of images (although it does use special code to display the thumbnails and images according to an embodiment).

### **Binding Snapshots**

Because a snapshot is triggered by a property assignment, that assignment can also occur due to a binding. Thus combining this snapshot property functionality with the associative binding capability leads to a way to take snapshots based on reported sensor data.

5 Figure 11 illustrates a camera snapshot binding mechanism. The steps depicted are:

1. User presses “take picture” button on remote, remote sends “Device 1 Prop 0 = 1”
2. Gateway finds the binding in the table (Dev 4 Prop 0 = Snap\_#)
3. The # at the end tells the camera code to append a random number
- 10 4. Gateway camera code gets the data update, initiates an HTTP GET to the camera
5. Gateway camera code sends the image to the server
6. Gateway reports updated data like any other data update.

### **15 Camera Integration**

Embodiments of the server and gateway incorporate a number of features that simplify the installation and use of still and video cameras.

#### **Camera Type Abstraction**

As is the case for attached devices, cameras are abstracted on the gateway so that  
20 neither the client nor the server infrastructure necessarily has specific knowledge of the camera type, thus they may handle all cameras identically according to an embodiment. (Note: the client application—in our case the portal—may use some specific camera knowledge in order to present the video and stills transparently to the user).

#### **Integrated Stills and Video**

25 The camera stills and video are integrated into the user interface so that the user never sees any camera-specific web pages. Figure 12 illustrates a camera environment.

#### **Firewall-Proof Still Images**

According to an embodiment, the images from the IP-attached cameras supported are  
30 not viewed from beyond the user’s own local network unless the user’s router opens a port and forwards the camera requests to the camera. However, since the gateway is behind the same firewall as the camera, it gets the image from the camera and transfers it to the server via HTTP port 80 (which is always open). The images thus become available to the user on the Internet (protected by username/password).

### **Integrated Video Dynamic DNS Replacement**

Viewing video from the camera involves the client changing router settings to forward TCP requests to their camera. Then, the portal allows the client to access the video without the client necessarily knowing the Internet address of the client's system. The gateway is in regular communication with the server, and upon update the server saves the gateway's current WAN address. When the client wants to see video from the client's camera, the server inserts the gateway's WAN address into the video image link (href). If the user's IP address changes frequently, the user can access their camera's video from anywhere.

### **Installation**

Network cameras on the market come with a variety of installation methods. An embodiment of the gateway eliminates the need for client involvement by automatically configuring the camera hardware.

During the camera configuration, the gateway creates private administrator password, then a view-only user with a random password that is subsequently used to get camera images (still or video). The gateway searches for the camera on the local network to obtain its IP address (as assigned by the user's router). Since the gateway itself is automatically configured via DHCP, it knows the subnet and approximate address range that the router is using for the DHCP-assigned addresses.

### **Configuration**

According to an embodiment, the camera configuration capability is exposed via camera configuration properties. Should the user want to change the camera's address or client user name/password, the user can do so in one place, on the system portal. The changes are passed down to the gateway (as camera configuration property updates) where it causes the gateway to reconfigure the camera hardware. Differences between different camera types are handled by the gateway software. These properties are handled and logged as other properties.

### **Router Port Forwarding Assistance**

Setting a router's port forwarding table to support remote video viewing may involve:

1. Determine that port forwarding is called for
2. Find the router's configuration web page
3. Figure out what to enter as the server address
4. Figure out what to enter as the server port
5. Know what to put where

6. Know if it is working correctly

An embodiment of the system addresses these items. Note that the user is logged on from the user's own network (the "Local Client" example in Figure 12) to configure the user's router.

5 **Determining Port Forwarding Is Desired**

When the user accesses a camera from the system portal, the system server performs a test to check whether the camera is accessible from the Internet. If it is, the camera page includes a link to a page that will display the video. If the camera is not accessible, the video link instead opens a camera assistance page that guides the user through steps to configure their router's port forwarding.

10 **Finding the Router's Web Page**

Since the gateway is on the same internal network as the camera, it knows what the router's address is (it is the default gateway passed back in the DHCP assignment). The portal generates a link on the camera assistance page that takes the user right to the user's router's configuration web page.

**Address, Port and Where to Put Them**

Since the camera's address and port are available via properties, the portal reads these properties and includes these properties in descriptive text on the camera assistance page. That page also contains a link to a router help page, where the user can select the user's router and get specific help on what to do to configure it.

**Device Test**

The camera assistance page has a button to test whether the port forwarding is a success or not. It uses the server's test-camera-access API to make the determination, and displays either a pass or fail message to let the user know.

**Various Embodiments**

In addition to the foregoing, the following are various examples of embodiments of the invention.

Some embodiments of a method for premises management networking include monitoring premises management devices connected to a gateway at a premises; controlling premises management devices connected to the gateway at the premises; receiving, at the premises, an uplink-initiation signal associated with a network operations center server; and in response to the uplink-initiation signal, initiating, from the gateway at the premises, communications between the gateway and the network operations center server; and

communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices.

The uplink-initiation signal can be received via telephone and/or broadband connection. The gateway can initiate communications between the gateway and the network operations center server with at least an HTTP message and/or at least an XML message. The premises management devices can manage energy of the premises, security of the premises, and/or safety of the premises. Many embodiments provide a hosted solution for property developers, owners and managers as well as service providers (ISPs, telcos, utilities, etc.) such as communication service providers and Internet portal providers. Some embodiments offer a complete, turnkey, reliable, and/or cost-effective solution for the delivery of telemetry services (e.g., energy management, security, safety, access, health monitoring, messaging, etc.) to customers.

An embodiment of the invention is directed to a business method for premises management. Some embodiments of a business method for premises management include making an Internet portal available for access to a vendee, such as a premises vendee, communication service vendee, and/or an Internet portal vendee; and at least after a transaction between the vendor and the vendee, such as a premises transaction, a communication services transaction, and/or Internet portal services transaction, providing premises management services via the Internet portal to the vendee.

The Internet portal can be branded with a brand of the vendor according to an embodiment. Examples of a premises vendor include a home builder, premises builder, and premises manager. Examples of a premises vendee include a home buyer, premises buyer, and premises tenant. Examples of a communication service vendor include an Internet service provider, a telephone company, a satellite television company, and a cable television company. Examples of a communication service vendee include a customer of the Internet service provider, a customer of the telephone company, a customer of the satellite television company, and a customer of the cable television company. Premises management services can manage energy of the premises, security of the premises, and/or safety of the premises.

An embodiment of the invention is directed to a system. The system includes a network of premises management devices, a gateway coupled to the network and premises management devices, a server coupled to the gateway by a communication medium and a portal coupled to the communications medium. The portal provides communication with the premises management devices.

According to various embodiments in the invention alone or in various combinations: the communications medium may comprise the Internet; the portal may comprise an internet portal; and/or the portal may be branded with the name of a vendor of a product associated with the premises. The product may comprise a building, and/or the vendor may comprise a party that leases the premises. The vendor may also or alternatively comprise a property management organization. The server may be included within a network operations center. The logic may comprise, according to various embodiments of the invention, software, hardware, or a combination of software and hardware.

Another embodiment to the invention is directed to a gateway. The gateway includes an interface coupled to a network of premises management devices, logic that receives data from different premises management devices, and an interface coupled to a communications medium that is coupled to a server. The server is coupled to a portal coupled to the communications medium. The portal provides communications with the premises management devices.

According to various embodiments of the invention alone or in various combinations: the communications medium may comprise the Internet; the portal may comprise an internet portal; and/or the portal may be branded with the name of a vendor of a product associated with the premises. The product may comprise a building; the vendor may comprise a party that leases the premises; the vendor may comprise a property management organization; and/or the server may be included within a network operations center.

Another embodiment of the invention is directed to premises management system. The premises management system includes a network of premises management devices and a gateway coupled to the network of premises management devices. The gateway includes logic that receives data from different premises management devices and an interface coupled to a communications medium that is coupled to a server. The server is coupled to a portal coupled to the communications medium, and the portal provides communication with the premises management devices. The logic may comprise, according to various embodiments of the invention, software, hardware, or a combination of software and hardware.

Another embodiment of the invention is directed to a system that includes: a network of premises management devices; a gateway coupled to the network of premises management devices; a server coupled to the gateway by a communications medium and a portal coupled to the communications medium, the portal providing communication with the premises management devices.



According to various embodiments in the invention, alone, or in various combinations: the common format includes a set of properties for each type of device; the format includes an index for each device and an index for each property of each device; the network comprises a network operations center; the network of premises management devices includes at least a camera; the system includes logic that reinterprets abstracted data in the common format from the different premises management devices; the server includes a device definition file for reinterpreting the abstracted data; the system includes a set of standard function types that define standard properties; the standard properties include temperature; the system includes client software that queries measurements corresponding to the respective property without specifying the type of device from which the measurement is to be received; the server includes a set of formatter classes that convert between the format of data in which data is passed from the gateway to the server in a type in which the data is stored in the server; the formatter classes are instantiated dynamically; the system includes device definitions for respective premises management devices; and/or the server is included within a network operations center.

An embodiment of the invention is directed to a gateway that includes: an interface coupled to a network of premises management devices; logic that abstracts data from different premises management devices using a common format; and an interface coupled to a communications medium that is coupled to a server. The server is coupled to a portal coupled to the communications medium, and the portal provides communication with the premises management devices. The gateway may include logic to interact with various aspects of the various systems described herein.

Another embodiment in the invention is directed to a gateway that includes: an interface coupled to a network of premises management devices, the network including at least a first device comprising a source of data and at least a second device comprising a recipient of the data; logic that abstracts data from different premises management devices using a common format; logic that maps data from a first device least comprising the source of data to data on a second device comprising the recipient of the data; and an interface coupled to a communications medium that is coupled to a server, wherein the server is coupled to a portal coupled to the communications medium, the portal providing communication with the premises management devices.

According to various embodiments of the invention, in various combinations or alternatively: the mapping is based on a property of the first device and a corresponding property of the second device; the mapping is stored in a table in the server; the mapping is

based on a correspondence between an index of a property of the first device with an index of a property of the second device; gateway includes logic that checks whether there are any corresponding properties on a corresponding device that comprises a recipient of data if corresponding data from a device that comprises a source of the corresponding data changes; and/or the logic comprises hardware, software, or a combination of hardware and software.

Another embodiment of the invention is directed to a system that includes: a set of one or more premises management devices, the set of one or more premises management devices including at least a camera; a gateway coupled to the set of one or more network of premises management devices, the gateway including logic that abstracts data from a premises management device using a common format, general to different devices; a server coupled to the gateway by a communications medium; and a portal coupled to the communications medium, the portal providing communication with at least a device in the set of one or more premises management devices.

According to various embodiments of the invention, alternatively, or in various combinations: the system includes logic that transmits data from the gateway to the server using HTTP protocol; the data from the gateway includes an image from the camera; the gateway includes logic that pushes data to the server from the set of one or more premises management devices; the system includes logic that causes an image from the camera served from the server to be displayed; the system includes logic that causes an image from the camera to be transmitted from the gateway to the server in response to an uplink-initiation signal; the uplink communication signal is received via telephone; the uplink communication signal is received via telephone without requiring answering of a telephone call; the uplink communication signal is received via broadband connection; at least a device in the set of one or more network of premises management devices manages energy of the premises; at least a device in the set of one or more network of premises management devices manages security of the premises; at least a device in the set of one or more network of premises management devices manages safety of the premises; the camera includes at least a property specific to a camera and at least a property common with at least another type of device; the property specific to a camera causes the camera to take a picture; the property specific to a camera causes a picture taken by the camera to be uploaded to the server; the system includes logic that causes a picture to be taken based on the state of another device in the set of one or more premises management devices; another device in the set comprises a motion sensor; the system includes the plurality of different types of cameras and wherein the gateway includes logic that abstracts data from the different types of cameras into a common format for

delivery to the server; the system includes a router that couples the gateway to the communications medium; the camera comprises an internet protocol (IP) camera; and images from the camera are provided over the communications medium only if the gateway initiates a transfer of the image to the server.

5           Another embodiment of the invention is directed to a system that includes: a set of one or more premises management devices, the set of one or more premises management devices including at least a camera; a gateway coupled to the set of one or more network of premises management devices; a server coupled to the gateway by a communications medium, and a portal coupled to the communications medium, the portal providing  
10 communication with at least a device in the set of one or more premises management devices. The gateway includes logic that pushes data from the set of one or more premises management devices to the server.

          According to various embodiments of the invention, alternatively, or in various combinations: the gateway does not allow direct access to the set of one or more premises  
15 management devices from the communications medium; the system includes logic that causes an image from the camera to be transmitted from the gateway to the server in response to an uplink-initiation signal; the uplink communication signal is received via telephone; the uplink communication signal is received via telephone without requiring answering of a telephone call; the uplink communication signal is received via broadband connection; at  
20 least a device in the set of one or more network of premises management devices manages security of the premises; the camera includes at least a property specific to a camera and at least a property common with at least another type of device; the property specific to a camera causes the camera to take a picture; the system includes logic that causes a picture to be taken based on the state of another device in the set of one or more premises management  
25 devices; the system includes a plurality of different types of cameras and the gateway includes logic that abstracts data from the different types of cameras into a common format for delivery to the server; and/or the camera comprises an internet protocol (IP) camera.

          Another embodiment of the invention is directed to a gateway that includes: an interface coupled to a set of one or more premises management devices, the set of one or  
30 more premises management devices including at least a camera; and an interface coupled to a communications medium that is coupled to a server, wherein the server is coupled to a portal coupled to the communications medium, the portal providing communication with the premises management devices; and logic that pushes data from one or more premises management devices to the server.

Components of the gateway, server, system and/or other aspects described above include any collection of computing components and devices operating together.

Components of these items can also be components of subsystems or within a larger computer system or network. The components can also be coupled among any number of components (not shown), for example other buses, controllers, memory devices and data input/output (IO) devices in any number of combinations. Further common components of these items can be distributed among various numbers or combinations of other processor-based components according to various embodiments of the invention.

Aspects of the gateway, server, system and other items described here and may be implemented as functionality programmed into any variety of circuitry, including programmable logic devices, (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for implementing aspects these items include:

microcontrollers with memory (such as electronically erasable programmable read only memory (EEPROM)), embedded microprocessors, firmware, software, etc. Furthermore, aspects of the gateway, server and other elements may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

The various functions or processes disclosed herein may be described as data and/or instructions embodied in various computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such formatted data and/or instructions by carrier waves include, but are not limited to, transfers (uploads, downloads, e-mail, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g.,

HTTP, FTP, SMTP, etc.). When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of components and/or processes under the ICS may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs.

Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of "including, but not limited to." Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words "herein," "hereunder," "above," "below," and words of similar import refer to this application as a whole and not to any particular portions of this application. When the word "or" is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

The above description of illustrated embodiments of the system is not intended to be exhaustive or to limit the system to the precise form disclosed. While specific embodiments of, and examples for, the system are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the system, as those skilled in the relevant art will recognize. The teachings of the system provided herein can be applied to other processing systems and methods, not only for the systems and methods described above.

The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the system in light of the above detailed description.

In general, in the following claims, the terms used should not be construed to limit the system to the specific embodiments disclosed in the specification and the claims, but should be construed to include all processing systems that operate under the claims. Accordingly, the system is not limited by the disclosure, but instead the scope of the system is to be determined entirely by the claims.

While certain aspects of the system are presented below in certain claim forms, the inventors contemplate the various aspects of the system in any number of claim forms. For example, while only one aspect of the system is recited as embodied in machine-readable medium, other aspects may likewise be embodied in machine-readable medium.

Accordingly, the inventors reserve the right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the system.

## CLAIMS

## WHAT IS CLAIMED IS:

1. A method for premises management networking, comprising:  
monitoring premises management devices connected to a gateway at a premises;  
5 controlling premises management devices connected to the gateway at the premises;  
receiving, at the premises, an uplink-initiation signal associated with a network  
operations center server;  
in response to the uplink-initiation signal, initiating, from the gateway at the premises,  
communications between the gateway and the network operations center server; and  
10 communicating, during the communications between the gateway and the network  
operations center server, information associated with the premises management devices.
2. The method of claim 1, wherein the uplink-initiation signal is received via telephone.
3. The method of claim 1, wherein the uplink-initiation signal is received via broadband  
connection.
- 15 4. The method of claim 1, wherein the gateway initiates communications between the  
gateway and the network operations center server with at least an HTTP message.
5. The method of claim 1, wherein the gateway initiates communications between the  
gateway and the network operations center server with at least an XML message.
6. The method of claim 1, wherein the premises management devices manage energy of  
20 the premises.
7. The method of claim 1, wherein the premises management devices manage security of  
the premises.
8. The method of claim 1, wherein the premises management devices manage safety of  
the premises.
- 25 9. A business method for premises management, comprising:  
making an Internet portal available for access to a premises vendee; and  
at least after a transaction for a premises between a premises vendor and the premises  
vendee, providing premises management services via the Internet portal to the premises  
vendee.

10. The business method of claim 9, further comprising:  
branding the Internet portal with a brand of the premises vendor.
11. The business method of claim 9, wherein the premises vendor is a home builder.
- 5 12. The business method of claim 9, wherein the premises vendee is a home buyer.
13. The business method of claim 9, wherein the premises vendor is a premises builder.
14. The business method of claim 9, wherein the premises vendee is a premises  
10 buyer.
15. The business method of claim 9, wherein the premises vendor is a premises manager.
16. The business method of claim 9, wherein the premises vendee is a premises tenant.
- 15 17. The business method of claim 9, wherein the premises management services manage energy of the premises.
18. The business method of claim 9, wherein the premises management services manage security of the premises.
19. The business method of claim 9, wherein the premises management services  
20 manage safety of the premises.
20. A business method for premises management, comprising:  
making an Internet portal available for access to a communication service vendee; and  
at least after a transaction for communication services to a premises between a  
communication service vendor and the communication service vendee, providing premises  
25 management services via the Internet portal to the communication service vendee.
21. The business method of claim 20, further comprising:  
branding the Internet portal with a brand of the communication service vendor.



22. The business method of claim 20, wherein the communication service vendor is an Internet service provider.
23. The business method of claim 20, wherein the communication service vendee is a customer of the Internet service provider.
- 5 24. The business method of claim 20, wherein the communication service vendor is a telephone company.
25. The business method of claim 20, wherein the communication service vendee is a customer of the telephone company.
26. The business method of claim 20, wherein the communication service vendor  
10 is a satellite television company.
27. The business method of claim 20, wherein the communication service vendee is a customer of the satellite television company.
28. The business method of claim 20, wherein the communication service vendor is a cable television company.
- 15 29. The business method of claim 20, wherein the communication service vendee is a customer of the cable television company.
30. The business method of claim 20, wherein the premises management services manage energy of the premises.
31. The business method of claim 20, wherein the premises management services  
20 manage security of the premises.
32. The business method of claim 20, wherein the premises management services manage safety of the premises.
33. A business method for premises management, comprising:  
making an Internet portal available for access to an Internet portal vendee; and  
25 at least after a transaction for Internet portal services to a premises between an Internet portal vendor and the Internet portal vendee, providing premises management services via the Internet portal to the Internet portal vendee.

34. The business method of claim 33, further comprising:  
branding the Internet portal with a brand of the Internet portal vendor.
35. The business method of claim 33, wherein the premises management services manage energy of the premises.
- 5 36. The business method of claim 33, wherein the premises management services manage security of the premises.
37. The business method of claim 33, wherein the premises management services manage safety of the premises.

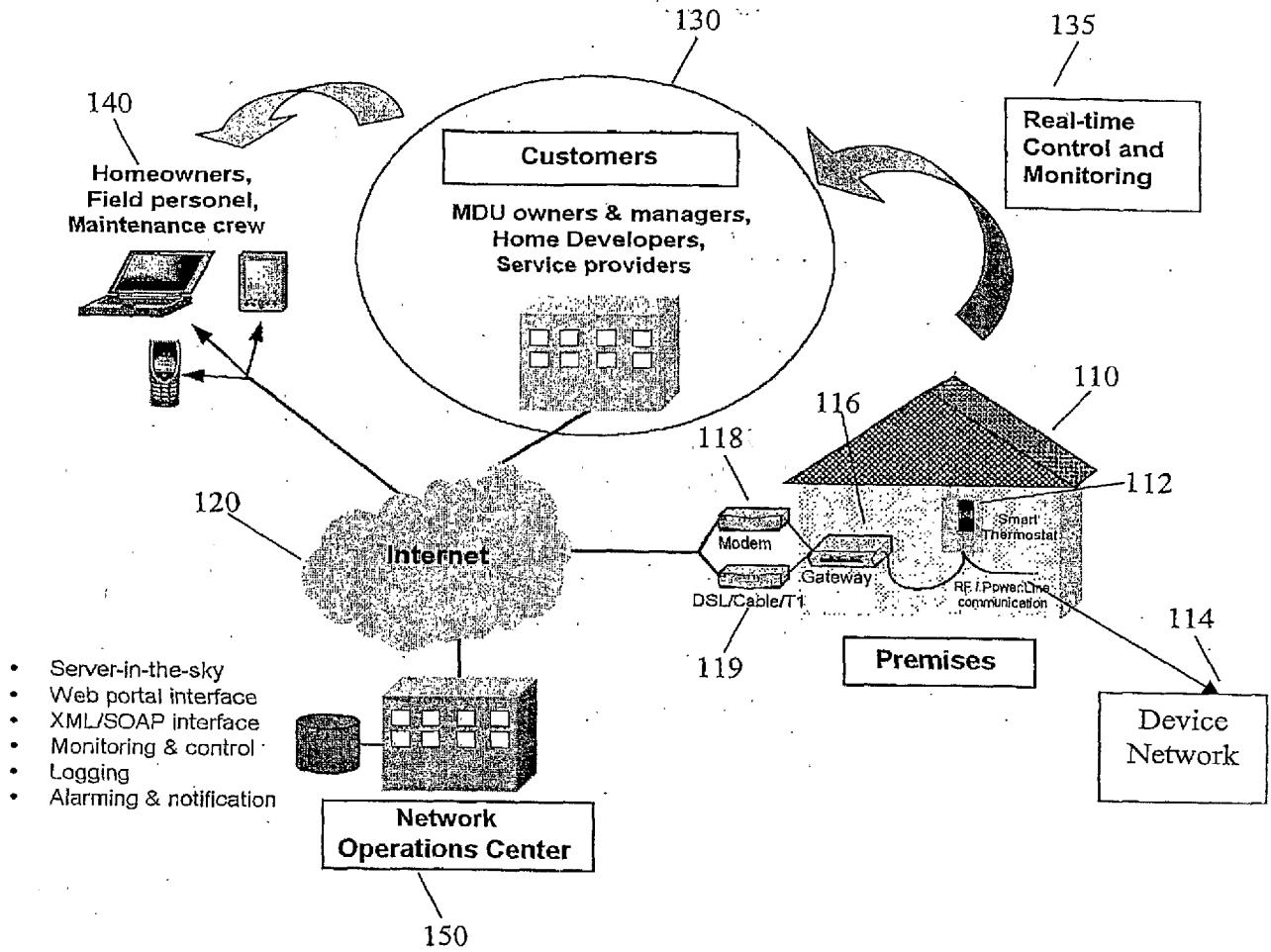


FIGURE 1

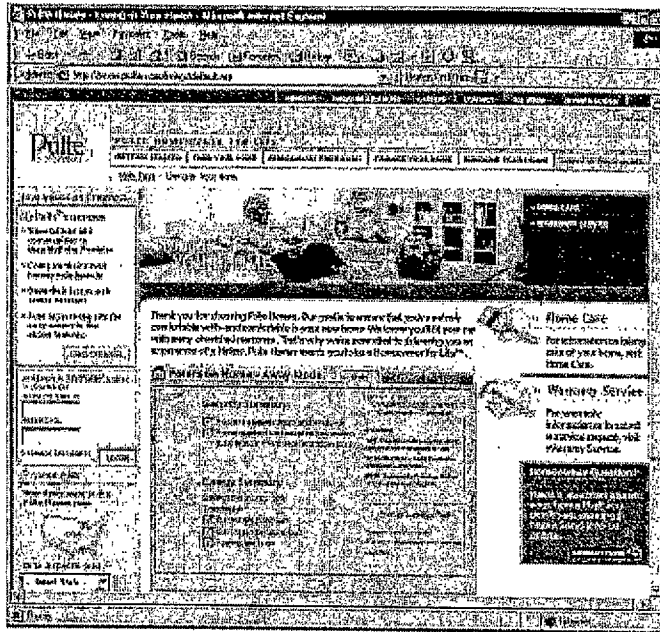


FIGURE 2

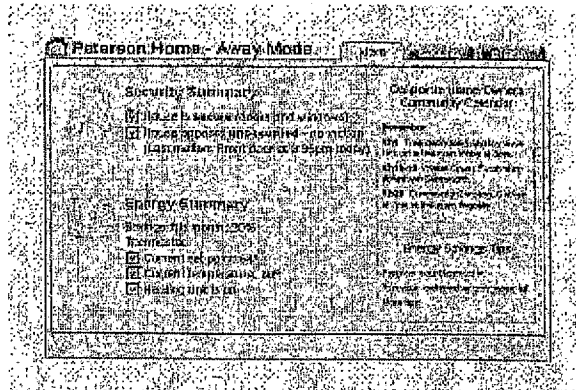


FIGURE 3A

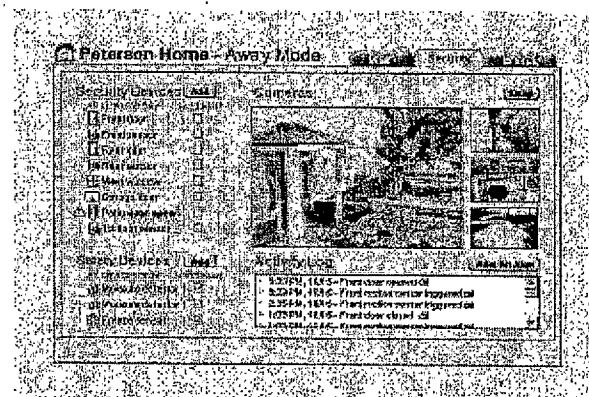


FIGURE 3B

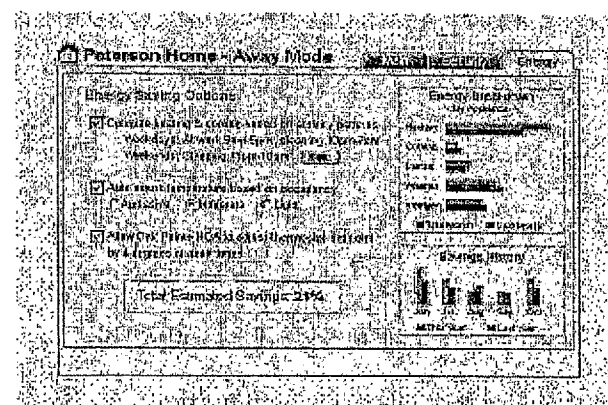


FIGURE 3C

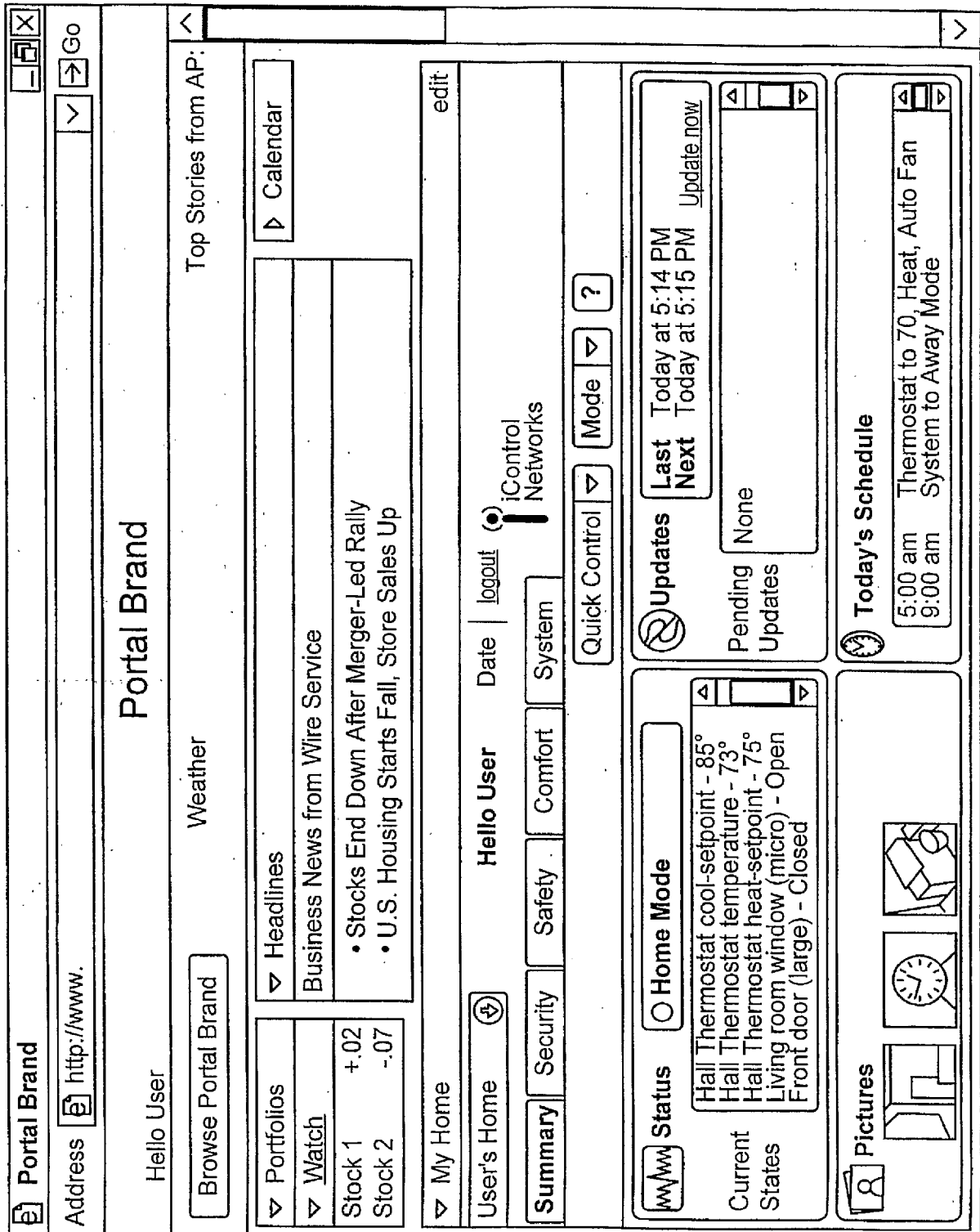


Figure 3D

**Summary** | **Address** http://www. | **Go**

**System** | **User Name** | **Date** | **Sign Out**

**Summary** | **Details** | **Notification** | **Automation** | **Schedules** | **System** | **System Company Name**

**Quick Control** | **Mode** | **Mode** | **?** | **?**

**Status** | **Away Mode**

Hall motion sensor - Empty  
 Thermostat temperature - 72°  
 Floor lamp - Off  
 Mail Box door - Closed  
 Front door (recessed) - Closed

**Current States**

**Updates**

Last Today at 3:59 PM  
 Next Today at 4:00 PM

Pending Updates

None

**Pictures**

Time 1 Date 1

Time 2 Date 2

Time 3 Date 3

**Today's Schedule**

5:00 am Thermostat to 70, Heat, Auto Fan  
 9:00 am System to Away Mode  
 9:15 am Turn Foyer Lights Off  
 7:30 pm Turn Sidewalk Lights Off

**Alarm History**

Past 7 Days

△ Hall motion sensor 2:45p 3/4  
 △ Hall motion sensor 2:11p 3/4  
 △ Hall motion sensor 12:49p 3/4  
 △ Hall motion sensor 12:16p 3/4

**Reminders**

12/31 Change Furnace Filter (yearly) OK  
 2/15 Update Sprinkler Schedule (seasonal) OK  
 3/1 Clean Gutters (Spring) OK

Figure 3E

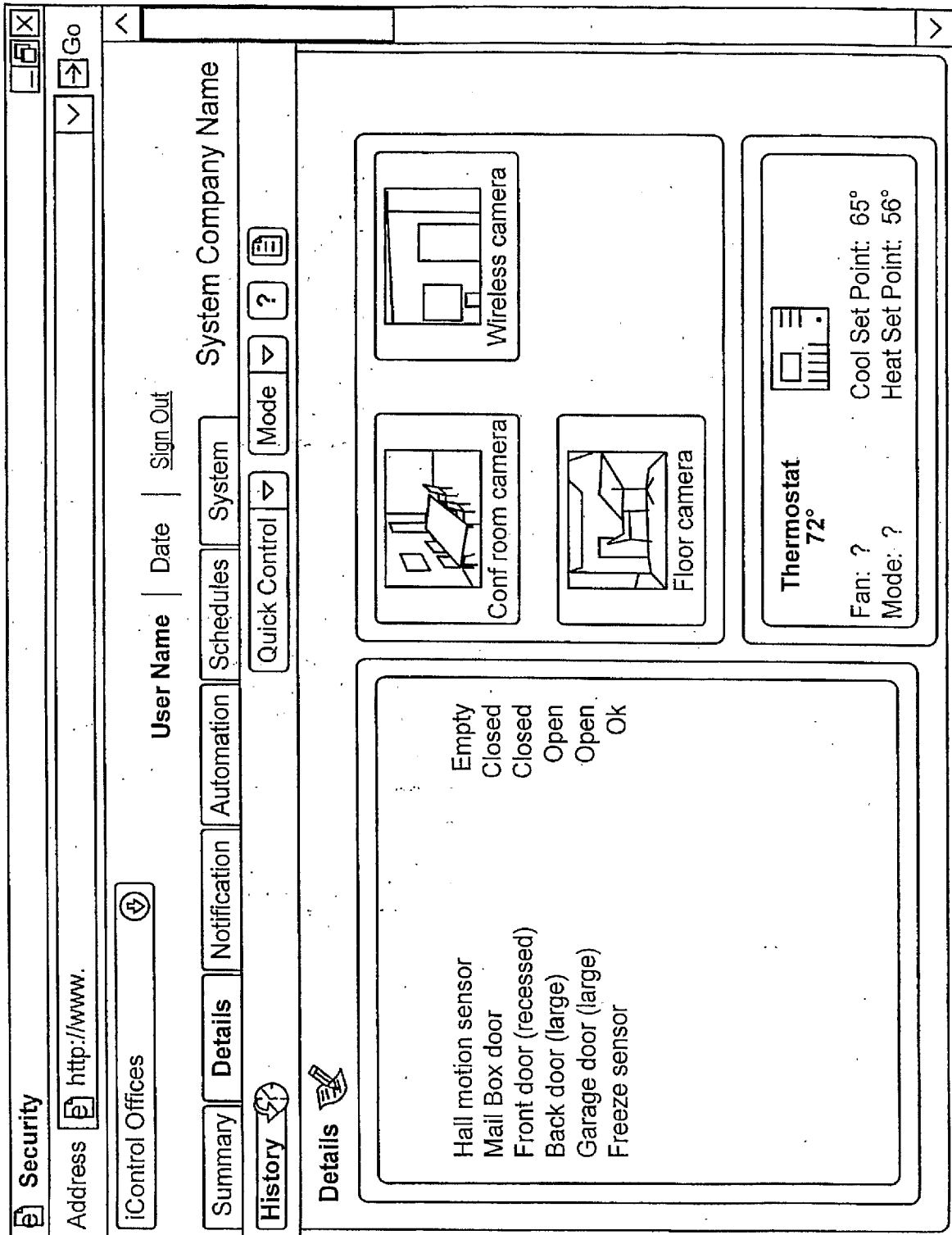


Figure 3F



**Automation**

Address <http://www>

**iControl Offices**

User Name | Date | [Sign Out](#)

Summary | Details | Notification | Automation | Schedules | System | System Company Name

Quick Control Mode ?

	Home	Sleep	Away
Back door (large)	Open	None	None
Back door (large)	Closed	None	None
Hall motion sensor	Occupied	None	Conf room camera Picture...
Hall motion sensor	Empty	None	None
Front door (recessed)	Open	None	None
Front door (recessed)	Closed	None	None
Mail Box door	Open	None	None
Mail Box door	Closed	None	None
Garage door (large)	Open	None	None
Garage door (large)	Closed	None	None

**Remote controls operate the same in all modes**

- Keychain remote Lamp button on
- Keychain remote Lamp button off
- Keychain remote Star button
- Keychain remote Lock button
- Keychain remote Unlock button
- Floor lamp Level...
- Floor lamp Level...
- Wireless camera Picture...
- Change Mode mode...
- Change Mode mode...

Figure 3G

System
Go

Address

iControl Offices
Date
Sign Out

System Company Name

Summary
Details
Notification
Automation
Schedules
System
Quick Control
Mode
?
?

History
Admin

**System**  
Add Device

Name	Last Update	Device
Gateway	Today at 4:01 PM	iControl Networks: Beta Gateway
Back door (large)	Today at 3:13 PM	GE Security: 60-670-95R Door/Window Switch
Freeze sensor	Today at 3:30 PM	GE Security: 60-742-95R Freeze Sensor
Conf room camera	Today at 3:51 PM	Axis Communications: 205
Floor camera	Today at 3:55 PM	Axis Communications: 205
Hall motion sensor	Today at 3:11 PM	GE Security: 60-639-95R Passive Infrared Motoin Detector
Thermostst	Today at 4:00 PM	GE Security: 60-909-95 Thermostat
Front door (recessed)	Today at 3:47 PM	GE Security: 60-741-95 Recessed Door/Window Switch
Keychain remote	3/2 5:14 PM	GE Security: 4 Button Remote 60-659-95R
Mail Box door	Today at 3:33 PM	GE Security: 60-688-95 Micro Door/Window Switch
Floor lamp	Today at 4:01 PM	Axsys Automation: Lamp Module
Wireless camera	Today at 3:51 PM	Axis Communications: 205
Garage door (large)	Today at 3:06 PM	GE Security: 60-670-95R Door/Window Switch

Figure 3H

9 / 17

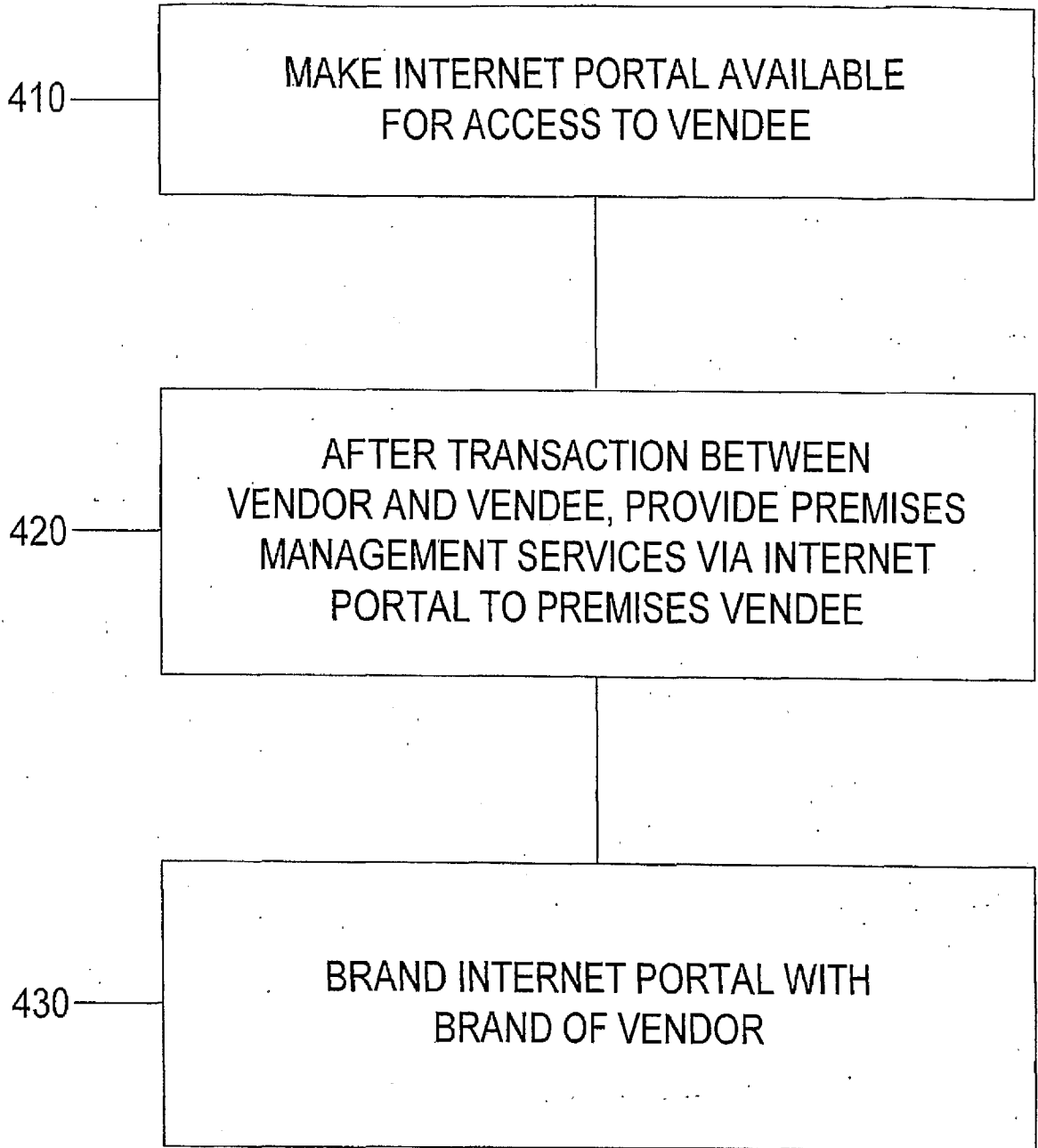


FIGURE 4

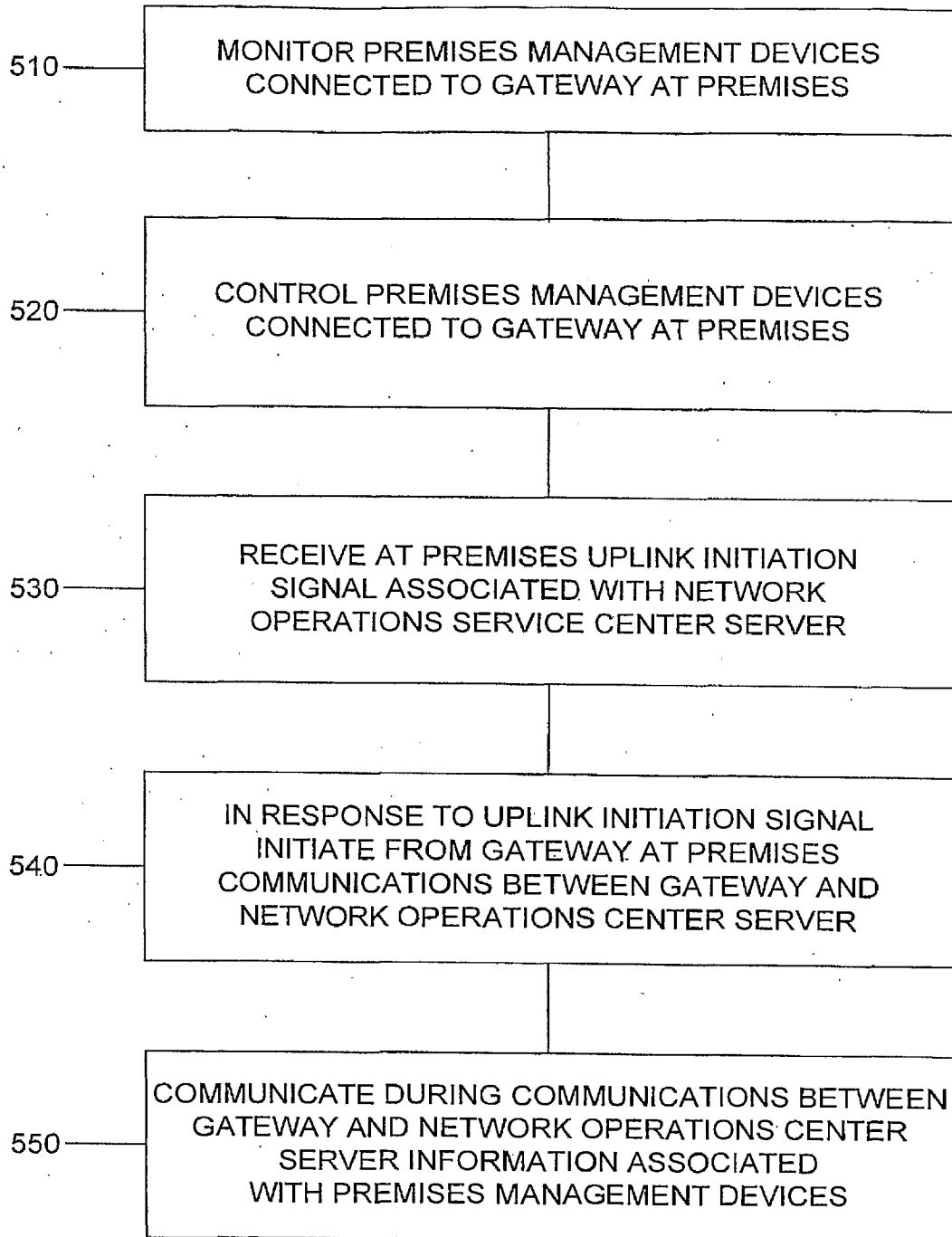


FIGURE 5

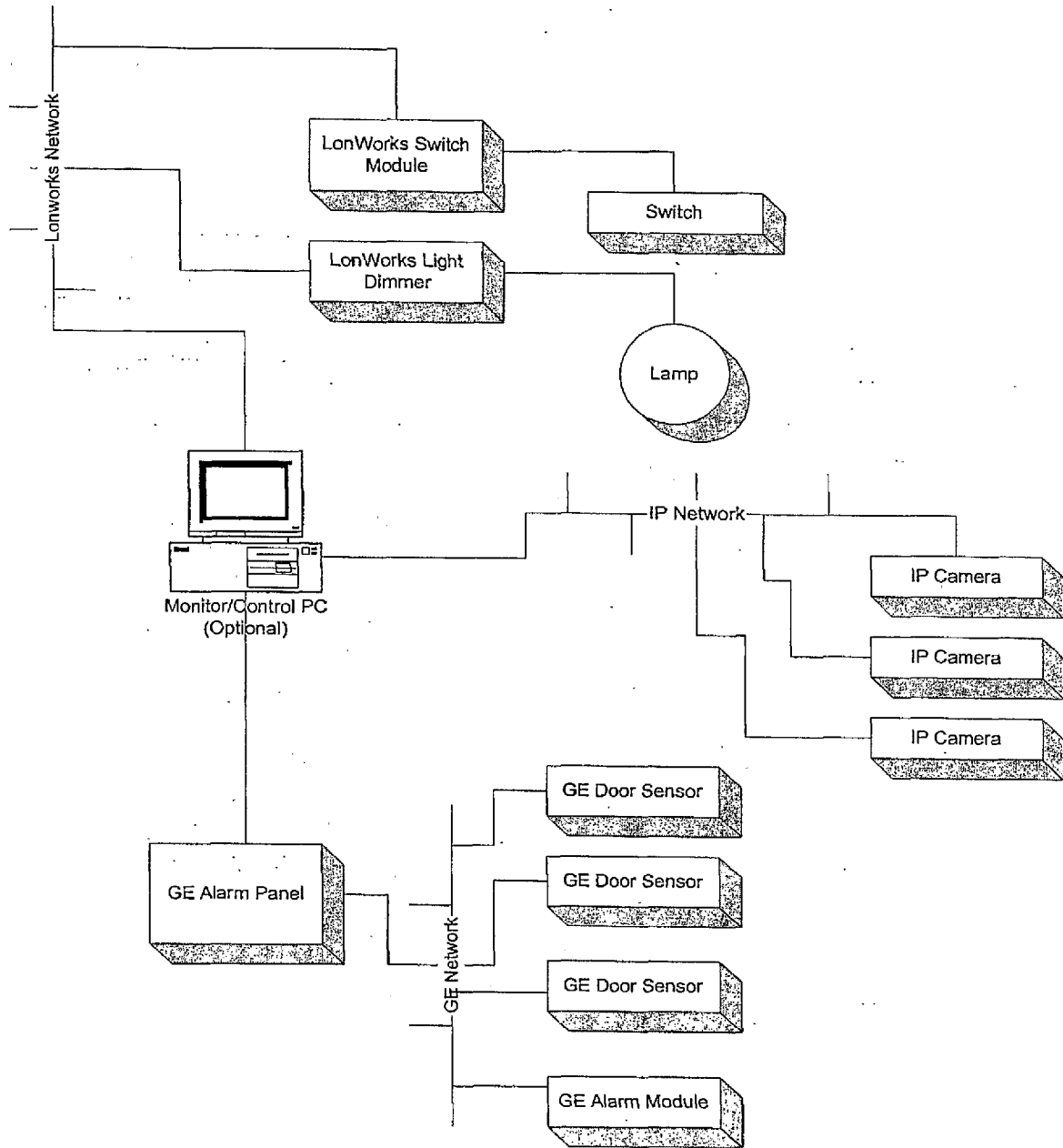


Figure 6

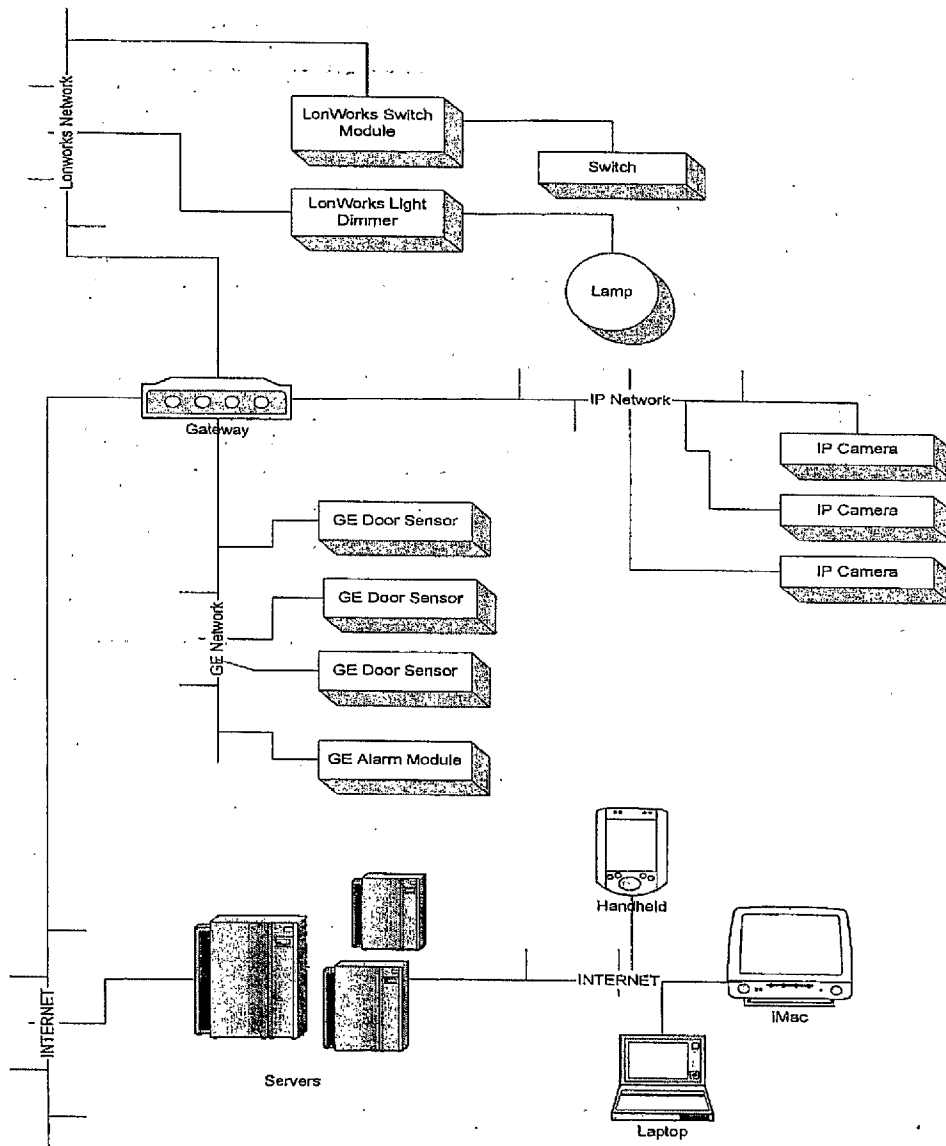


Figure 7 - System Architecture

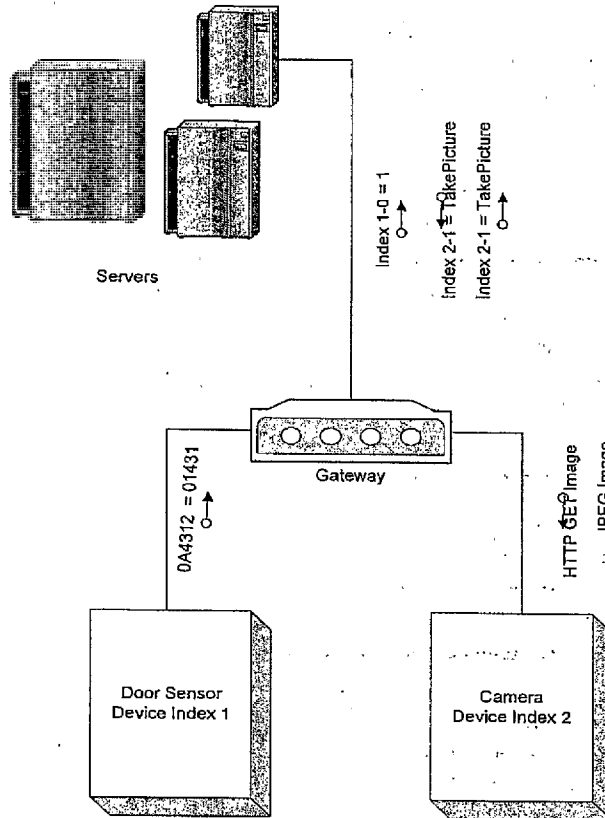


Figure 8 - Gateway Data Handling

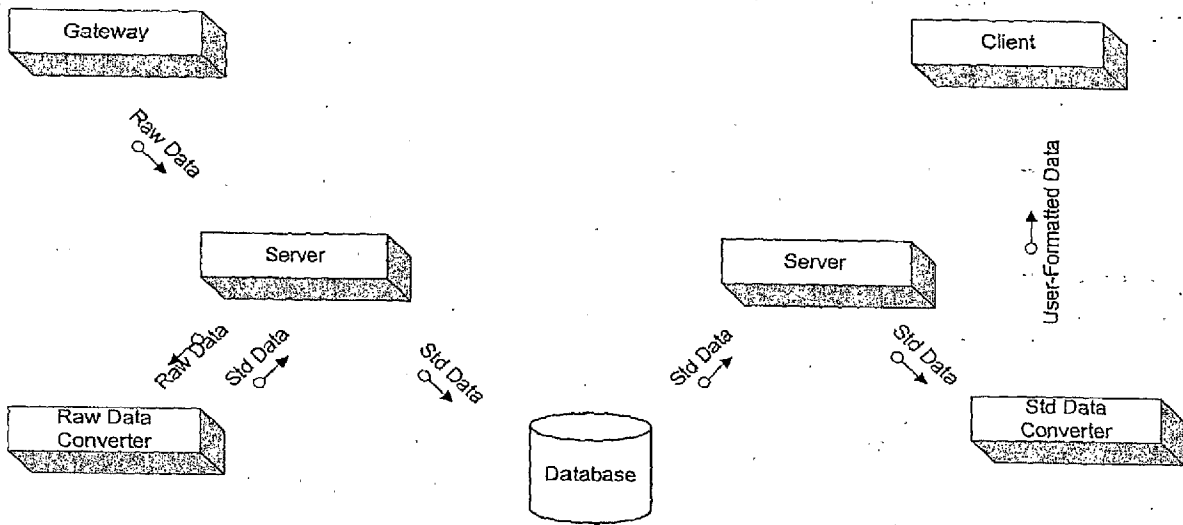


Figure 9 - Data Conversion



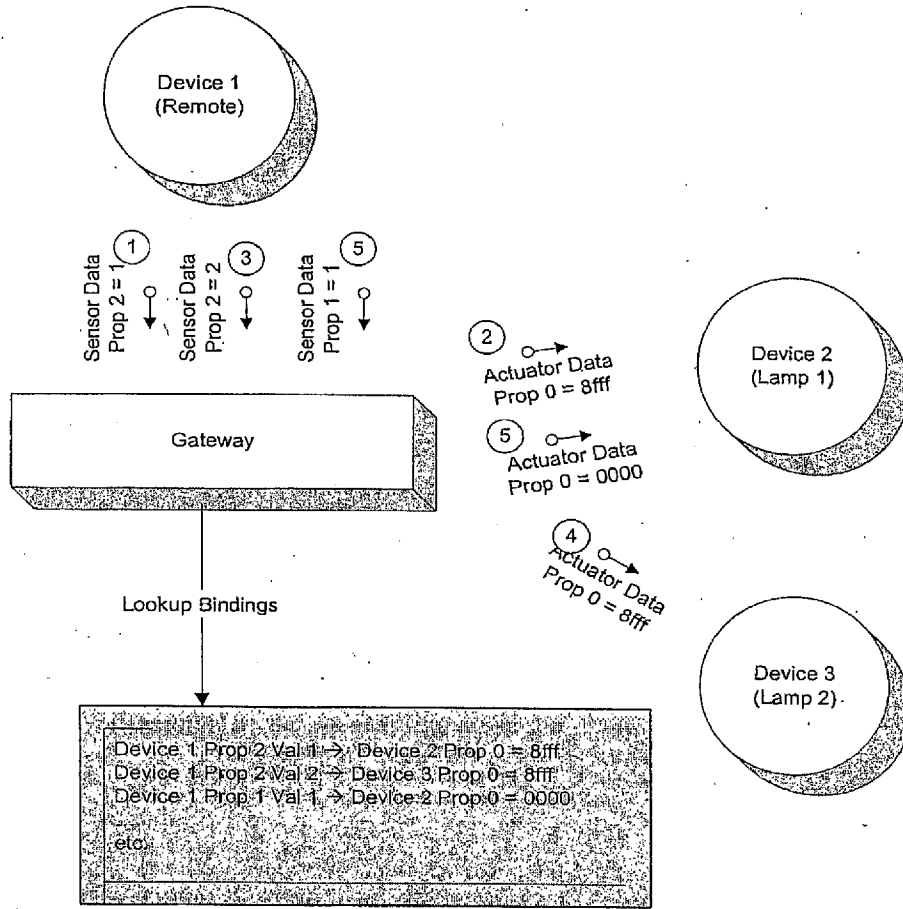


Figure 10 - Binding Data Flow

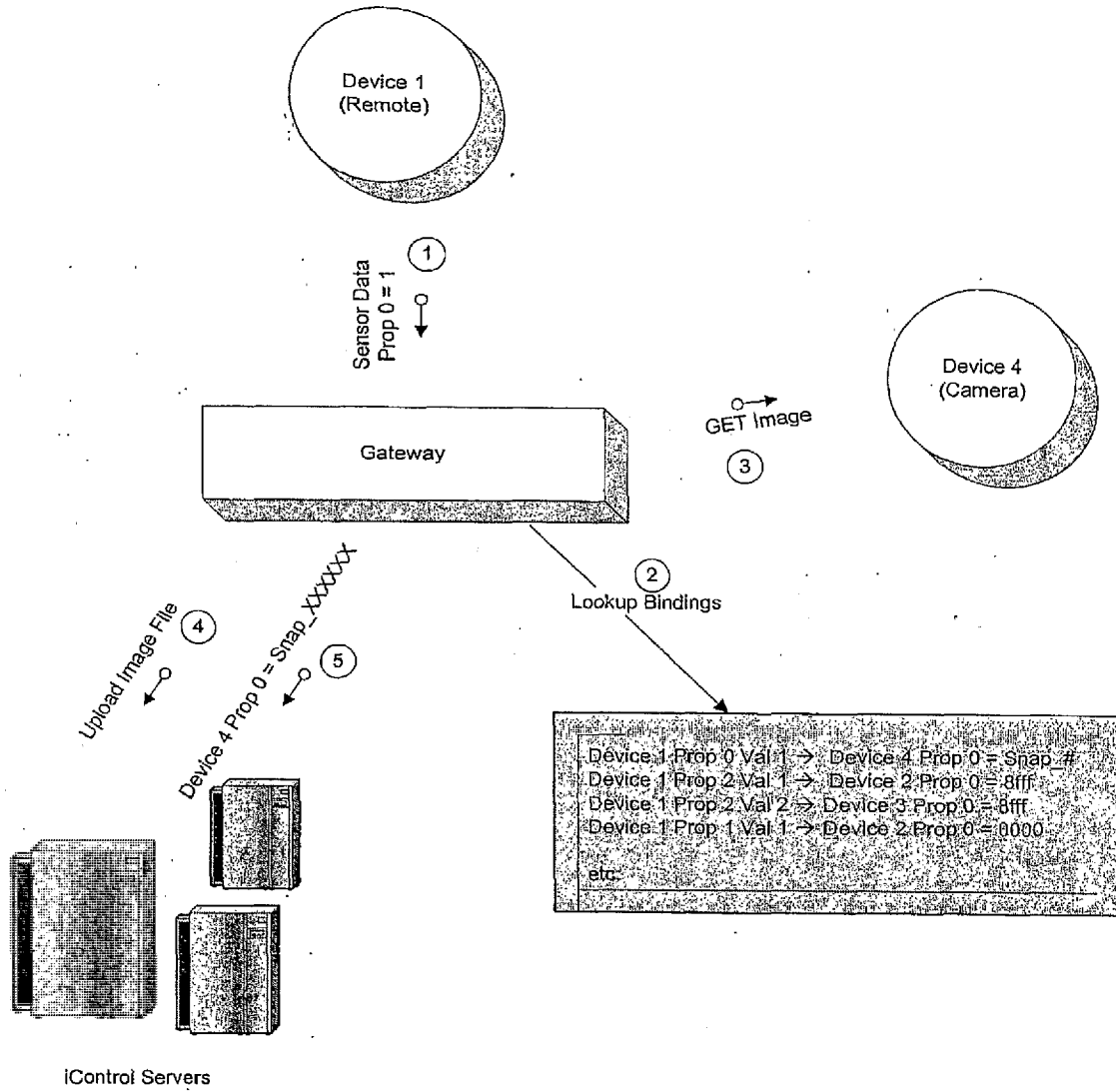


Figure 11

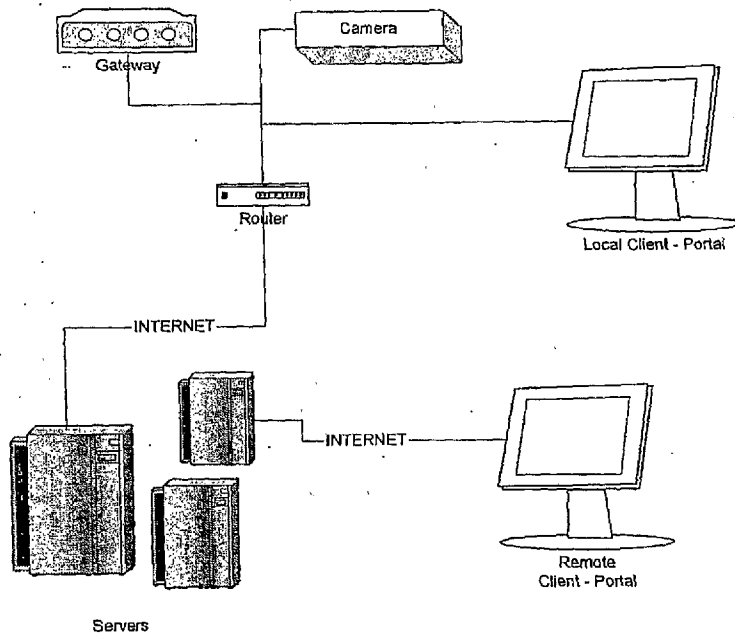


Figure 12 - Camera Image/Video Architecture

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
29 September 2005 (29.09.2005)

PCT

(10) International Publication Number  
**WO 2005/091218 A3**

(51) International Patent Classification:  
H04L 12/56 (2006.01)

(21) International Application Number:  
PCT/US2005/008766

(22) International Filing Date: 16 March 2005 (16.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/553,934 16 March 2004 (16.03.2004) US  
60/553,932 16 March 2004 (16.03.2004) US  
60/652,475 11 February 2005 (11.02.2005) US

(71) Applicant (for all designated States except US): **ICON-TROL NETWORKS, INC** [US/US]; 502 Waverly Street, Suite 302, Palo Alto, CA 94301 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **RAJI, Reza** [US/US]; 1921 Oakdell Drive, Menlo Park, CA 94025 (US). **GUTT, Gerald** [US/US]; 11693 Tortoise Trail, Tucson, AZ 85743 (US). **STEVENS, Chris** [US/US]; 730 Bryant Street, Palo Alto, CA 94301 (US).

(74) Agents: **WILLMAN, George, A.** et al.; Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94306-1050 (US).

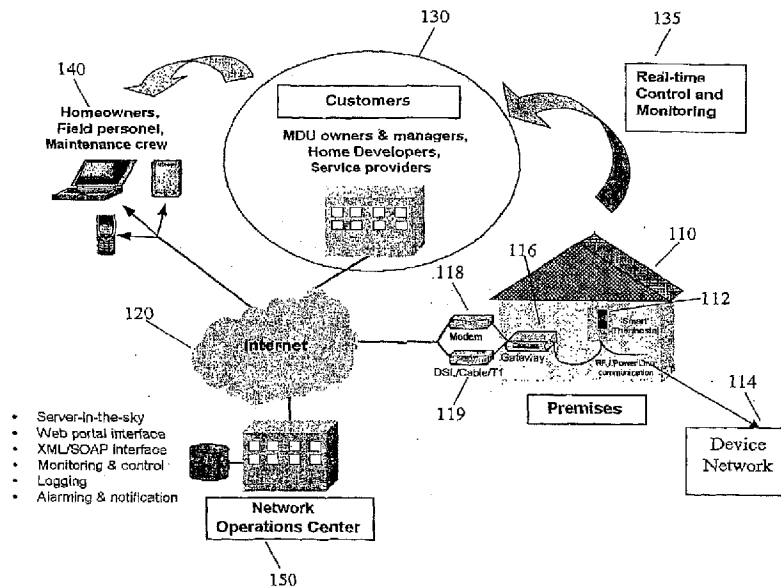
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:  
— with international search report

[Continued on next page]

(54) Title: PREMISES MANAGEMENT SYSTEM



(57) Abstract: Some embodiments of a method for premises management networking include monitoring premises management devices connected to a gateway at a premises; controlling premises management devices connected to the gateway at the premises; receiving, at the premises, an uplink-initiation signal associated with a network operations center server; and in response to the uplink-initiation signal, initiating, from the gateway at the premises, communications between the gateway and the network operations center server; and communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices.

WO 2005/091218 A3



— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

**(88) Date of publication of the international search report:**

27 July 2006

**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/US05/08766

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC: **H04L 12/56( 2006.01)**  
  
 USPC: 370/401  
 According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**  
 Minimum documentation searched (classification system followed by classification symbols)  
 U.S. : 370/401, 229, 230, 352, 389, 400, 465, 466  
  
 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
  
 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2003/0051009 A1 (SHAH et al) 13 March 2003 (13.03.2003), paragraphs 16-29 and Figures 1-2	11-4, 7-9, 18-20, 31-33, 33-37 ----- 4-6, 10-17, 21-30, 34-35
Y	US 2002/0083342 A1 (WEBB et al) 27 June 2002 (27.06.2002), paragraphs 4 and 27	5-6, 17, 30, and 35

Further documents are listed in the continuation of Box C.       See patent family annex.

* Special categories of cited documents:		"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier application or patent published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 11 April 2006 (11.04.2006)	Date of mailing of the international search report 23 MAY 2006
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Huy Vu Telephone No. (703) 272-2600

## PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:

RICHARD L. GREGORY  
COURTNEY STANIFORD & GREGORY LLP  
P.O. BOX 9686  
SAN JOSE, CA 95157

PCT

NOTIFICATION OF TRANSMITTAL OF  
THE INTERNATIONAL SEARCH REPORT AND  
THE WRITTEN OPINION OF THE INTERNATIONAL  
SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing (day/month/year) <b>22 OCT 2009</b>	
Applicant's or agent's file reference ICON.P011WO	<b>FOR FURTHER ACTION</b> See paragraphs 1 and 4 below
International application No. PCT/US 09/53485	International filing date (day/month/year) 11 August 2009 (11.08.2009)
Applicant <b>ICONTROL NETWORKS, INC.</b>	

1.  The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

**Filing of amendments and statement under Article 19:**

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 8270

**For more detailed instructions, see the notes on the accompanying sheet.**

2.  The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
3.  **With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:**
- the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.
- no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until **30 months** from the priority date (in some Offices even later); otherwise, the applicant must, within **20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer:  Lee W. Young  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--

Form PCT/ISA/220 (January 2004)

(See notes on accompanying sheet)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ICON.P011WO	<b>FOR FURTHER ACTION</b>	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 09/53485	International filing date (day/month/year) 11 August 2009 (11.08.2009)	(Earliest) Priority Date (day/month/year) 11 August 2008 (11.08.2008)
Applicant ICONTROL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- the international application in the language in which it was filed.
- a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b.  This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c.  With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2.  Certain claims were found unsearchable (see Box No. II).

3.  Unity of invention is lacking (see Box No. III).

4. With regard to the title,

- the text is approved as submitted by the applicant.
- the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- the text is approved as submitted by the applicant.
- the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. 1
  - as suggested by the applicant.
  - as selected by this Authority, because the applicant failed to suggest a figure.
  - as selected by this Authority, because this figure better characterizes the invention.
- b.  none of the figures is to be published with the abstract.



INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US 09/53485

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC(8) - G08B 13/00 (2009.01)  
USPC - 340/541  
According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
USPC: 340/541

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
USPC: 340/541, 539.19; 348/156 (text search - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
PubWEST(USPT,PGPB,EPAB,JPAB); Google Scholar, Dialog Web (DB:344, 347, 348, 349, 371, 654, 345, 351, 65, 35, 2)  
Search Terms: temperature, lighting, cellular, GPRS, broadband, xml, api, touchscreen, video, timeline, TUI, LAN, network, security system, mobile, widget, animation, history, time, panel, camera, webcam, IP, web

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2007/0298772 A1 (OWENS et al.) 27 December 2007 (27.12.2007), entire document, especially; para [0034], [0037]-[0039], [0045]-[0054], [0057]-[0068], [0073], [0074], Fig. 1-3	1, 2, 46-53, 60, 69-80, 82 ----- 3-45, 54-59, 61-68, 81
Y	US 2008/0065681 A1 (FONTIJN et al.) 13 March 2008 (13.03.2008), entire document, especially; para [0006], [0007], [0010]-[0016], [0019], [0035]-[0039], [0043]	3-45
Y	US 5,086,385 A (LAUNEY et al.) 04 February 1992 (04.02.1992), entire document, especially; col 15, ln 52 to col 16, ln 6, col 16, ln 48-61, col 19, ln 10-19, Fig. 1, 3a-3n	54-59, 61-68
Y	US 2008/0042826 A1 (HEVIA et al.) 21 February 2008 (21.02.2008), entire document, especially; para [0006]-[0009], [0026]	12, 14, 81
A	US 2006/0200845 A1 (FOSTER et al.) 07 September 2006 (07.09.2006), entire document	1 - 82

Further documents are listed in the continuation of Box C.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 16 October 2009 (16.10.2009)	Date of mailing of the international search report <b>22 OCT 2009</b>
---	--

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--

From the  
INTERNATIONAL SEARCHING AUTHORITY

To: RICHARD L. GREGORY  
COURTNEY STANIFORD & GREGORY LLP  
P.O. BOX 9686  
SAN JOSE, CA 95157

**PCT**

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing  
(day/month/year) **22 OCT 2009**

Applicant's or agent's file reference  
ICON.P011WO

**FOR FURTHER ACTION**  
See paragraph 2 below

International application No.  
PCT/US 09/53485

International filing date (day/month/year)  
11 August 2009 (11.08.2009)

Priority date (day/month/year)  
11 August 2008 (11.08.2008)

International Patent Classification (IPC) or both national classification and IPC  
IPC(8) - G08B 13/00 (2009.01)  
USPC - 340/541

Applicant ICONTROL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US  
Mail Stop PCT, Attn: ISA/US  
Commissioner for Patents  
P.O. Box 1450, Alexandria, Virginia 22313-1450  
Facsimile No. 571-273-3201

Date of completion of this opinion  
16 October 2009 (16.10.2009)

Authorized officer:  
Lee W. Young  
PCT Helpdesk: 571-272-4300  
PCT OSP: 571-272-7774

**Box No. I**      **Basis of this opinion**

1. With regard to the **language**, this opinion has been established on the basis of:
  - the international application in the language in which it was filed.
  - a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
  
2.  This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
  
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
  - a. (means)
    - on paper
    - in electronic form
  
  - b. (time)
    - in the international application as filed
    - together with the international application in electronic form
    - subsequently to this Authority for the purposes of search
  
4.  In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
  
5. Additional comments:

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	3-45, 54-59, 61-68, 81	YES
	Claims	1, 2, 46-53, 60, 69-80, 82	NO
Inventive step (IS)	Claims	None.	YES
	Claims	1 - 82	NO
Industrial applicability (IA)	Claims	1 - 82	YES
	Claims	None.	NO

2. Citations and explanations:

Claims 1, 2, 46-53, 60, 69-80 and 82 lack novelty under PCT Article 33(2) as being anticipated by US 2007/0298772 A1 to Owens et al. (hereinafter 'Owens').

As per claim 1, Owens discloses a system comprising: an interface device comprising a display (FIG. 2, part 74 and para [0059]) coupled to a processor, wherein the processor is coupled to a local network and a security system at a first location (FIG. 2, part 32 para [0049]); and a plurality of interfaces coupled to the processor and presented to a user via the display, wherein the plurality of interfaces include a security interface (FIG. 2, part 56) integrated with a network interface (FIG. 2, part 46), wherein the security interface allows the user to control functions of the security system and to access data collected by the security system (para [0057], wherein the network interface allows the user to control functions of network components coupled to the local network and to access content of a remote network coupled to the local network (para [0047] and [0058]).

As per claim 2, Owens discloses the system of claim 1, and Owens further discloses wherein the plurality of interfaces comprises control icons for controlling components of the security system and the network components (para [0060]-[0062]).

As per claim 46, Owens discloses the system of claim 1, and Owens further discloses wherein the plurality of interfaces comprise an energy management user interface (EMUI) (FIG. 3, parts 80-88 and para [0051]-[0056]).

As per claim 47, Owens discloses the system of claim 46, and Owens further discloses wherein the EMUI enables control of energy management components (para [0051] and [0054]).

As per claim 48, Owens discloses the system of claim 46, and Owens further discloses wherein the EMUI displays energy usage information of the first location (para [0052] and [0053]).

As per claim 49, Owens discloses the system of claim 46, and Owens further discloses wherein the network components comprise the energy management components (para [0047] and [0052]).

As per claim 50, Owens discloses the system of claim 46, and Owens further discloses wherein the energy management components comprise at least one of device controllers, system controllers, lighting controllers and temperature controllers (para [0051] and [0054]).

As per claim 51, Owens discloses the system of claim 50, and Owens further discloses wherein the EMUI comprises control icons for the device controllers (FIG. 3, parts 80, 86, 90, 88).

As per claim 52, Owens discloses the system of claim 50, and Owens further discloses wherein the EMUI comprises control icons for the system controllers (FIG. 3, part 78).

As per claim 53, Owens discloses the system of claim 50, and Owens further discloses wherein the EMUI comprises control icons for the lighting controllers (FIG. 3, part 80).

As per claim 60, Owens discloses the system of claim 50, and Owens further discloses wherein the EMUI comprises control icons for the temperature controllers (FIG. 3, part 88 wherein HVAC is a temperature controller).

As per claim 69, Owens discloses the system of claim 1, and Owens further discloses wherein the interface device comprises at least one of a remote client device, a personal computer (PC), a cellular telephone, and a personal digital assistant (PDA) (FIG. 2, part 30 and para [0045]).

As per claim 70, Owens discloses the system of claim 1, and Owens further discloses a remote server coupled to the interface device, the remote server managing at least one of the plurality of interfaces and the security system (FIG. 2, parts 46 and 34).

As per claim 71, Owens discloses the system of claim 70, and Owens further discloses wherein the remote server allows a user to configure content of the interface device (para [0052] and [0074]).

—Continued on the Supplemental Box—

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

V.2. Citations and explanations:

As per claim 72, Owens discloses the system of claim 70, and Owens further discloses wherein the remote server provides user portals that enable content and information displayed on the interface device to be displayed on other devices (para [0073]).

As per claim 73, Owens discloses the system of claim 1, and Owens further discloses wherein the interface device integrates content with the access and control of the security system (para [0060], [0062], [0064] and [0066]).

As per claim 74, Owens discloses the system of claim 73, and Owens further discloses wherein the content comprises interactive content including Internet widgets (para [0060] and [0061], wherein the various menus shown in FIG. 3 are Internet widgets).

As per claim 75, Owens discloses the system of claim 1, and Owens further discloses wherein the network interface enables transfer of at least one of content and Internet widgets to and from the local network (para [0073]).

As per claim 76, Owens discloses the system of claim 1, and Owens further discloses wherein the network interface enables control of functions of peripheral devices of the first location coupled to the local network (para [0073] and [0074]).

As per claim 77, Owens discloses the system of claim 1, and Owens further discloses wherein the plurality of interfaces is configurable (para [0052] and [0053]).

As per claim 78, Owens discloses the system of claim 1, and Owens further discloses wherein the network interface enables communication and control of a plurality of network devices coupled to the local network (para [0049]).

As per claim 79, Owens discloses the system of claim 1, and Owens further discloses wherein the network interface enables communication with and control of a plurality of security system components, wherein the security system comprises the plurality of security system components (para [0058]).

As per claim 80, Owens discloses the system of claim 1, and Owens further discloses wherein the remote network is the Internet and the interface device comprises a web browser (para [0047]).

As per claim 82, Owens discloses the system of claim 1, and Owens further discloses wherein the interface device allows a user to control functions of peripheral devices coupled to at least one of other network components and other security systems located at remote locations (FIG. 1, parts 14 and 16 which are separate systems).

Claims 3-11, 13 and 15-45 lack an inventive step under PCT Article 33(3) as being obvious over Owens, in view of US 2008/0065681 A1 to Fontijn et al. (hereinafter 'Fontijn').

As per claim 3, Owens discloses the system of claim 1, and further discloses wherein the plurality of interfaces are able to display pre-recorded information (para [0037] and [0059]), however, Owens does not specifically disclose wherein the plurality of interfaces comprises a timeline user interface (TUI). Fontijn discloses that timeline user interface is a common way to store and interact with video files and other files that have a particular sequence in electronic devices (para [0006] and [0007]). It would have been obvious to one of ordinary skill in the art to have the plurality of interfaces of Owens comprise a timeline user interface as disclosed by Fontijn as this is the common interface for interacting with video, audio, and text files such as would be recorded by a security system.

As per claim 4, Owens in view of Fontijn discloses the system of claim 3, and Fontijn further discloses wherein the TUI comprises a variable-length timeline (para [0007] and [0011]).

As per claim 5, Owens in view of Fontijn discloses the system of claim 3, and Fontijn further discloses wherein a time scale of the TUI can be dynamically changed (para [0010] and [0038]).

As per claim 6, Owens in view of Fontijn discloses the system of claim 3, and Owens further discloses wherein the TUI comprises component data presented in a timeline (para [0057], [0062], and [0068] wherein in view of Fontijn the status of the components would be presented in a timeline).

As per claim 7, Owens in view of Fontijn discloses the system of claim 6, and Owens further discloses wherein the component data comprises component state presented in a timeline (para [0057], [0062], and [0068] wherein in view of Fontijn the status of the components would be presented in a timeline).

As per claim 8, Owens in view of Fontijn discloses the system of claim 6, and Fontijn further discloses wherein the component data comprises component history presented in a timeline (para [0037]-[0039]).

As per claim 9, Owens in view of Fontijn discloses the system of claim 6, and Owens further discloses wherein the component data corresponds to at least one of a plurality of security components and the network components, wherein the security system comprises the plurality of security components (para [0049] and [0057]).

--Continued on next page.--

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

V.2. Citations and explanations:

As per claim 10, Owens in view of Fontijn discloses the system of claim 6, and Owens further discloses wherein the component data is at least one of photos and video from a camera (para [0058], wherein the data is video).

As per claim 11, Owens in view of Fontijn discloses the system of claim 10, and Fontijn further discloses wherein an event captured in at least one of the photos and the video are depicted on the timeline using icons (para [0039]).

As per claim 13, Owens in view of Fontijn discloses the system of claim 6, and Owens further discloses wherein the component data comprises security system state (para [0057] and [0062]).

As per claim 15, Owens in view of Fontijn discloses the system of claim 6, and Owens further discloses wherein the network components comprise energy management components (para [0047] and [0052]).

As per claim 16, Owens in view of Fontijn discloses the system of claim 15, and Owens further discloses wherein the component data comprises state data of the energy management components (para [0047] and [0052]).

As per claim 17, Owens in view of Fontijn discloses the system of claim 15, and Owens further discloses wherein the energy management components comprise at least one of device controllers, system controllers, lighting controllers and temperature controllers (FIG. 3, parts 80, 86, 90, 88).

As per claim 18, Owens in view of Fontijn discloses the system of claim 17, and Owens further discloses wherein the TUI comprises control icons for the device controllers (FIG. 3, parts 80, 86, 90, 88).

As per claim 19, Owens in view of Fontijn discloses the system of claim 17, and Owens further discloses wherein the TUI comprises control icons for the system controllers (FIG. 3, part 78).

As per claim 20, Owens in view of Fontijn discloses the system of claim 17, and Owens further discloses wherein the TUI comprises control icons for the lighting controllers (FIG. 3, part 80).

As per claim 21, Owens in view of Fontijn discloses the system of claim 17, and Owens further discloses wherein the TUI comprises control icons for the temperature controllers (FIG. 3, part 88 wherein HVAC is a temperature controller).

As per claim 22, Owens discloses the system of claim 1, however, Owens does not specifically disclose wherein the plurality of interfaces comprises a slideshow timeline editor (STE), wherein the STE enables generation of slideshow animations. Fontijn discloses wherein video files are stored in a timeline file or slideshow (in the case of images) para [0006] and [0012]). Fontijn discloses such a file allows for grouping similar data together and for easier understanding of a group of multimedia data (para [0011]-[0013]).

As per claim 23, Owens in view of Fontijn discloses the system of claim 22, and Fontijn further discloses wherein the STE enables creation and management of a plurality of content formats and a plurality of content sources for a display (para [0011] and [0012]).

As per claim 24, Owens in view of Fontijn discloses the system of claim 23, and Owens further discloses wherein the display comprises at least one of a touchscreen, a television, a remote client device display, a personal computer (PC) display, a cellular telephone display, and a personal digital assistant (PDA) display (para [0034]).

As per claim 25, Owens in view of Fontijn discloses the system of claim 22, and Fontijn further discloses wherein the STE comprises a widget palette, a preview screen, and slideshow timeline tool (para [0006], [0015], [0038] and [0039] wherein they are presented in a slideshow timeline and/or preview screen).

As per claim 26, Owens in view of Fontijn discloses the system of claim 25, and Fontijn further discloses wherein the STE comprises a plurality of tracks (para [0006] and [0012]).

As per claim 27, Owens in view of Fontijn discloses the system of claim 25, and Fontijn further discloses wherein the widget palette comprises widget icons corresponding to a widget, and descriptive text corresponding to the widget icons (para [0011] wherein the annotation is the descriptive text and file is presented as a widget).

As per claim 28, Owens in view of Fontijn discloses the system of claim 27, and Owens further discloses wherein the widgets comprise at least one of a clock widget, a calendar widget, a photo widget, a news widget, a weather widget, a sports widget, a stock widget, a ticker widget, and a traffic widget (FIG. 2, part 68 wherein a clock widget is displayed, further it would have been obvious to one of ordinary skill in the art that the wireless device of Owens would be able to display widgets for calendar, photo, news, weather, sports etc. as these are common capabilities of PDA's).

As per claim 29, Owens in view of Fontijn discloses the system of claim 27, and Owens further discloses wherein the widgets comprise an event widget, wherein the event widget corresponds to events detected by components of the security system (FIG. 3, part 76).

As per claim 30, Owens in view of Fontijn discloses the system of claim 27, and Owens further discloses wherein the widgets correspond to components of the security system (FIG. 3, parts 84, 94, and 96).

--Continued on next page.--

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

V.2. Citations and explanations:

As per claim 31, Owens in view of Fontijn discloses the system of claim 27, and Owens further discloses wherein the widgets correspond to the network components (FIG. 3, parts 82 and 92 among others).

As per claim 32, Owens in view of Fontijn discloses the system of claim 27, and Owens further discloses wherein the widgets comprise an action widget, wherein the action widget corresponds to actions taken via the network components (para [0035]).

As per claim 33, Owens in view of Fontijn discloses the system of claim 27, and Owens further discloses wherein a selected widget icon, when selected by a user, is loaded into the preview screen and runs in the preview screen to present via the interface device functionality of a widget corresponding to the selected widget icon (para [0062], [0069] and [0073]).

As per claim 34, Owens in view of Fontijn discloses the system of claim 27, and Fontijn further discloses wherein the selected widget icon is moved into the slideshow timeline tool, wherein the slideshow timeline tool enables placement of the selected widget icon on a timeline, wherein the placement on the timeline controls a start time and a stop time of the widget (para [0012], [0013], and [0015]).

As per claim 35, Owens in view of Fontijn discloses the system of claim 34, and Fontijn further discloses wherein the timeline comprises a plurality of selected widget icons placed at intervals along the timeline (para [0011], [0014] and [0016]).

As per claim 36, Owens in view of Fontijn discloses the system of claim 35, and Fontijn further discloses wherein the placement on the timeline of the plurality of selected widget icons controls a respective start time and stop time of a plurality of widgets corresponding to the plurality of widget icons (para [0015]).

As per claim 37, Owens in view of Fontijn discloses the system of claim 36, and Fontijn further discloses wherein the respective start time and stop time of a widget is a time relative to at least one of a respective start time and stop time of another widget of the plurality of widgets (para [0015] and [0016]).

As per claim 38, Owens in view of Fontijn discloses the system of claim 36, and Fontijn further discloses wherein the respective start time and stop time of a widget is an actual clock time (para [0019], which discloses that the file includes a code with the actual date and time).

As per claim 39, Owens in view of Fontijn discloses the system of claim 35, and Fontijn further discloses wherein the slideshow animation runs on the interface device (para [0017] and [0038], wherein in view of Owens it is played on a PDA).

As per claim 40, Owens in view of Fontijn discloses the system of claim 39, and Fontijn further discloses wherein the slideshow animation runs automatically under control of the timeline (para [0035] and [0043]).

As per claim 41, Owens in view of Fontijn discloses the system of claim 39, however, Owens in view of Fontijn does not specifically disclose wherein execution of the slideshow animation is initiated manually via an icon on the interface device. However, it would have been obvious to one of ordinary skill in the art to have such a slideshow initiated manually via an icon on the interface device of Owens in view of Fontijn as this is an easy graphical method of initiating a slideshow on a device such as a PDA.

As per claim 42, Owens in view of Fontijn discloses the system of claim 39, Owens further discloses wherein execution of the slideshow animation is initiated automatically in response to at least one of communication from the network components and communication from security components of the security system (para [0061] and [0062]).

As per claim 43, Owens in view of Fontijn discloses the system of claim 39, however, Owens in view of Fontijn does not specifically disclose wherein execution of the slideshow animation is initiated automatically via a time schedule. However, it would have been obvious to one of ordinary skill in the art to have the slideshow animation of Owens in view of Fontijn be able to initiated automatically via a time schedule, as this allows a user to have a particular security feature monitored at a set time of day allowing for a routine.

As per claim 44, Owens in view of Fontijn discloses the system of claim 22, and Owens further discloses wherein the STE enables generation of slideshow animations integrated with events, wherein the events are events detected by components of the security system (para [0061] and [0062]).

As per claim 45, Owens in view of Fontijn discloses the system of claim 22, and Owens further discloses wherein the STE enables generation of slideshow animations integrated with actions, wherein the actions are actions taken via the network components (para [0067]-[0073]).

Claims 54-59 and 61-68 lack an inventive step under PCT Article 33(3) as being obvious over Owens, in view of US 5,086,385 A to Launey et al. (hereinafter 'Launey').

As per claim 54, Owens discloses the system of claim 53, however, Owens does not specifically disclose wherein the EMUI comprises a plurality of control phases. Launey discloses in a home automation system including a home security system (FIG. 1, part 38) to have various devices such as home lighting and temperature controlled in a plurality of phases/time periods (col 15, ln 52 to col 16, ln 6). It would have been obvious to one of ordinary skill in the art to have the components of the system of Owens function on a plurality of control phases as disclosed by Launey as this allows the system to automatically set features such as temperature to save energy and to anticipate a user's needs.

--Continued on next page.--

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.  
Continuation of:

**V.2. Citations and explanations:**

As per claim 55, Owens in view of Launey discloses the system of claim 54, and Launey further discloses wherein each phase corresponds to a time period (col 15, ln 52 to col 16, ln 6).

As per claim 56, Owens in view of Launey discloses the system of claim 54, and Launey further discloses wherein the EMUI comprises a first plurality of regions that include information of the phases (col 15, ln 52-58 and FIG. 3a-3n).

As per claim 57, Owens in view of Launey discloses the system of claim 56, and Launey further discloses wherein the EMUI comprises a second plurality of regions that include information of the lighting controllers (FIG. 3m).

As per claim 58, Owens in view of Launey discloses the system of claim 57, and Launey further discloses wherein the information of the lighting controllers comprises a lighting level of a region of the first location, the lighting level corresponding to a phase (col 15, ln 52 to col 16, ln 6 and col 19, ln 10-19).

As per claim 59, Owens in view of Launey discloses the system of claim 58, wherein the information of the lighting controllers comprises a lighting state of the lighting controller of a region of the first location, the lighting state corresponding to a phase (col 15, ln 52 to col 16, ln 6 and col 19, ln 10-19).

As per claim 61, Owens discloses the system of claim 60, however, Owens does not specifically disclose wherein the EMUI comprises a plurality of control phases. Launey discloses in a home automation system including a home security system (FIG. 1, part 38) to have various devices such as home lighting and temperature controlled in a plurality of phases/time periods (col 15, ln 52 to col 16, ln 6). It would have been obvious to one of ordinary skill in the art to have the components of the system of Owens function on a plurality of control phases as disclosed by Launey as this allows the system to automatically set features such as temperature to save energy and to anticipate a user's needs.

as per claim 62, Owens in view of Launey discloses the system of claim 61, and Launey further discloses wherein each phase corresponds to a time period (col 15, ln 52 to col 16, ln 6).

As per claim 63, Owens in view of Launey discloses the system of claim 61, and Launey further discloses wherein the EMUI comprises a first plurality of regions that include information of the phases (col 15, ln 52-58 and FIG. 3a-3n).

As per claim 64, Owens in view of Launey discloses the system of claim 63, and Launey further discloses wherein the EMUI comprises a second plurality of regions that include information of the temperature controllers (FIG. 3A, environmental control col 16, ln 48-61).

As per claim 65, Owens in view of Launey discloses the system of claim 64, and Launey further discloses wherein the information of the temperature controllers comprises a temperature of a region of the first location, the temperature corresponding to a phase (col 16, ln 48-61).

As per claim 66, Owens in view of Launey discloses the system of claim 65, and Launey further discloses wherein the temperature is a current temperature of the region (col 16, ln 48-61).

As per claim 67, Owens in view of Launey discloses the system of claim 65, however, Owens in view of Launey does not specifically disclose wherein the temperature is at least one historic temperature of the region. However, it would have been obvious to one of ordinary skill in the art through routine experimentation to have the temperature of the system of Owens in view of Launey be based on historic temperatures of the region as this allows for easier adjustment by taking into account past preferences.

As per claim 68, Owens in view of Launey discloses the system of claim 65, Launey further discloses wherein the information of the temperature controllers comprises a temperature setting of the temperature controller of a region of the first location, the temperature setting corresponding to a phase (col 15, ln 52 to col 16, ln 6 and col 16, ln 48-61).

Claim 81 lacks an inventive step under PCT Article 33(3) as being obvious over Owens, in view of US 2008/0042826 A1 to Hevia et al. (hereinafter 'Hevia').

As per claim 81, Owens discloses the system of claim 1, however, Owens does not specifically disclose wherein the interface device integrates at least one of a security system control panel and an Internet browser. Hevia discloses the use of an alarm panel in a home security system (para [0026]). It would have been obvious to one of ordinary skill in the art to have the system of Owens in view of Fontijn include an alarm panel as disclosed by Hevia as this is the common means for interfacing with a security system.

Claims 12 and 14 lack an inventive step under PCT Article 33(3) as being obvious over Owens in view of Fontijn, and further in view of Hevia.

As per claim 12, Owens in view of Fontijn discloses the system of claim 10, however, Owens in view of Fontijn does not specifically disclose wherein the camera is an Internet Protocol (IP) camera. Hevia discloses using an IP camera in a home security system (para [0026]). It would have been obvious to one of ordinary skill in the art to have the cameras of the system of Owens in view of Fontijn be IP cameras as disclosed by Hevia as this allows for the use of cheap and readily available cameras in the security system (Hevia para [0006], [0008] and [0009]).

--Continued on next page.--



**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.  
Continuation of:

V.2. Citations and explanations:

As per claim 14, Owens in view of Fontijn discloses the system of claim 6, however, Owens in view of Fontijn does not specifically disclose wherein the component data comprises alarm panel state, wherein the security system comprises the alarm panel. Hevia discloses the use of an alarm panel in a home security system (para [0026]). It would have been obvious to one of ordinary skill in the art to have the system of Owens in view of Fontijn include an alarm panel as disclosed by Hevia as this is the common means for interfacing with a security system.

Claims 1 - 82 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: RICHARD GREGORY  
 COURTNEY STANIFORD & GREGORY LLP  
 P.O. BOX 9686  
 SAN JOSE, CA 95157

PCT

NOTIFICATION OF TRANSMITTAL OF  
 THE INTERNATIONAL SEARCH REPORT AND  
 THE WRITTEN OPINION OF THE INTERNATIONAL  
 SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing (day/month/year)	12 NOV 2009
Applicant's or agent's file reference ICON.P012WO	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US2009/055559	International filing date (day/month/year) 31 August 2009
Applicant ICONTROL NETWORKS, INC.	

1.  The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.  
**Filing of amendments and statement under Article 19:**  
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):  
**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.  
**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70  
**For more detailed instructions, see the notes on the accompanying sheet.**
2.  The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
3.  **With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:**  
 the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.  
 no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.
4. **Reminders**  
 Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.  
 The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.  
 Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.  
 In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.  
 See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver Telephone No. 571-272-7774
---	--

Form PCT/ISA/220 (January 2004)

(See notes on accompanying sheet)

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ICON.P012WO	<b>FOR FURTHER ACTION</b> see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US2009/055559	International filing date ( <i>day/month/year</i> ) 31 August 2009	(Earliest) Priority Date ( <i>day/month/year</i> ) 29 August 2008
Applicant CONTROL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

## 1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- the international application in the language in which it was filed.
- a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b.  This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c.  With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2.  Certain claims were found unsearchable (see Box No. II).

3.  Unity of invention is lacking (see Box No. III).

4. With regard to the title,

- the text is approved as submitted by the applicant.
- the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- the text is approved as submitted by the applicant.
- the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. 2
- as suggested by the applicant.
- as selected by this Authority, because the applicant failed to suggest a figure.
- as selected by this Authority, because this figure better characterizes the invention.
- b.  none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US2009/055559

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC(8) - H02M 7/00 (2009.01)  
 USPC - 307/64  
 According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**  
 Minimum documentation searched (classification system followed by classification symbols)  
 IPC(8) - H02M 7/00 (2009.01)  
 USPC - 320/137; 307/43-44, 64; 714/14, 22; 323/276

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
 MicroPatent

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,579,197 A (MENGELT et al) 26 November 1996 (26.11.1996) see document	1-22
Y	US 6,462,507 B2 (FISHER, JR) 08 October 2002 (08.10.2002) see document	1-22
Y	WO 89/07855 A1 (BAVARO) 24 August 1989 (24.08.1989) see document	3, 12 and 20-21
Y	US 4,860,185 A (BREWER et al) 22 August 1989 (22.08.1989) see document	9 and 15
A	US 6,865,690 B2 (KOCIN) 08 March 2005 (08.03.2005) see document	1-22
A	US 4,779,007 A (SCHLANGER et al) 18 October 1988 (18.10.1988) see document	1-22
A	US 6,795,322 B2 (AIHARA et al) 21 September 2004 (21.09.2004) see document	1-22

Further documents are listed in the continuation of Box C.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 23 October 2009	Date of mailing of the international search report <b>12 NOV 2009</b>
--	--

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	---

PATENT COOPERATION TREATY

From the  
INTERNATIONAL SEARCHING AUTHORITY

To: RICHARD GREGORY  
COURTNEY STANIFORD & GREGORY LLP  
P.O. BOX 9686  
SAN JOSE, CA 95157

PCT

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Applicant's or agent's file reference ICON.P012WO		Date of mailing (day/month/year) <b>12 NOV 2009</b>
International application No. PCT/US2009/055559		FOR FURTHER ACTION See paragraph 2 below
International filing date (day/month/year) 31 August 2009	Priority date (day/month/year) 29 August 2008	
International Patent Classification (IPC) or both national classification and IPC IPC(8) - H02M 7/00 (2009.01) USPC - 307/64		
Applicant ICONTROL NETWORKS, INC.		

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion <b>23 October 2009</b>	Authorized officer: <b>Blaine R. Copenheaver</b>  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--	--

Form PCT/ISA/237 (cover sheet) (July 2009)

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITYInternational application No.  
PCT/US2009/055559

## Box No. 1 Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
- the international application in the language in which it was filed.
- a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2.  This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
- a. (means)
- on paper
- in electronic form
- b. (time)
- in the international application as filed
- together with the international application in electronic form
- subsequently to this Authority for the purposes of search
4.  In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US2009/055559

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-22	YES
	Claims	None	NO
Inventive step (IS)	Claims	None	YES
	Claims	1-22	NO
Industrial applicability (IA)	Claims	1-22	YES
	Claims	None	NO

2. Citations and explanations:

Claims 1-2, 4-8, 10-11, 13-14, 16-19 and 22 lack an inventive step under PCT Article 33(3) as being obvious over Mengelt et al., hereinafter referred to as Mengelt, in view of Fisher, Jr., hereinafter referred to as Fisher.

With regards to claims 1-2, Fig. 3 of Mengelt discloses a device (back-up power system 40) comprising: a main AC power system (20) that sends AC power/input signal (see col. 6, lines 48-50); a battery module (battery 64 in combination with charger 66, inverter 56 and transformer 59) coupled to the AC main power system (see fig. 3); the battery module comprising battery charging circuitry (66) coupled to a battery (64); and an output controller (controller 50 in combination with relay coil 51 and switches 48,49) coupled to the AC main power system and the battery module (see fig. 3); wherein the output controller comprises inherent detector circuitry (microprocessor program; see col. 10, lines 40-59) that detects a state of the input signal that represents power or lack thereof from the AC main supply system, wherein the output controller automatically controls the coupling of one of a main AC power system output and a battery module output to a device output according to the state of the input signal (see col. 6, line 50-col. 8, line 22 for the complete discussion).

Yet, Mengelt does not specifically discuss the device further comprising a transformer module that receives an input signal; a battery module coupled to the transformer module, wherein the transformer module comprises transformer circuitry, and wherein the transformer circuitry receives the input signal; and an output controller coupled to the transformer module, wherein the output controller automatically controls the coupling of one of a transformer module output and a battery module output to a device output according to the state of the input signal.

However, the use of transformer modules with inherent transformer circuitry that receive AC voltage input signals in combination with battery modules that are coupled to transformer modules in back-up power systems for the purpose of supplying power to both a load and the batteries is notoriously well known and of common knowledge in the art as evidenced by Fisher (see Fig. 2 as well as col. 4, lines 28-67 and col. 5, lines 16-33 of Fisher). More over, Fisher teaches that it would be desirable to connect a transformer to a main AC power supply system for the purpose of supplying a specified level of energy and power to a load in situations where electrical power or energy cannot easily or economically be directly supplied to the load from public utility electric power grids or other large electric power sources (see col. 5, lines 24-33 of Fisher). Also, the additional coupling of output controllers to transformer modules in back-up power systems, wherein the output controllers automatically control the coupling of one of a transformer module output and a battery module output to a device output according to the state of the input signal, for the purpose of supplying back-up power from the batteries to a load/device in the event that power from the main supply is interrupted is notoriously well known and of common knowledge in the art as evidenced by Fisher (see fig. 2 as well as col. 4, lines 28-67 of Fisher).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the device of Mengelt incorporate a well known transformer module into the circuit arrangement described above by connecting the transformer module with the inherent transformer circuitry to the main AC power system of Mengelt, wherein the transformer circuitry of the transformer module receives an input signal/AC power; wherein the battery module of Mengelt is coupled to the transformer module; and the output controller of Mengelt is coupled to the transformer module such that the output controller automatically controls the coupling of one of a transformer module output and a battery module output to a device output according to the state of the input signal/AC voltage, for the purpose of facilitating power from the main AC power supply to the battery module and load in order to keep the battery module charged and the load properly powered when the AC power from the main system is present, while switching to the battery module to power the load in the event that the main AC power is interrupted, as shown and taught by Fisher.

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US2009/055559

## Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

With regards to claim 10, Fig. 3 of Mengelt discloses a device (battery back-up power system 40) comprising:

a main AC power system (20) that sends AC power/input signal (see col. 6, lines 48-50);

a battery module (battery 64 in combination with charger 66, inverter 56 and transformer 59), wherein the battery module comprising battery charging circuitry (66) coupled to a battery (64); and

an output controller (controller 50 in combination with relay coil 51 and switches 48,49) having a first input (connected to lines 52 and 53; see fig. 3) and a second input (connected to line 55), wherein the second input of the output controller is coupled to a battery output of the battery module, and wherein the output controller automatically switches one of the main AC power output and the battery output as a device output according to a state of the input signal (see col. 6, line 50-col. 8, line 22 for the complete discussion).

Yet, Mengelt does not specifically discuss the device further comprising transformer circuitry, wherein the transformer circuitry receives an input signal; regulator circuitry coupled to the transformer circuitry; a battery module coupled to the regulator circuitry; and wherein the first input of the output controller is coupled to a power output of the regulator circuitry.

However, the use of transformer circuitry, wherein the transformer circuitry receives an input signal, in combination with regulator circuitry that is coupled to the transformer circuitry, battery modules that are coupled to the regulator circuitry; and wherein, the first input of output controllers are coupled to the power output of the regulator circuitry in back-up power systems/devices for the purpose of supplying power to both a load and the batteries is well known and of common knowledge in the art as evidenced by Fisher (see fig. 2 and 5 as well as col. 4, lines 28-67, col. 5, lines 16-33, col. 7, lines 9-33 and col. 9, lines 11-21 of Fisher; wherein figs. 2 and 5 disclose the transformer 24 coupled to regulator 26, wherein regulator 26 is coupled to charging circuitry in energy storage device 22; and the first input of sensor/output controller 32 is coupled to the power output of the regulator via energy converter 28). More over, Fisher teaches that it would be desirable to connect a transformer to a main AC power supply system for the purpose of supplying a specified level of energy and power to a load in situations where electrical power or energy cannot easily or economically be directly supplied to the load from public utility electric power grids or other large electric power sources (see col. 5, lines 24-33 of Fisher). In addition, it would be desirable to couple a regulator to the transformer and battery charging circuitry for the purpose of conditioning the current to match with the battery module and the load in order to properly power the charger and load, respectively, as taught by Fisher (see col. 4, lines 32-35 of Fisher, for example). Also, it would be desirable to couple the first input of the output controller to the power output of the regulator circuitry for the purpose of having the ability to switch the output from the regulator output to the battery output in the event that conditioned current from the main power supply is not present.

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have device of Mengelt incorporate a well known transformer circuitry into the circuit arrangement described above by connecting the transformer circuitry along with an accompanied regulator to the main AC power system of Mengelt, wherein the transformer circuitry receives an input signal/AC power; coupling a well known battery module to the regulator circuitry; and coupling the first input of the output controller to the power output of the regulator circuitry, as shown by Fisher, for the purpose of facilitating power from the main AC power supply to the battery module and load in order to keep the battery module charged and the load properly powered by conditioning the current to match the charging circuitry and load via the transformer and coupled regulator when the AC power from the main system is present, while switching to the battery module to power the load in the event that the conditioned current from the main AC power via the transformer circuitry and coupled regulator is interrupted, as shown and taught by Fisher.

With regards to claim 16, Mengelt discloses a method comprising:

receiving an input signal at a device (see fig. 3 and col. 6, lines 45-58, which discloses the main AC power system delivering an input signal in the form of AC current to the back-up power system or device 40, wherein the device receives the input signal/AC current at input terminals 41 and 43);

Yet, Mengelt does not specifically discuss the following steps: generating a first output signal by transforming the input signal; charging a battery of the device with the first output signal; providing a second output signal that is an output of the battery; detecting a state of the input signal; and automatically controlling an output of the device to be one of the first output signal and the second output signal according to the state of the input signal.

However, the steps of generating a first output signal by transforming the input signal; charging a battery of the device with the first output signal; providing a second output signal that is an output of the battery; detecting a state of the input signal; and automatically controlling an output of the device to be one of the first output signal and the second output signal according to the state of the input signal, for the purpose of providing uninterruptible conditioned current to a load well known and of common knowledge in the art as shown and taught by Fisher (see fig. 2 and 5 as well as col. 4, lines 28-67, col. 5, lines 16-33, col. 7, lines 9-33 and col. 9, lines 11-21 of Fisher).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Mengelt additionally include the well known steps that are described above for the purpose of providing uninterruptible conditioned current to a load, as shown and taught by Fisher.

With regards to claims 4-6, Mengelt does not specifically discuss the transformer module comprising regulator circuitry that is coupled to the transformer circuitry; wherein a regulator circuitry output is coupled to the detector circuitry and the output controller; and wherein the battery charging circuitry is coupled to the regulator circuitry.

However, the use of regulators as part of the transformer module and coupled to the detector circuitry in electrical devices and back-up power systems is well known and of common knowledge in the art as evidenced by Fisher (see fig. 2 of Fisher, which disclose the transformer 24 coupled to regulator 26, wherein regulator 26 is coupled to charging circuitry in energy storage device 22). More over, it would be desirable to couple a regulator to a transformer, detector circuitry, output controller and battery charging circuitry for the purpose of conditioning the current to match with the battery module and the load in order to properly power the charging circuitry and load, respectively, as taught by Fisher (see col. 4, lines 32-35 of Fisher, for example).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the device of Mengelt in view of Fisher incorporate a transformer module that includes a regulator, wherein the regulator is coupled to a transformer, detector circuitry, output controller and battery charging circuitry in the arrangement described above, for the purpose of conditioning the current to match with the battery module and the load in order to properly power the charger and load, respectively, as taught by Fisher.

With regards to claims 7-8 and 13-14, Mengelt discloses the input signal inherently being an alternating current AC signal (see fig. 3 as well as col. 6, lines 47-50, wherein the AC current is inputted across lines 45-46 from main AC supply system to the load in order to power it); wherein the device output is an alternating current AC signal (see fig. 3 as well as col. 6, lines 47-50 and col. 7, lines 8-25, which discuss powering the load with AC from the device/back-up power system 40).



**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.  
PCT/US2009/055559

**Supplemental Box**

**In case the space in any of the preceding boxes is not sufficient.**

Continuation of:

With regards to claim 11, Mengelt discloses the device comprising an detector (microprocessor program; see col. 10, lines 40-59) that is inherently coupled to the output controller by being a part of the controller, wherein the detector provides a control signal to the controller in response to a detected state of the input signal (see col. 7, line 32-col. 10, line 7 for a complete discussion).

Yet, Mengelt does not specifically discuss the detector coupled to the regulator circuitry.

However it would be for the detector to be coupled to the regulator circuitry for the purpose of determining whether or not the conditioned current from the main power supply is present while having the ability to switch the output from the regulator output to the battery output, as shown and taught by Fisher (see fig. 2 and col. 7, lines 9-33 and col. 9, lines 11-21 of Fisher, for example).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the detector of Mengelt coupled to the regulator circuitry for the purpose of determining whether or not the conditioned current from the main power supply is present while having the ability to switch the output from the regulator output to the battery output, as shown and taught by Fisher, in the event that current from the main power supply via the transformer circuitry and regulator is interrupted.

With regards to claim 17, Mengelt in view of Fisher does not specifically discuss the step of automatically controlling comprises coupling the first output signal to the output of the device when the state of the input signal is present.

However, Fig. 3 as well col. 6, line 45-col. 7, line 6 of Mengelt teach the concept of coupling output signals that generate from the input terminals 41,42 to the output of the device, through output terminals 43,44 via the switches 48,49, when the state of the input signal is present for the purpose of supplying power to a load (wherein, the input signal represents AC current that is originally derived from main AC power system 20; see col. 6, lines 47-50 of Mengelt).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the automatically controlling step of Mengelt in view of Fisher comprise coupling the first output signal to the output of the device when the state of the input signal is present for the purpose of supplying conditioned current to a load in order to properly power it.

With regards to claim 18, Mengelt in view of Fisher does not specifically discuss the charging of the battery occurs when the state of the input signal is present.

However, the concept of charging the battery of a back-up power system when the state of an input signal is present is well known and of common knowledge in the art as evidenced by Mengelt (see Fig. 3 as well as col. 7, lines 25-31 of Mengelt, wherein the AC current signal from the main AC power system represents the input signal).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the method of Mengelt in view of Fisher require that the charging of the battery occur when the state of the input signal is present for the purpose of keeping the battery fully charged and ready to provide conditioned back-up current that properly powers a load, as shown and taught by Mengelt.

With regards to claim 19, Mengelt in view of Fisher does not specifically discuss the step of automatically controlling comprises coupling the second output signal to the output of the device when the state of the input signal is absent.

However, the step of automatically coupling the second output signal to the output of a devices that correspond to back-up power systems when the state of the input signal is absent is well known and of common knowledge in the art as evidenced by Mengelt (see col. 7, lines 12-25 and 32-59 of Mengelt, wherein the AC current signal from the main AC power system represents the input signal).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the automatically controlling step of Mengelt in view of Fisher comprise coupling the second output signal to the output of the device when the state of the input signal is absent for the purpose of providing uninterruptible power to a load by supplying back-up power from the battery in the event that main power supply is not present, as shown and taught by Mengelt.

With regards to claim 22, Mengelt discloses the input signal being an alternating current AC signal, and the output of the device being an alternating current AC signal (see fig. 3 as well as col. 6, lines 47-50 and col. 7, lines 8-25, which discuss powering the load with AC from the device/back-up power system 40).

Claims 3, 12 and 20-21 lack an inventive step under PCT Article 33(3) as being obvious over Mengelt in view of Fisher, as applied to claims 2, 10 and 16 above, and further in view of Bavaro.

With regards to claims 3 and 12, Mengelt does not specifically discuss the transformer circuitry comprises a step-down transformer that reduces a voltage of the input signal.

However, the use of step-down transformers in electrical devices to lower the voltage from a main AC power source to a lower, desired voltage that is suitable for powering a specified load is notoriously well known and of common knowledge in the art as evidenced by Bavaro (see pg. 9, the first three lines of the last paragraph of Bavaro).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the device of Mengelt in view of Fisher incorporate a well known step-down transformer, as shown by Bavaro, into the transformer circuitry for the purpose of lowering the voltage from the main AC supply to a lower, desired voltage that is suitable for properly powering the load.

With regards to claim 20, Mengelt does not specifically discuss that the transforming step comprises reducing a voltage of the input signal.

However, the step of reducing voltages of input signals in electrical devices from a main AC power supply for the purpose of properly powering load that requires lower voltages in order to operate as designed is notoriously well known and of common knowledge in the art as evidenced by Bavaro (see pg. 9, the first three lines of the last paragraph of Bavaro).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the transforming step of Mengelt in view of Fisher comprise reducing a voltage of the input signal for the purpose of properly powering a load that requires a lower voltage to operate as designed, as shown and taught by Bavaro.

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITYInternational application No.  
PCT/US2009/055559**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

With regards to claim 21, Mengelt does not specifically discuss that the transforming step comprises regulating the voltage of the input signal.

However, the step of regulating the voltages of input signals in electrical devices for the purpose of conditioning the current to match with charging circuitry and loads in order to properly power the charging circuitry and loads, respectively, is well known and of common knowledge in the art as taught by Fisher (see col. 4, lines 32-35 of Fisher, for example).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the transforming step of Mengelt in view of Fisher comprise the step of regulating the voltage of input signals for the purpose of conditioning the current to match with the charging circuitry and a load in order to properly power the charging circuitry and the load, respectively, as taught by Fisher.

Claims 9 and 15 lack an inventive step under PCT Article 33(3) as being obvious over Mengelt in view of Fisher, as applied to claims 1 and 10 above, and further in view of Brewer et al., hereinafter referred to as Brewer.

With regards to claims 9 and 15, Mengelt in view of Fisher does not specifically discuss the device output being a direct current DC signal. However, the use of direct current DC signals as the output of power systems for the purpose of supplying DC powered loads with DC signals is well known and of common knowledge in the art as evidenced by Brewer (see fig. 1 as well as col. 4, lines 13-32 of Brewer, for example).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to have the device output of Mengelt in view of Fisher be a direct current DC signal for the purpose of supply DC signals to devices that are powered by DC current, as shown and taught by Brewer.

Claims 1-22 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

From the INTERNATIONAL SEARCHING AUTHORITY

To: RICHARD GREGORY  
 GREGORY & MARTENSEN LLP  
 2018 BISSONNET STREET  
 HOUSTON, TX 77005

**PCT**

NOTIFICATION OF TRANSMITTAL OF  
 THE INTERNATIONAL SEARCH REPORT AND  
 THE WRITTEN OPINION OF THE INTERNATIONAL  
 SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing  
 (day/month/year) **30 DEC 2010**

Applicant's or agent's file reference <b>ICON.P014WO</b>	<b>FOR FURTHER ACTION</b> See paragraphs 1 and 4 below
International application No. <b>PCT/US2010/050585</b>	International filing date (day/month/year) <b>28 September 2010.</b>
Applicant <b>ICONTROL NETWORKS, INC.</b>	

1.  The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

**Filing of amendments and statement under Article 19:**

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70

For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 – 9.011.

2.  The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3.  With regard to any protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

**4. Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see [www.wipo.int/pct/en/texts/time\\_limits.html](http://www.wipo.int/pct/en/texts/time_limits.html) and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the ISA/  
 Mail Stop PCT, Attn: ISA/US  
 Commissioner for Patents  
 P.O. Box 1450, Alexandria, Virginia 22313-1450  
 Facsimile No. 571-273-3201

Authorized officer  
**Blaine R. Copenheaver**  
 PCT Helpdesk: 571-272-4300  
 Telephone No. PCT OSP: 571-272-7774

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ICON.P014WO	<b>FOR FURTHER ACTION</b> see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US2010/050585	International filing date ( <i>day/month/year</i> ) 28 September 2010	(Earliest) Priority Date ( <i>day/month/year</i> ) 28 September 2009
Applicant ICONTROL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

## 1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- the international application in the language in which it was filed.  
 a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b.  This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c.  With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2.  Certain claims were found unsearchable (see Box No. II).

3.  Unity of invention is lacking (see Box No. III).

4. With regard to the title,

- the text is approved as submitted by the applicant.  
 the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- the text is approved as submitted by the applicant.  
 the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. \_\_\_\_\_  
 as suggested by the applicant.  
 as selected by this Authority, because the applicant failed to suggest a figure.  
 as selected by this Authority, because this figure better characterizes the invention.
- b.  none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US2010/050585

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC(8) - G06F 15/16 (2010.01) USPC - 709/219 According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC(8) - G06B 1/08; G06F 13/00; G06F 15/16 (2010.01) USPC - 709/219, 220, 223 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Google Patent, Google Scholar, PatBase		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009/0070436 A1 (DAWES et al) 12 March 2009 (12.03.2009) entire document	1-96
Y	US 6,789,147 B1 (KESSLER et al) 07 September 2004 (07.09.2004) entire document	1-96
Y	US 6,052,052 A (DELMONACO) 18 April 2000 (18.04.2000) entire document	3-5, 54-56
A	US 2005/0216580 A1 (RAJI et al) 29 September 2005 (29.09.2005) entire document	1-96
<input type="checkbox"/> Further documents are listed in the continuation of Box C.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 16 December 2010		Date of mailing of the international search report <b>30 DEC 2010</b>
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201		Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

PATENT COOPERATION TREATY

From the  
INTERNATIONAL SEARCHING AUTHORITY

To: RICHARD GREGORY  
GREGORY & MARTENSEN LLP  
2018 BISSONNET STREET  
HOUSTON, TX 77005

PCT

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing  
(day/month/year) 30 DEC 2010

Applicant's or agent's file reference  
ICON.P014WO

FOR FURTHER ACTION

See paragraph 2 below

International application No.  
PCT/US2010/050585

International filing date (day/month/year)  
28 September 2010

Priority date (day/month/year)  
28 September 2009

International Patent Classification (IPC) or both national classification and IPC  
IPC(8) - G06F 15/16 (2010.01)  
USPC - 709/219

Applicant ICONTROL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion  16 December 2010	Authorized officer:  Blaine R. Copenheaver  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--	---

Form PCT/ISA/237 (cover sheet) (July 2009)

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITYInternational application No.  
PCT/US2010/050585

## Box No. I Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:
- the international application in the language in which it was filed.
- a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2.  This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
- a. (means)
- on paper
- in electronic form
- b. (time)
- in the international application as filed
- together with the international application in electronic form
- subsequently to this Authority for the purposes of search
4.  In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2010/050585

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**1. Statement**

Novelty (N)	Claims	<u>1-96</u>	YES
	Claims	<u>None</u>	NO
Inventive step (IS)	Claims	<u>None</u>	YES
	Claims	<u>1-96</u>	NO
Industrial applicability (IA)	Claims	<u>1-96</u>	YES
	Claims	<u>None</u>	NO

**2. Citations and explanations:**

Claim1-2, 6-53, and 57-96 lack an inventive step under PCT Article 33(3) as being obvious over Dawes et al., hereinafter referred to as Dawes, in view of Kessler et al., hereinafter referred to as Kessler.

Regarding claims 1 and 52, Dawes disclose a system (abstract, integrated security system) and method (para. 0017, method) comprising: a security processor (104, connect server; para. 0124, processor within security system), wherein the security processor (104; para. 0312-0313, processor) is coupled to a security system at a premise (110; para. 0065, processor based system that manages home security; para. 0042, premise devices and security system), the security system (110) including security system components (para. 0045, includes components); and an interactive security system (102, gateway (attached to touch screen); fig. 12, 1202) at the premise coupled to the security processor and to a remote network (para. 0196, touch screen with processor at remote location; para. 0315; para. 0373), wherein the security processor (104) controls communications between the security system (110) and the interactive security system (102; 1202; para. 0441, processor provides for transfer of data collected by the system), the interactive security system (102; 1202) generating in the premise a sub network comprising network components (para. 0128, gateway at premise generates a sub-network, comprising devices), wherein the interactive security system (102; 1202; para. 0131, integrated security system) controls communications between the security system components (1216, 1226), the network components (fig. 12, sensors 1-3), and the remote network (fig. 12, security panels 1-n) (para. 0190), but is silent on the particulars of a security co-processor. However, Kessler in discussing an interface for a security coprocessor (title) disclose a security coprocessor (212; col. 3, ln. 1, coprocessor). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the coprocessor of Kessler with the system and method of Dawes for the purpose of increasing the efficiency of a system and its host processor (col. 10, ln. 26-29 – Kessler).

Regarding claims 2 and 53, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the security system (110) supplies power (para. 0207, provide power), but is silent on the particulars of a security coprocessor.

However, Kessler in discussing an interface for a security coprocessor (title) disclose a security coprocessor (212; col. 3, ln. 1, coprocessor). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the coprocessor of Kessler with the system and method of Dawes for the purpose of increasing the efficiency of a system and its host processor (col. 10, ln. 26-29 – Kessler).

Regarding claims 6 and 65, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the interactive security system (102) automatically establishes a coupling with the security system (110) and forms a security network by electronically integrating communications and functions of the network components and the security system components (para. 0235, automate installation and sensor enrollment; para. 0244-0245; para. 0274, automatically detects sensor addition and adds to the integrated system; para. 0333).

Regarding claims 7 and 66, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the interactive security system (102) comprises an interface for control of the security system components and the network components (para. 0131, touch screen provides interface to devices and sensors).

Regarding claims 8 and 67, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, wherein the interactive security system (102) provides access to the communications and the functions of the security network (110) (108, internet, cellular network) via remote client devices (120; para. 0059, remote client devices).

Regarding claims 9 and 68, Dawes in view of Kessler disclose the system and method of claims 8 and 67, respectively, Dawes further disclose wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices (para. 0059, client devices 120, include PCs, mobile phones and PDAs).



**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2010/050585

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claims 10 and 69, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the interactive security system automatically discovers the security system components (para. 0046, automatically discovers system components).

Regarding claims 11 and 70, Dawes in view of Kessler disclose the system and method of claims 10 and 69, respectively, Dawes further disclose wherein the interactive security system uses protocols of the security system to discover the security system components (para. 0046, supports various protocols; para. 0048, protocols).

Regarding claims 12 and 71, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the interactive security system automatically establishes a coupling with the security system components (para. 0200 automatically couples or connects to CMS to configure sensors).

Regarding claims 13 and 72, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the interactive security system (102) is coupled to the central monitoring station (199) via the remote network that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location (para. 0423).

Regarding claims 14 and 73, Dawes in view of Kessler disclose the system and method of claims 13 and 72, respectively, Dawes further disclose wherein the interactive security system transmits event data of at least one of the security system components and the network components to the central monitoring station (199, CMS) over the remote network (para. 0424, transmit event data of the security system components over the secondary (remote) communication link).

Regarding claims 15 and 74, Dawes in view of Kessler disclose the system and method of claims 14 and 73, respectively, Dawes further disclose wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components (para. 0425; para. 0429).

Regarding claims 16 and 75, Dawes in view of Kessler disclose the system and method of claims 14 and 73, respectively, Dawes further disclose wherein the event data comprises changes in device states of the network components, data of the network components, and data received by the network components (para. 0438).

Regarding claims 17 and 76, Dawes in view of Kessler disclose the system and method of claims 13 and 72, respectively, Dawes further disclose wherein the remote network includes a broadband coupling (para. 0470, broadband coupling).

Regarding claims 18 and 77, Dawes in view of Kessler disclose the system and method of claims 13 and 72, respectively, Dawes further disclose wherein the remote network includes a General Packet Radio Service (GPRS) coupling (para. 0050-0052, GPRS network).

Regarding claims 19 and 78, Dawes in view of Kessler disclose the system and method of claims 13 and 72, respectively, Dawes further disclose wherein the interactive security system transmits messages comprising event data of at least one of the security system components and the network components to remote client devices over the remote network (para. 0428, transmits over secondary (remote) communication link).

Regarding claims 20 and 79, Dawes in view of Kessler disclose the system and method of claims 19 and 78, respectively, Dawes further disclose wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components (para. 0425; para. 0429).

Regarding claims 21 and 80, Dawes in view of Kessler disclose the system and method of claims 19 and 78, respectively, Dawes further disclose wherein the event data comprises changes in device states of the network components, data of the network components, and data received by the network components (para. 0438).

Regarding claims 22 and 81, Dawes in view of Kessler disclose the system and method of claims 13 and 72, respectively, Dawes further disclose wherein the interactive security system receives control data for control of at least one of the security system components and the network components from remote client devices via the secondary communication link (para. 0430; para. 0494).

Regarding claims 23 and 82, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the interactive security system automatically discovers the network components (para. 0432).

Regarding claims 24 and 83, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the interactive security system automatically installs the network devices in the security network (para. 0433).

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.  
PCT/US2010/050585

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.  
Continuation of:

Regarding claims 25 and 84, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the interactive security system receives control data for control of the network devices from remote client devices (para. 0437, gateway system (interactive security system)).

Regarding claims 26 and 85, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the network component is an Internet Protocol device (para. 0365, internet protocol device).

Regarding claims 27 and 85, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the network component is a camera (para. 0074, camera).

Regarding claim 28 and 85, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the network component is a touch screen (para. 0127, touch screen; para. 0131, touch screen).

Regarding claims 29 and 85, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the network component is a device controller that controls an attached device (para. 0476).

Regarding claims 30 and 85, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the network component is a sensor (para. 0045, sensor).

Regarding claims 31 and 86, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the security system components include one or more of sensors, cameras, input/output (VO) devices, and accessory controllers (para. 0046, components such as sensors; para. 0074, components or devices such as sensors, cameras, panels, etc.).

Regarding claims 32 and 57, Dawes in view of Kessler disclose the system and method of claims 1 and 52, Dawes further disclose comprising a touch screen (para. 0127, touch screen), wherein the interactive security system is a component of the touch screen (para. 0127, interactive touch screen).

Regarding claims 33 and 58, Dawes in view of Kessler disclose the system and method of claims 32 and 57, respectively, Dawes further disclose comprising segregating via the touch screen data traffic between the security system, the sub network and the remote network, the segregating comprising using separate security and privacy policies for components coupled to the security system, the sub network and the remote network (para. 0128-0129).

Regarding claims 34 and 59, Dawes in view of Kessler disclose the system and method of claims 32 and 57, respectively, Dawes further disclose comprising simultaneously presenting a plurality of interfaces on the touch screen, the plurality of interfaces including a security interface for accessing and controlling the security system and the security system components (para. 0315; para. 0373; para. 0533), wherein the security system interface is ever present in a dedicated region of the touch screen (para. 0136, dedicated region).

Regarding claims 35 and 60, Dawes in view of Kessler disclose the system and method of claims 34 and 59, respectively, Dawes further disclose wherein the plurality of interfaces (para. 0375, plurality of interfaces) include a sub network interface for accessing and controlling the network components (para. 0128-0129, sub network transfer data and information between sub network; para. 0139; para. 0179-0181), and a remote network interface for accessing the remote network (para. 0373, transfer data within remote network; para. 0375).

Regarding claims 36 and 61, Dawes in view of Kessler disclose the system and method of claims 34 and 59, respectively, Dawes further disclose comprising enabling interaction among at least one of the security system components (para. 0449) and the network components (fig. 5, items 255-257) via the plurality of interfaces (para. 0375; para. 0048, support devices via interfaces).

Regarding claims 37 and 62, Dawes in view of Kessler disclose the system and method of claim 32 and 57, respectively, Dawes further disclose comprising electronically retrieving content via the touch screen (208) and the remote network (para. 0376), and integrating the content in at least one of the touch screen, the security system, the security system components, and the network components, wherein the content includes a software application and interactive content in the form of internet widgets (para. 0068-0069, widgets; fig. 8, displays internet widgets).

Regarding claims 38 and 63, Dawes in view of Kessler disclose the system and method of claims 32 and 57, respectively, Dawes further disclose comprising an application engine coupled to the touch screen (para. 0143; para. 0388), wherein the application engine controls a plurality of applications (para. 0144, controls a first and second application), wherein the plurality of applications includes a resident application that manages interactions between the plurality of applications (para. 0144, first application is the premise (resident) application, the second applications include all other applications).

Regarding claims 39 and 64, Dawes in view of Kessler disclose the system and method of claims 38 and 63, respectively, Dawes further disclose wherein the resident application determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority (para. 0356, priority of applications; para. 0519).

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.  
PCT/US2010/050585

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.  
Continuation of:

Regarding claims 40 and 87, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose comprising a security server at a second location different from the first location, wherein security server is coupled to the interactive security system (para. 0376, coupled to the gateway (interactive security system)).

Regarding claims 41 and 88, Dawes in view of Kessler disclose the system and method of claims 40 and 87, respectively, Dawes further disclose wherein the interactive security system (102) control communications between the network devices (120), the security system components (fig. 2, 208), and the security server (104).

Regarding claims 42 and 89, Dawes in view of Kessler disclose the system and method of claims 40 and 87, respectively, Dawes further disclose wherein the security server (104) performs creation, modification, deletion and configuration of at least one of the security components and the network components (para. 0079).

Regarding claims 43 and 90, Dawes in view of Kessler disclose the system and method of claims 40 and 87, respectively, Dawes further disclose wherein the security server (104) creates automations, schedules and notification rules associated with at least one of the security components and the network components (para. 0079, Network Manager 222 is part of the server 104).

Regarding claims 44 and 91, Dawes in view of Kessler disclose the system and method of claims 40 and 87, respectively, Dawes further disclose wherein the security server (104) manages access to current and logged state data for at least one of the security components and the network components (para. 0080-0081, Data Manager 224 is part of the server 104).

Regarding claims 45 and 92, Dawes in view of Kessler disclose the system and method of claims 40 and 87, respectively, Dawes further disclose wherein the security server (104) manages access to current and logged state data for couplings between the interactive security system and at least one of the security components and the network components (para. 0081).

Regarding claims 46 and 93, Dawes in view of Kessler disclose the system and method of claims 40 and 87, respectively, Dawes further disclose wherein the security server (104) manages communications with at least one of the security components (260, device connect) and the network components (para. 0074, server provides management of objects associated with integrated security system (components)).

Regarding claims 47 and 94, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the security server (104) creates, modifies and terminates users corresponding to the security system (para. 0078, Registry Manager 220 is part of the server 104).

Regarding claims 48 and 95, Dawes in view of Kessler disclose the system and method of claims 1 and 52, respectively, Dawes further disclose wherein the security server (104) generates and transfers notifications to remote client devices (120, client types), the notifications comprising event data (para. 0042, notifications; para. 0070; para. 0075-0076; para. 0205).

Regarding claims 49 and 96, Dawes in view of Kessler disclose the system and method of claims 48 and 95, respectively, Dawes further disclose wherein the notifications include one or more of short message service messages and electronic mail messages (para. 0046, email and SMS alerts; para. 0084).

Regarding claim 50, Dawes disclose a system (abstract, integrated security system) comprising: a security processor (104, connect server; para. 0124, processor within security system), wherein the security processor (104; para. 0312-0313, processor) is coupled to a security system at a premise (110; para. 0065, processor based system that manages home security; para. 0042, premise devices and security system), the security system (110) including security system components (para. 0045, includes components); and a touch screen (fig. 2, item 208; fig. 1, depicts touch screen pad) comprising an interactive security system (102, gateway (attached to touch screen); fig. 12, 1202) coupled to the security processor (104; para. 0312-0313) and to a remote network (para. 0196, touch screen with processor at remote location; para. 0315; para. 0373), wherein the security processor (104) controls communications between the security system (110) and the touch screen (208; fig. 1, depicts touch screen pad), the touch screen generating in the premise a sub network comprising network components (para. 0128, gateway at premise generates a sub-network, comprising devices), wherein the touch screen (102, touch screen connected to gateway; 1202; para. 0131, integrated security system) controls communications between the security system components (1216, 1226), the network components (fig. 12, sensors 1-3), and the remote network (fig. 12, security panels 1-n) (para. 0190), but is silent on the particulars of a security co-processor.

However, Kessler in discussing an interface for a security coprocessor (title) disclose a security coprocessor (212; col. 3, in. 1, coprocessor). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the coprocessor of Kessler with the system of Dawes for the purpose of increasing the efficiency of a system and its host processor (col. 10, in. 26-29 – Kessler).

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US2010/050585

## Supplemental Box

In case the space in any of the preceding boxes is not sufficient.  
Continuation of:

Regarding claim 51, Dawes disclose a system (abstract, integrated security system) comprising: a security processor (104, connect server; para. 0124, processor within security system), wherein the security processor (104; para. 0312-0313, processor) is coupled to a security system at a premise (110; para. 0065, processor based system that manages home security; para. 0042, premise devices and security system), the security system (110) including security system components (para. 0045, includes components and coupled to a central monitoring station (199) via a first communication link (para. 0423, primary (first) communication link); and an interactive security system (102, gateway (attached to touch screen); fig. 12, 1202) at the premise coupled to the security processor and to a remote network (para. 0196, touch screen with processor at remote location; para. 0315; para. 0373) via a second communication link different from the first communication link (para. 0423, secondary communication link which is different than primary communication link), wherein the security processor (104) controls communications between the security system (110) and the interactive security system (102; 1202; para. 0441, processor provides for transfer of data collected by the system), the interactive security system (102; 1202) generating in the premise a sub network comprising network components (para. 0128, gateway at premise generates a sub-network, comprising devices), wherein the interactive security system (102; 1202; para. 0131, integrated security system) controls communications between the security system components (1216, 1226), the network components (fig. 12, sensors 1-3), and the remote network (fig. 12, security panels 1-n) (para. 0190), but is silent on the particulars of a security co-processor.

However, Kessler in discussing an interface for a security coprocessor (title) disclose a security coprocessor (212; col. 3, ln. 1, coprocessor). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the coprocessor of Kessler with the system of Dawes for the purpose of increasing the efficiency of a system and its host processor (col. 10, ln. 26-29 – Kessler).

Claims 3-5 and 54-56 lack an inventive step under PCT Article 33(3) as being obvious over Dawes in view of Kessler, and further in view of Delmonaco.

Regarding claims 3 and 54, Dawes in view of Kessler disclose the system and method of claims 2 and 53, respectively, Dawes further disclose a security system (110), and the interactive security system (102), but is silent on a power switch coupled to the systems, and the security coprocessor.

However, Kessler in discussing an interface for a security coprocessor (title) disclose a security coprocessor (212; col. 3, ln. 1, coprocessor). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the coprocessor of Kessler with the system and method of Dawes for the purpose of increasing the efficiency of a system and its host processor (col. 10, ln. 26-29 – Kessler).

Moreover, the particulars of a power switch are notoriously well known in the art as evidenced by Delmonaco. Delmonaco in discussing a portable alarm system (title) disclose a power switch (8, power switch). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the aforementioned improvements of Delmonaco with the system and method of Dawes for the purpose of providing a flexible supply interface (col. 4, lns. 11-14 – Delmonaco).

Regarding claims 4 and 55, Dawes in view of Kessler in further view of Delmonaco disclose the system and method of claims 3 and 54, respectively, Dawes further disclose wherein the security system (110) supplies power to the interactive security system (102, gateway connected to touch screen), but is silent on the particulars of a power switch.

However, the particulars of a power switch are notoriously well known in the art as evidenced by Delmonaco. Delmonaco in discussing a portable alarm system (title) disclose a power switch (8, power switch). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the aforementioned improvements of Delmonaco with the system and method of Dawes for the purpose of providing a flexible supply interface (col. 4, lns. 11-14 – Delmonaco).

Regarding claims 5 and 56, Dawes in view of Kessler in further view of Delmonaco disclose the system and method of claims 4 and 55, respectively, Dawes further disclose wherein the security system (110) signals the security processor of an external power failure (para. 0164, external power failure causes the system to switch to battery; para. 0173), but is silent on the particulars of a security coprocessor, and the security coprocessor signals the power switch to terminate power to the interactive security system.

However, Kessler in discussing an interface for a security coprocessor (title) disclose a security coprocessor (212; col. 3, ln. 1, coprocessor). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the coprocessor of Kessler with the system and method of Dawes for the purpose of increasing the efficiency of a system and its host processor (col. 10, ln. 26-29 – Kessler).

Moreover, the particulars of a power switch terminating power are notoriously well known in the art as evidenced by Delmonaco. Delmonaco in discussing a portable alarm system (title) disclose a power switch (8, power switch) that terminates power (col. 6, lns. 8-10, disconnect all power circuits). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the aforementioned improvements of Delmonaco with the system and method of Dawes for the purpose of providing a flexible supply interface (col. 4, lns. 11-14 – Delmonaco).

Claims 1-96 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:  
 RICHARD L. GREGORY JR.  
 GREGORY & MARTENSEN LLP  
 2018 BISSONNET STREET  
 HOUSTON, TX 77005

PCT

NOTIFICATION OF TRANSMITTAL OF  
 THE INTERNATIONAL SEARCH REPORT AND  
 THE WRITTEN OPINION OF THE INTERNATIONAL  
 SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing  
 (day/month/year) **02 MAR 2011**

Applicant's or agent's file reference ICON.P015WO	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US 10/57674	International filing date (day/month/year) 22 November 2010 (22.11.2010)
Applicant <b>ICONTROL NETWORKS, INC.</b>	

- The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.  
**Filing of amendments and statement under Article 19:**  
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):  
**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.  
**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70  
**For more detailed instructions, see PCT Applicant's Guide, International Phase, paragraphs 9.004 – 9.011.**
- The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
- With regard to any protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
  - the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.
  - no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.
- 4. Reminders**  
 The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.  
 Shortly after the expiration of 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).  
 Within 19 months from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later); otherwise, the applicant must, within 20 months from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.  
 In respect of other designated Offices, the time limit of 30 months (or later) will apply even if no demand is filed within 19 months.  
 For details about the applicable time limits, Office by Office, see [www.wipo.int/pct/en/texts/time\\_limits.html](http://www.wipo.int/pct/en/texts/time_limits.html) and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer  <b>Lee W. Young</b> PCT Helpdesk: 571-272-4300 Telephone No. PCT OSP: 571-272-7774
---	--

Form PCT/ISA/220 (July 2010)

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ICON.P015WO	<b>FOR FURTHER ACTION</b> see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US 10/57674	International filing date ( <i>day/month/year</i> ) 22 November 2010 (22.11.2010)	(Earliest) Priority Date ( <i>day/month/year</i> ) 20 November 2009 (20.11.2009)
Applicant ICONTROL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

## 1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- the international application in the language in which it was filed.  
 a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b.  This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c.  With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2.  Certain claims were found unsearchable (see Box No. II).

3.  Unity of invention is lacking (see Box No. III).

4. With regard to the title,

- the text is approved as submitted by the applicant.  
 the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- the text is approved as submitted by the applicant.  
 the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. 7E  
 as suggested by the applicant.  
 as selected by this Authority, because the applicant failed to suggest a figure.  
 as selected by this Authority, because this figure better characterizes the invention.
- b.  none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (July 2009)

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 10/57674

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC(8) - G06F 3/00 (2011.01) USPC - 715/700 According to International Patent Classification (IPC) or to both national classification and IPC																						
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC(8): G06F 3/00 (2011.01) USPC: 715/700 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched IPC(8): G06F 3/00 (2011.01) USPC: 715/700, 701, 702, 866; 717/168, 174; 709/223, 224; 705/1.1, 325, 412 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) pubWEST(USPT,PGPB,EPAB,JPAB,USOCR); Google(Web); Search terms used: remote wireless monitor alert premise site automation touchscreen management controlling home energy temperature HVAC health download update application module z-wave cellular IP security network server host portal widget toolbar gadget API abstraction interface linking priority																						
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>																						
<table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X -- Y</td> <td>US 2005/0125083 A1 (Kiko) 09 June 2005 (09.06.2005), entire document especially Fig. 1-1 to 1-4, 2-f to 2-i, 17a, 17b; para [0083], [0097]-[0099], [0119], [0126], [0128], [0130], [0136]-[0143], [0149], [0151], [0156], [0158], [0165], [0169], [0175], [0180], [0239], [0242], [0244], [0247]</td> <td>1-3, 5-43, 45-52, 55-93, 96, 97 4, 44, 53, 54, 94, 95</td> </tr> <tr> <td>Y</td> <td>US 2008/0084296 A1 (Kutzik et al.) 10 April 2008 (10.04.2008), entire document especially para [0026], [0029], [0175], [0179]</td> <td>4</td> </tr> <tr> <td>Y</td> <td>US 2009/0165114 A1 (Baurm et al.) 25 June 2009 (25.06.2009), entire document especially para [0072], [0138], [0154]</td> <td>44, 53, 54, 94, 95</td> </tr> <tr> <td>A</td> <td>US 2005/0222820 A1 (Chung) 06 October 2005 (06.10.2005), entire document</td> <td>1-97</td> </tr> <tr> <td>A</td> <td>US 2001/0034754 A1 (Etwahab et al.) 25 October 2001 (25.10.2001), entire document</td> <td>1-97</td> </tr> <tr> <td>A</td> <td>US 2006/0009863 A1 (Lingemann) 12 January 2006 (12.01.2006), entire document</td> <td>1-97</td> </tr> </tbody> </table>	Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X -- Y	US 2005/0125083 A1 (Kiko) 09 June 2005 (09.06.2005), entire document especially Fig. 1-1 to 1-4, 2-f to 2-i, 17a, 17b; para [0083], [0097]-[0099], [0119], [0126], [0128], [0130], [0136]-[0143], [0149], [0151], [0156], [0158], [0165], [0169], [0175], [0180], [0239], [0242], [0244], [0247]	1-3, 5-43, 45-52, 55-93, 96, 97 4, 44, 53, 54, 94, 95	Y	US 2008/0084296 A1 (Kutzik et al.) 10 April 2008 (10.04.2008), entire document especially para [0026], [0029], [0175], [0179]	4	Y	US 2009/0165114 A1 (Baurm et al.) 25 June 2009 (25.06.2009), entire document especially para [0072], [0138], [0154]	44, 53, 54, 94, 95	A	US 2005/0222820 A1 (Chung) 06 October 2005 (06.10.2005), entire document	1-97	A	US 2001/0034754 A1 (Etwahab et al.) 25 October 2001 (25.10.2001), entire document	1-97	A	US 2006/0009863 A1 (Lingemann) 12 January 2006 (12.01.2006), entire document	1-97	<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/>
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																				
X -- Y	US 2005/0125083 A1 (Kiko) 09 June 2005 (09.06.2005), entire document especially Fig. 1-1 to 1-4, 2-f to 2-i, 17a, 17b; para [0083], [0097]-[0099], [0119], [0126], [0128], [0130], [0136]-[0143], [0149], [0151], [0156], [0158], [0165], [0169], [0175], [0180], [0239], [0242], [0244], [0247]	1-3, 5-43, 45-52, 55-93, 96, 97 4, 44, 53, 54, 94, 95																				
Y	US 2008/0084296 A1 (Kutzik et al.) 10 April 2008 (10.04.2008), entire document especially para [0026], [0029], [0175], [0179]	4																				
Y	US 2009/0165114 A1 (Baurm et al.) 25 June 2009 (25.06.2009), entire document especially para [0072], [0138], [0154]	44, 53, 54, 94, 95																				
A	US 2005/0222820 A1 (Chung) 06 October 2005 (06.10.2005), entire document	1-97																				
A	US 2001/0034754 A1 (Etwahab et al.) 25 October 2001 (25.10.2001), entire document	1-97																				
A	US 2006/0009863 A1 (Lingemann) 12 January 2006 (12.01.2006), entire document	1-97																				
<table border="1"> <thead> <tr> <th colspan="2">* Special categories of cited documents:</th> </tr> </thead> <tbody> <tr> <td>"A" document defining the general state of the art which is not considered to be of particular relevance</td> <td>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</td> </tr> <tr> <td>"E" earlier application or patent but published on or after the international filing date</td> <td>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</td> </tr> <tr> <td>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</td> <td>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</td> </tr> <tr> <td>"O" document referring to an oral disclosure, use, exhibition or other means</td> <td>"&amp;" document member of the same patent family</td> </tr> <tr> <td>"P" document published prior to the international filing date but later than the priority date claimed</td> <td></td> </tr> </tbody> </table>		* Special categories of cited documents:		"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family	"P" document published prior to the international filing date but later than the priority date claimed										
* Special categories of cited documents:																						
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention																					
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone																					
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art																					
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family																					
"P" document published prior to the international filing date but later than the priority date claimed																						
Date of the actual completion of the international search 08 February 2011 (08.02.2011)	Date of mailing of the international search report 02 MAR 2011																					
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774																					

Form PCT/ISA/210 (second sheet) (July 2009)

PATENT COOPERATION TREATY

From the  
INTERNATIONAL SEARCHING AUTHORITY

To: RICHARD L. GREGORY JR.  
GREGORY & MARTENSEN LLP  
2018 BISSONNET STREET  
HOUSTON, TX 77005

PCT

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing  
(day/month/year) 02 MAR 2011

Applicant's or agent's file reference  
ICON.P015WO

FOR FURTHER ACTION  
See paragraph 2 below

International application No.

PCT/US 10/57674

International filing date (day/month/year)

22 November 2010 (22.11.2010)

Priority date (day/month/year)

20 November 2009 (20.11.2009)

International Patent Classification (IPC) or both national classification and IPC

IPC(8) - G06F 3/00 (2011.01)

USPC - 715/700

Applicant ICON CONTROL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion  08 February 2011 (08.02.2011)	Authorized officer:  Lee W. Young  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	---	--

Form PCT/ISA/237 (cover sheet) (July 2009)



WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITYInternational application No.  
PCT/US 10/57674

Box No. 1 Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:
- the international application in the language in which it was filed.
- a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2.  This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a)).
3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
- a. (means)
- on paper
- in electronic form
- b. (time)
- in the international application as filed
- together with the international application in electronic form
- subsequently to this Authority for the purposes of search
4.  In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 10/57674

<b>Box No. V</b>	<b>Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</b>		
<b>1. Statement</b>			
Novelty (N)	Claims	<u>4, 44, 53, 54, 94, 95</u>	YES
	Claims	<u>1-3, 5-43, 45-52, 55-93, 96, 97</u>	NO
Inventive step (IS)	Claims	<u>NONE</u>	YES
	Claims	<u>1-97</u>	NO
Industrial applicability (IA)	Claims	<u>1-97</u>	YES
	Claims	<u>NONE</u>	NO
<b>2. Citations and explanations:</b>			
Claims 1-3, 5-43, 45-52, 55-93, 96 and 97 lack novelty under PCT Article 33(2) as being anticipated by US 2005/0125083 A1 (Kiko).			
Regarding claim 1, Kiko teaches a device comprising: a housing at a premise, wherein the housing contains a touchscreen display coupled to a processor (Fig. 1-1 to 1-4; Fig. 17a, 17b; a touch panel server controller containing / housing connectors and modules; para [0140]-[0143], [0151]), wherein the processor is coupled to at least one remote network (para [0128], [0136]); an application engine coupled to the processor, wherein the application engine controls a plurality of applications executing under the processor (a plurality of automation applications are hosted; para [0097], [0099], [0149]); a receptacle in the housing, wherein the receptacle includes a connector coupled to the processor (para [0139], [0140], [0151]); and a plurality of modules each having a form-factor for connecting to the receptacle, wherein each module of the plurality of modules includes components corresponding to a function of a plurality of functions (Fig. 2f to 2i; para [0151], [0139], [0140]), wherein the components of each module are coupled to the processor and the application engine via the connection of the module to the receptacle and the components dynamically reconfigure the touchscreen to operate according to the function of the module (Fig. 1-1 to 1-4; para [0139]-[0142], [0180]).			
Regarding claim 61, Kiko teaches a method comprising: containing in a housing at a premise a touchscreen display coupled to a processor (Fig. 1-1 to 1-4; Fig. 17a, 17b; a touch panel server controller containing / housing connectors and modules; para [0140]-[0143], [0151]), wherein the housing comprises a receptacle that includes a connector coupled to the processor (Fig. 1-1 to 1-4; para [0140], [0141], [0165]); coupling the processor to at least one remote network (para [0128], [0136]); controlling a plurality of applications executing under the processor with an application engine (a plurality of automation applications are hosted; para [0097], [0099], [0149]); and receiving at the receptacle individual ones of a plurality of modules, wherein each module of the plurality of modules includes components corresponding to a function of a plurality of functions (para [0139], [0140], [0151]), wherein the components of each module are coupled to the processor and the application engine via the connection of the module to the receptacle and the components dynamically reconfigure the touchscreen to operate according to the function of the module (Fig. 1-1 to 1-4; para [0139]-[0142], [0180]).			
Regarding claims 2, 3, 5 and 62, Kiko teaches that the plurality of modules includes at least one of an energy management module for energy management on the premise (para [0097], [0119], [0156], [0158], [0175], [0180]), a thermostat module for temperature management on the premise (para [0097], [0119], [0156], [0158], [0175], [0180]), a remote health monitoring module for human health monitoring on the premise, and a monitoring module for human monitoring on the premise (para [0097], [0119], [0156], [0158], [0175], [0180]).			
Regarding claims 6 and 63, Kiko teaches presenting a plurality of interfaces to a user via the touchscreen, wherein the plurality of interfaces are coupled to the processor and correspond to the plurality of modules (remote monitoring of a plurality of automation functions via GUI / menus; para [0142], [0143], [0180], [0247]).			
Regarding claims 7 and 64, Kiko teaches that an interface of the plurality of interfaces corresponds to the function of the module (remote monitoring of a plurality of automation functions via GUI / menus; para [0142], [0143], [0180], [0247]).			
Regarding claims 8, 9, 10 and 65, Kiko teaches modular applications that present the plurality of interfaces on the touchscreen, wherein the modular applications are downloaded via the at least one remote network, wherein the processor dynamically updates the plurality of interfaces using the modular applications (server / Internet downloadable applications and upgrades; para [0083], [0140]).			
Regarding claims 11 and 66, Kiko teaches that the plurality of interfaces provides interactivity with a plurality of devices located at the premise (para [0119], [0143], [0180]).			
Regarding claims 12 and 67, Kiko teaches that a device of the plurality of devices is a radio frequency (RF) device (para [0242]).			
Regarding claims 13, 14, 15, 16, 17, 20 and 68, Kiko teaches that the plurality of devices includes at least one of a Z-Wave device (para [0242]), an Internet Protocol device (para [0242]), a camera (para [0158]), another touchscreen (para [0128], [0138], [0143]), a device controller that controls an attached device (para [0247]), and a sensor (para [0156], [0169]).			
-CONTINUED IN SUPPLEMENTAL BOX-			

Form PCT/ISA/237 (Box No. V) (July 2009)

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 10/57674

## Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Box No. V. 2. Citations and explanations:

Regarding claim 18, Kiko teaches that the device controller is a thermostat (para [0156], [0169]).

Regarding claim 19, Kiko teaches that the device controller is an energy meter (para [0099], [0119]).

Regarding claims 21 and 69, Kiko teaches that the plurality of modules includes a security module that generates through the touchscreen a security network by integrating into the touchscreen a security system located at the premise, wherein the security system includes a plurality of security components (para [0097], [0158], [0180]).

Regarding claims 22 and 70, Kiko teaches that the security module includes security system software that runs on the processor of the touchscreen (Fig. 1-1 to 1-4), wherein the security system software controls operation of the security system and interoperability of the plurality of security components (para [0097], [0138], [0158]).

Regarding claims 23 and 71, Kiko teaches controlling with the security system software processing of state data of the plurality of security components (para [0099], [0119]).

Regarding claims 24, 25 and 72, Kiko teaches determining via the security system software alarm system state and generating alarm reports (para [0158], [0175], [0247]).

Regarding claim 26, Kiko teaches that the touchscreen with the security module establishes communication with the at least one remote network (para [0137], [0180]).

Regarding claims 27 and 73, Kiko teaches using the touchscreen with the security module to generate a subnetwork in the premise which incorporates the touchscreen, wherein the subnetwork includes at least one component and is independent from the security network (a VPN establishes external, i.e., independent, sub/tunnel-networks; para [0130]).

Regarding claims 28 and 74, Kiko teaches controlling via the touchscreen an exchange of data between a first component of the security network and a second component of one of the subnetwork and the remote network (client devices tunnel to remote / VPN network components; para [0128], [0138]).

Regarding claims 29 and 75, Kiko teaches generating and presenting to a user via the touchscreen a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system (para [0142], [0158], [0247]), wherein the network interface allows the user to transfer content to and from the at least one remote network (para [0244], [0247]).

Regarding claims 30 and 76, Kiko teaches running a first application engine under the processor, wherein the first application engine executes a security application that provides the security interface (para [0097], [0099], [0142], [0158], [0247]).

Regarding claims 31 and 77, Kiko teaches running a second application engine under the processor, wherein the second application engine executes a content application that provides the network interface (para [0128], [0137], [0138], [0242]).

Regarding claims 32 and 78, Kiko teaches generating via the touchscreen and a module a subnetwork in the premise which incorporates the touchscreen (para [0180], [0130], [0239], [0242]), wherein the subnetwork includes at least one component and is independent from any other network of the premise (a VPN establishes external, i.e., independent, sub/tunnel-networks; para [0130]).

Regarding claims 33 and 79, Kiko teaches controlling via the touchscreen an exchange of data between the at least one component of the subnetwork and any other component of the premise coupled to the touchscreen (para [0130], [0239], [0242], [0244]).

Regarding claims 34 and 80, Kiko teaches establishing a coupling between a remote server and the touchscreen, the remote server managing at least one of the touchscreen and the plurality of functions (para [0128], [0136], [0239], [0242], [0244]).

Regarding claim 35, Kiko teaches that the remote server allows a user to configure content of the touchscreen (para [0126], [0140], [0247]).

Regarding claim 36, Kiko teaches that the remote server provides user portals that enable content and information displayed on the touchscreen to be displayed on remote devices (para [0140], [0142], [0239], [0247]).

Regarding claim 37, Kiko teaches that the remote devices access the plurality of functions via the portals (web browser interfaces via tunnels; para [0128], [0130], [0142], [0143], [0180]).

Regarding claim 81, Kiko teaches accessing the plurality of functions via remote devices (para [0136], [0143], [0180]).

Regarding claims 38 and 82, Kiko teaches that the touchscreen includes a wireless transceiver for communicating with remote devices (para [0137], [0242]).

--CONTINUED IN NEXT SUPPLEMENTAL BOX--

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.  
PCT/US 10/57674

**Supplemental Box**

**In case the space in any of the preceding boxes is not sufficient.**

Continuation of:  
Box No. V. 2. Citations and explanations:

Regarding claims 39 and 83, Kiko teaches that at least one module includes a wireless transceiver for communicating with remote devices (para [0137], [0242]).

Regarding claim 40, Kiko teaches that the touchscreen plays live video from a camera at the premise (para [0158], [0244]).

Regarding claims 41 and 84, Kiko teaches presenting a network interface to a user via the touchscreen, transferring content to and from the at least one remote network using the network interface (para [0136], [0142]).

Regarding claims 42 and 85, Kiko teaches that the network interface allows the user to integrate the content with the plurality of applications (para [0099], [0138], [0139]).

Regarding claims 43 and 86, Kiko teaches that network interface allows the user to integrate the content with components of the modules (para [0097], [0099], [0138], [0139]).

Regarding claims 45 and 87, Kiko teaches that the content includes at least one of interactive content in the form of internet widgets, an application (para [0139], [0142], [0180]), an update to an application of the plurality of applications (para [0139], [0142]), and an update to a component of a module (para [0139], [0142]).

Regarding claim 46, Kiko teaches that the network interface allows the user to control functions of devices of the premise (para [0143], [0247]).

Regarding claims 47 and 88, Kiko teaches that the plurality of applications provides interactivity with the plurality of functions (para [0139], [0142], [0143], [0180]).

Regarding claims 48 and 89, Kiko teaches that the plurality of applications provides interactivity with a plurality of devices of the premise (para [0138], [0143]).

Regarding claims 49 and 90, Kiko teaches that the plurality of devices is coupled to the processor (Fig. 2f; para [0138], [0143], [0143]).

Regarding claims 50 and 91, Kiko teaches that the plurality of devices is coupled to the processor via a wireless coupling (Fig. 2f; para [0128], [0137]).

Regarding claims 51 and 92, Kiko teaches that the plurality of devices is coupled to the processor via a module of the plurality of modules (Fig. 2f; para [0097], [0138], [0139]).

Regarding claims 52 and 93, Kiko teaches that the plurality of applications includes a resident application that manages interactions between the plurality of applications (resident application protocol stack and OS; para [0149], [0239], [0244]).

Regarding claims 55 and 96, Kiko teaches that the resident application manages interactions between a plurality of devices at the premise (resident application protocol stack and OS can self-upgrade; para [0139], [0149], [0239], [0244]).

Regarding claims 56 and 97, Kiko teaches a core engine coupled to the processor, the core engine controlling dynamic provisioning of the plurality of applications and content (resident application protocol stack and core / main functions of the OS / processor; Fig. 2f; para [0149], [0239], [0244]).

Regarding claim 57, Kiko teaches that the core engine manages images received from a plurality devices of the premise (Fig. 1-1 to 1-4, 2f; para [0156], [0158], [0244]).

Regarding claim 58, Kiko teaches that the images include video (para [0156], [0158], [0244]).

Regarding claim 59, Kiko teaches that the processor is coupled to the at least one remote network via a broadband coupling (para [0242]).

Regarding claim 60, Kiko teaches that the processor is coupled to the at least one remote network via a cellular data coupling (para [0128], [0244]).

—CONTINUED IN NEXT SUPPLEMENTAL BOX—

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITYInternational application No.  
PCT/US 10/57674

## Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Box No. V. 2. Citations and explanations:

Claim 4 lacks an inventive step under PCT Article 33(3) as being obvious over Kiko in view of US 2008/0084296 A1 to Kutzik et al. (hereinafter 'Kutzik').

Regarding claim 4, Kiko further teaches monitoring temperature and humans (para [0097], [0119], [0156], [0158], [0175], [0180]), but Kiko fails to teach that the plurality of modules include a remote health monitoring module for human health monitoring on the premise. Kutzik teaches that the plurality of modules include a remote health monitoring module for human health monitoring on the premise to provide a more useful and safe remote health / temperature monitoring system (para [0026], [0029], [0175], [0179]). It would have been obvious to one of ordinary skill in the art at the time of the applicant's claimed invention to modify the device of Kiko to include a plurality of modules that include a remote health monitoring module for human health monitoring on the premise as taught by Kutzik to provide a more useful and safe monitoring system.

Claims 44, 53, 54, 94 and 95 lack an inventive step under PCT Article 33(3) as being obvious over Kiko in view of US 2009/0165114 A1 to Baum et al. (hereinafter 'Baum').

Regarding claim 44, Kiko further teaches interacting with automation devices through browser desktop clients (para [0128], [0149]), but Kiko fails to teach that the content includes interactive content in the form of internet widgets. Baum teaches that the content includes interactive content in the form of internet widgets to provide premise monitoring using a container provided by a third-party (para [0072], [0138]). It would have been obvious to one of ordinary skill in the art at the time of the applicant's claimed invention to modify the device of Kiko to include content that includes interactive content in the form of internet widgets as taught by Baum to provide more flexible and enhanced content.

Regarding claims 53 and 94, Kiko fails to teach that the resident application determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority. Baum teaches that the resident application determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority to perform better (para [0154]). It would have been obvious to one of ordinary skill in the art at the time of the applicant's claimed invention to modify the device (and associated method) of Kiko to include a resident application that determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority as taught by Baum to provide a higher quality of service.

Regarding claims 54 and 95, Baum further teaches that the resident application allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority (para [0154]).

Claims 1-97 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.

**PATENT COOPERATION T**

From the INTERNATIONAL SEARCHING AUTHORITY

**PCT**

NOTIFICATION OF TRANSMITTAL OF  
THE INTERNATIONAL SEARCH REPORT AND  
THE WRITTEN OPINION OF THE INTERNATIONAL  
SEARCHING AUTHORITY, OR THE DECLARATION

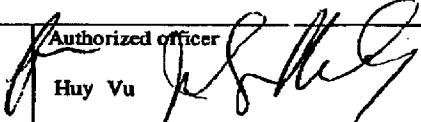
(PCT Rule 44.1)

To:  
GEORGE A. WILLMAN  
WILSON SONSINI GOODRICH & ROSATI  
650 PAGE MILL ROAD  
PALO ALTO, CA 94306-1050

**RECEIVED**  
  
MAY 26 2006  
  
WILSON, SONSINI,  
GOODRICH & ROSATI

Date of mailing (day/month/year)	<b>23 MAY 2006</b>
Applicant's or agent's file reference 30116-701601	<b>FOR FURTHER ACTION</b> See paragraphs 1 and 4 below
International application No. PCT/US05/08766	International filing date (day/month/year) 16 March 2005 (16.03.2005)
Applicant ICONTROL NETWORKS, INC.	

1.  The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.  
**Filing of amendments and statement under Article 19:**  
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):  
**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.  
**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70.  
**For more detailed instructions, see the notes on the accompanying sheet.**
2.  The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
3.  With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
  - the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.
  - no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.
4. **Reminders**  
Shortly after the expiration of 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.  
The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.  
Within 19 months from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later); otherwise, the applicant must, within 20 months from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.  
In respect of other designated Offices, the time limit of 30 months (or later) will apply even if no demand is filed within 19 months.  
See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer  Huy Vu Telephone No. (703) 272-2500
--	--

**PATENT COOPERATION TREATY**

**PCT**

**INTERNATIONAL SEARCH REPORT**

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 30116-701601	<b>FOR FURTHER ACTION</b>		see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US05/08766	International filing date ( <i>day/month/year</i> ) 16 March 2005 (16.03.2005)	(Earliest) Priority Date ( <i>day/month/year</i> ) 16 March 2004 (16.03.2004)	
Applicant ICONTROL NETWORKS, INC.			

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

**1. Basis of the Report**

a. With regard to the language, the international search was carried out on the basis of:

- the international application in the language in which it was filed.
- a translation of the international application into \_\_\_\_\_, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b.  With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2.  Certain claims were found unsearchable (See Box No. II)

3.  Unity of invention is lacking (See Box No. III)

4. With regard to the title,

- the text is approved as submitted by the applicant.
- the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- the text is approved as submitted by the applicant.
- the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

a. the figure of the drawings to be published with the abstract is Figure No. 1

- as suggested by the applicant.
- as selected by this Authority, because the applicant failed to suggest a figure.
- as selected by this Authority, because this figure better characterizes the invention.

b.  none of the figures is to be published with the abstract.

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US05/08766

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC: **H04L 12/56(2006.01)**

USPC: 370/401

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
 U.S. : 370/401, 229, 230, 352, 389, 400, 465, 466

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

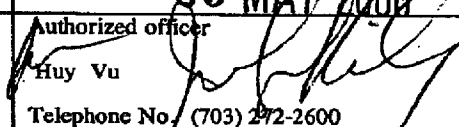
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	US 2003/0051009 A1 (SHAH et al) 13 March 2003 (13.03.2003), paragraphs 16-29 and Figures 1-2	11-4, 7-9, 18-20, 31-33, 33-37  4-6, 10-17, 21-30, 34-35
Y	US 2002/0083342 A1 (WEBB et al) 27 June 2002 (27.06.2002), paragraphs 4 and 27	5-6, 17, 30, and 35

Further documents are listed in the continuation of Box C.       See patent family annex.

* Special categories of cited documents:	"T"
"A" document defining the general state of the art which is not considered to be of particular relevance	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 11 April 2006 (11.04.2006)	Date of mailing of the international search report <b>23 MAY 2006</b>
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer  Huy Vu Telephone No. (703) 272-2600



PATENT COOPERATION TREATY

REC'D 29 MAY 2006

From the  
INTERNATIONAL SEARCHING AUTHORITY

WIPO PCT

PCT

To:  
GEORGE A. WILLMAN  
WILSON SONSINI GOODRICH & ROSATI  
650 PAGE MILL ROAD  
PALO ALTO, CA 94306-1050

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing  
(day/month/year) 28 MAY 2006

Applicant's or agent's file reference

FOR FURTHER ACTION

See paragraph 2 below

30116-701601

International application No.

International filing date (day/month/year)

Priority date (day/month/year)

PCT/US05/08766

16 March 2005 (16.03.2005)

16 March 2004 (16.03.2004)

International Patent Classification (IPC) or both national classification and IPC

IPC: H04L 12/56( 2006.01)

USPC: 370/401

Applicant

ICONTROL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

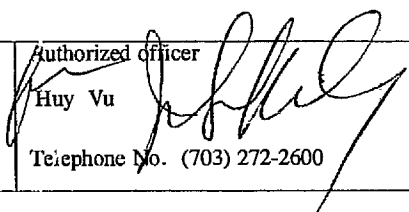
2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

<p>Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201</p>	<p>Date of completion of this opinion 11 April 2006 (11.04.2006)</p>	<p>Authorized officer Huy Vu Telephone No. (703) 272-2600</p> 
--	--	--

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US05/08766

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

- the international application in the language in which it was filed
- a translation of the international application into \_\_\_\_\_, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

- a sequence listing
- table(s) related to the sequence listing

b. format of material

- on paper
- in electronic form

c. time of filing/furnishing

- contained in the international application as filed.
- filed together with the international application in electronic form.
- furnished subsequently to this Authority for the purposes of search.

3.  In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US05/08766

Box No. V Reasoned statement under Rule 43 bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims <u>5-6, 10-17, 21-30, 34-35</u>	YES
	Claims <u>1-4, 7-9, 18-20, 31-33, 36-37</u>	NO
Inventive step (IS)	Claims <u>NONE</u>	YES
	Claims <u>1-37</u>	NO
Industrial applicability (IA)	Claims <u>1-37</u>	YES
	Claims <u>NONE</u>	NO

2. Citations and explanations:

Please See Continuation Sheet

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US05/08766

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

**V. 2. Citations and Explanations:**

Claims 1-4, 7-9, 18-20, 31-33, and 36-37 lack novelty under PCT Article 33(2) as being anticipated by Shah et al. (U.S. Publication US 2003/0051009 A1).

With respect to claim 1, Shah et al. discloses a method for premises management networking (See the abstract of Shah et al. for reference to a method for managing a network from a node residing outside the network). Shah et al. also discloses monitoring and controlling premises management devices connected to a gateway at a premises (See pages 1-2 paragraphs 16-21 and Figure 1 of Shah et al. for reference to monitoring and controlling devices 150, 160, 170, and 180 connected to an area network device access mechanism 130, which is a gateway, at the premises of an area network 120). Shah et al. further discloses receiving an uplink-initiation signal associated with a network operations center server at the premises and initiating from the gateway communications between the gateway and the network operations center server in response (See pages 1-3 paragraphs 16-29 and Figures 1-2 of Shah et al. for reference to an external node 110, which can be a centralized server, sending a communication to the network device access mechanism 130, and for reference to the network device access mechanism 130 initiating communications with the external node 110 in response). Shah et al. also discloses communicating information associated with the premises management devices (See pages 2-3 paragraphs 22-29 and Figure 2 of Shah et al. for reference to communicating information including device states and commands between the network access device mechanism 130 and the external node 110).

With respect to claims 9, 20, and 33, Shah et al. discloses a business method for premises management (See the abstract of Shah et al. for reference to a method for managing a network from a node residing outside the network). Shah et al. also discloses making an Internet portal available for access (See pages 1-2 paragraphs 16-21 and Figure 1 of Shah et al. for reference to making an external node 110 which can be a server containing an Internet portal, available). Shah et al. further discloses providing premises management service via the Internet portal (See pages 1-3 paragraphs 16-29 and Figures 1-2 of Shah et al. for reference to managing devices of a premises using the external node 110).

With respect to claim 2, Shah et al. discloses that the uplink-initiation signal is received via telephone (See page 1 paragraph 17 of Shah et al. for reference to the external node 110 being a wireless phone, meaning signals sent from the external node 110 are received via telephone links).

With respect to claim 3, Shah et al. discloses that the uplink-initiation signal is received via broadband connection (See page 1 paragraph 17 of Shah et al. for reference to the external node 110 being a computer, meaning signals sent from the external node 110 are received via a broadband Internet connection).

Form PCT/ISA/237 (Supplemental Box) (April 2005)

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US05/08766

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

With respect to claim 4, Shah et al. discloses communicating using HTTP messages (See page 2 paragraph 23 of Shah et al. for reference to using HTTP).

With respect to claims 7-8, 18-19, 31-32, and 36-37, Shah et al. discloses managing security and safety of the premises (See page 2 paragraph 21 of Shah et al. for reference to managing a home security system that provides security and safety for the premises of the area network 120).

Claims 10-16, 21-29, and 34 lack an inventive step under PCT Article 33(3) as being obvious over Shah et al.

With respect to claims 10, 21, and 34, Shah et al. does not specifically disclose branding the Internet portal.

Branding an Internet portal is old and well known in the art of communications.

To combine branding an Internet portal with the system and method of Shah et al., with the motivation being to provide a product/company association, lacks an inventive step.

With respect to claims 11-16 and 22-29, Shah et al. does not disclose that the vender is a home builder, premises builder, premises manager, Internet services provider, telephone company, satellite television company, and cable television company. Shah et al. also does not disclose that the vendee is a home buyer, premises buyer, premises tenant, a customer of an Internet service provider, a customer of a telephone company, a customer of a satellite television company, and a customer of a cable television company.

Having a vender be a home builder, premises builder, premises manager, Internet services provider, telephone company, satellite television company, and cable television company and having a vendee be a home buyer, premises buyer, premises tenant, a customer of an Internet service provider, a customer of a telephone company, a customer of a satellite television company, and a customer of a cable television company is old and well known in the art of communications.

To combine having a vender be a home builder, premises builder, premises manager, Internet services provider, telephone company, satellite television company, and cable television company and having a vendee be a home buyer, premises buyer, premises tenant, a customer of an Internet service provider, a customer of a telephone company, a customer of a satellite television company, and a customer of a cable television company with the system and method of Shah et al., with the motivation being to buy and sell a service, lacks an inventive step.

Claims 5-6, 17, 30, and 35 lack an inventive step under PCT Article 33(3) as being obvious over Shah et al. in view of Webb et al. (U.S. Publication US 2002/0083342 A1).

With respect to claim 5, Shah et al. does not disclose communicating using XML.

With respect to claim 5, Webb et al., in the field of communications, discloses communicating using XML (See page 3 paragraph 28 of Webb et al. for reference to a remote monitoring system that communicates using XML). Communicating using XML has the advantage of using a widely known and used communication protocol.

To combine communicating using XML, as suggested by Webb et al., with the system and method of Shah et al., with the motivation being to use a widely known and used communication protocol, lacks an inventive step.

With respect to claims 6, 17, 30, and 35, Shah et al. does not disclose managing energy of the premises.

With respect to claims 6, 17, 30, and 35, Webb et al., in the field of communications, discloses, managing energy of a premises (See page 1 paragraph 4 of Webb et al. for reference to remotely managing energy of a premises). Managing energy of a premise has the advantage of allowing remote control over the energy use of a premise.

To combine managing energy of a premise, as suggested by Webb et al., with the system and method Shah et al., with the motivation being to allow remote control over the energy use of a premise, lacks an inventive step.

Claims 1-37 meet industrial applicability as defined by PCT Article 33(4). Claims 1-37 have industrial applicability in the field of communications.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12189788
<b>Filing Date:</b>	12-Aug-2008
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Filer:</b>	Richard L. Gregory/Kim Moore
<b>Attorney Docket Number:</b>	ICON.P001D3

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Submission- Information Disclosure Stmt	1806	1	180	180
<b>Total in USD (\$)</b>				<b>180</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	12963887
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	98195
<b>Filer:</b>	Richard L. Gregory/Kim Moore
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	07-JUN-2012
<b>Filing Date:</b>	12-AUG-2008
<b>Time Stamp:</b>	18:38:58
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$180
RAM confirmation Number	5678
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / zip (if appl.)	Pages (if appl.)
SecureNet Technologies, LLC Exhibit 1003 Page 840					



1	Transmittal Letter	ICON_P001D3_IDS_transmittal_as_filed_07JUN2012.pdf	150476 ebe3d5cfd7fed6fdd58be6f88c0a97eae27def	no	2
<b>Warnings:</b>					
<b>Information:</b>					
2	Information Disclosure Statement (IDS) Form (SB08)	ICON_P001D3_IDS_as_filed_07JUN2012.pdf	1627975 69358beac93140a5db765a4aa9f209492e66fec	no	9
<b>Warnings:</b>					
<b>Information:</b>					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	ICON_P001D3_Foreign_Patent_documents_Part_A_as_filed_07JUN2012.pdf	15489612 c925a1703b36d75a0de91c2e8579c26be53002c7	no	101
<b>Warnings:</b>					
<b>Information:</b>					
4	Foreign Reference	ICON_P001D3_Foreign_Patent_documents_Part_B_as_filed_07JUN2012.pdf	11731177 8b854db6a59028f2a5e7a808a0b11170aee6557e	no	95
<b>Warnings:</b>					
<b>Information:</b>					
5	Foreign Reference	ICON_P001D3_Foreign_Patent_documents_Part_C_as_filed_07JUN2012.pdf	10325662 4d93b767db135cb0555e1333fe16048e9b607dd8	no	90
<b>Warnings:</b>					
<b>Information:</b>					
6	Foreign Reference	ICON_P001D3_Foreign_Patent_documents_Part_D_as_filed_07JUN2012.pdf	12146941 3902234a7d52f099375d99a9c61335873b71ec5d	no	84
<b>Warnings:</b>					
<b>Information:</b>					
7	Non Patent Literature	ICON_P001D3_NPL_documents_Part_A_as_filed_07JUN2012.pdf	8872378 10514a720f10df790bedbc06ed95992b2d680de5	no	47
<b>Warnings:</b>					
<b>Information:</b>					
8	Non Patent Literature	ICON_P001D3_NPL_documents_Part_B_as_filed_07JUN2012.pdf	4632581 6e7649d50413607abea9c389cd78d1e8aff98a6	no	29
<b>Warnings:</b>					
<b>Information:</b>					
9	Fee Worksheet (SB06)	fee-info.pdf	30491 9cc7a09d69f8714ddf97fdd306e74ee1935b811	no	2

<b>Warnings:</b>	
<b>Information:</b>	
<b>Total Files Size (in bytes):</b>	65007293
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>	

**IN THE UNITED STATES PATENT OFFICE**

In Re Patent Application of:	)	
	)	Examiner: Anthony Mejia
First Named Inventor: Marc Baum	)	Art Unit: 2451
	)	
Application No. 12/189,788	)	
	)	
Filed: August 12, 2008	)	
	)	
For: FORMING A SECURITY NETWORK	)	
INCLUDING INTEGRATED SECURITY	)	
SYSTEM COMPONENTS AND NETWORK	)	
<u>DEVICES</u>	)	

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Submission of Information Disclosure Statement**

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 (Substitute). Copies of references that are not U.S. Patents or U.S. Patent Publications are also enclosed. It is respectfully requested that the cited documents be considered and that the enclosed Information Disclosure Citation Form PTO-1449 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

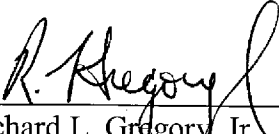
This Information Disclosure Statement is being submitted pursuant to 37 C.F.R. § 1.97(c).

Pursuant to 37 C.F.R. § 1.97(h), the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Attorney Docket No. ICON.P001D3  
Application No. 12/189,788

Respectfully submitted,  
Gregory & Sawrie LLP

Dated: June 7, 2012

  
\_\_\_\_\_  
Richard L. Gregory, Jr.  
Reg. No. 42,607

Gregory & Sawrie LLP  
2018 Bissonnet Street  
Houston, Texas 77005  
Telephone No.: (408) 821-8080  
Facsimile No.: (713) 364-1397



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes sub-tables for EXAMINER (MEJIA, ANTHONY), ART UNIT (2451), PAPER NUMBER, NOTIFICATION DATE (01/17/2012), and DELIVERY MODE (ELECTRONIC).

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

- rick@iprlaw.com
david@iprlaw.com
vlad@iprlaw.com

<b>Office Action Summary</b>	<b>Application No.</b> 12/189,788	<b>Applicant(s)</b> BAUM ET AL.	
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 14 November 2011.
- 2a)  This action is **FINAL**.
- 2b)  This action is non-final.
- 3)  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 4)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 5)  Claim(s) 1-3 and 5-51 is/are pending in the application.
  - 5a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 6)  Claim(s) \_\_\_\_\_ is/are allowed.
- 7)  Claim(s) 1-3 and 5-51 is/are rejected.
- 8)  Claim(s) \_\_\_\_\_ is/are objected to.
- 9)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 10)  The specification is objected to by the Examiner.
- 11)  The drawing(s) filed on \_\_\_\_\_ is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 13)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All    b)  Some \*    c)  None of:
    - 1.  Certified copies of the priority documents have been received.
    - 2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    - 3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_.

Art Unit: 2451

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicants' submission filed on **14 November 2011** has been entered.

### ***Response to Amendment***

2. Acknowledgement is made that Claim 4 has been canceled. Claims 1 and 49-51 have been amended in the instant application and now being presented.

### ***Priority***

3. Applicant's claim for the benefit of a prior-filed Application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has complied with the conditions for receiving the benefit of an earlier filing date.

Art Unit: 2451

***Response to Arguments***

4. Applicant's alleged arguments, see pages 10-19 of Remarks, filed, **14 November 2011**, with respect to Claims 1-3 and 5-51 rejection under 35 U.S.C. 103(a) have been fully considered but are not persuasive.

For instance, as per Claims 1 and 49-51, Applicants argue that Naidoo does not disclose coupling a gateway to a local network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added). Applicants further submit that Naidoo in view of Bilger and further in view of Rezvani still do not teach the argued limitation above.

As per applicant's arguments above, Examiner respectfully disagrees. Naidoo clearly teaches the step of: "...coupling a gateway to a local network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components..." Naidoo discloses a security system for monitoring a premises by integrating broadband features, including audio and video capabilities, web access and wireless capabilities which is typically located at the desired premises 110 to be monitored, and a monitoring client 133, typically located at a central station and operatively coupled to security



Art Unit: 2451

gateway 115 through a network 120. Often, security gateway 115 is located at the target site. However, on some occasions, some or all components of security gateway 115 may be located remotely, but remain operatively coupled to security sensors 105 and video cameras 112 which are at the premises. The components of security gateway 115 are configured to communicate with one another through system bus 605. In other embodiments, some or all of the components may be directly connected or otherwise operatively coupled to one another (*see* pars [0027-0030], [0047-0048], and [0078-0079], and *see* figs.1-2 and 6).

Furthermore, as per applicants arguments that Naidoo fails to teach, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server. Naidoo teaches that once a remote user is authenticated, remote user may access some or all of the features of base station 115. These features may include, without limitation, arming or disarming the security system; adjusting sensitivities of sensors (if present); adjusting alarm condition detection sensitivity; remote surveillance; adjusting camera settings; and reviewing alarms and recordings. security gateway 115 may be preempted whenever an alarm condition occurs so that CMS personnel have full control over cameras 112 and microphones 634 to respond to the alarm condition (pars [0040] and [0107]). Thus, Naidoo clearly teaches the limitation wherein objects corresponding to the security system components are maintained on the security server.

5. As per Claims 2-3, 5-9, 11-12, 15-25, 28, 30-45, and 48, Applicant's arguments are not persuasive as for the same reasons as discussed above.

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-3, 5-9, 11-12, 15-25, 28, 30-45, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo et al. (US 2003/0062997) (hereinafter as Naidoo) in further view of Bilger (US 6,756,998) and in further view of Rezvani et al. (US 6,686,838) (hereinafter as Rezvani).

Regarding Claim 1, Naidoo teaches a method comprising:

coupling a gateway to a local area network located in a first location and a security server in a second location (see figs.1-2), wherein the first location includes a security system comprising:

a plurality of security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the gateway and the security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

Art Unit: 2451

automatically establishing communications between the gateway and premise devices pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and forming a security network by electronically integrating, via the gateway, communications and functions of the plurality of premise devices and the security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (pars [0017], [0027-0030], [0040] [0047-0048], [0078-0079], [0107], and see figs.1-2 and 6).

The teachings of Naidoo do not explicitly teach the step of *automatically discovering security system components*.

However, Bilger in a similar field of endeavor discloses a home automation system interface for interfacing with a system that automatically controls controlled devices throughout the home including the step of *automatically discovering security system components at the gateway* (e.g., control objects are plug and play compatible and are automatically recognized by the central controller once connected to the network, col.8, lines 55-67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Bilger in order Naidoo's components to automatically install devices to the security system. One of ordinary skill in the art would have been motivated because it would ease installation of components by automatically installing the device to the security system.

Art Unit: 2451

In further the combined teachings of Naidoo and Bilger do not explicitly teach the step of *automatically discovering a plurality of premise devices at a gateway*.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Applicants are also respectfully reminded that broadly providing an automatic means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art. See MPEP 2144.04(III).

Art Unit: 2451

Regarding Claim 2, Naidoo further teaches the step of controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device (pars [0040-0041]).

Regarding Claim 3, Naidoo further teaches the step wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices (par [0040] and see fig.2).

Regarding Claim 5, Rezvani teaches wherein the method further comprises the step of:

using protocols of the security system to discover the security system components, wherein the gateway includes the protocols of the security system (see Rezvani; col. 2/lines 27-36; the remote sites may validate received registration protocol messages used during the new object discovery process to discovery new devices).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Art Unit: 2451

Regarding Claim 6, Rezvani teaches wherein the method further comprises the steps of:

requesting and receiving protocols of the security system from the security server, wherein the gateway receives and uses the protocols to discover the security system components (col. 2, lines 27-36; the remote sites may validate received registration protocol messages used during the new object discovery process to discover new devices).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Regarding Claim 7, Naidoo further teaches the step wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components (pars [0069], [0079], and [0087]).

Art Unit: 2451

Regarding Claim 8, Naidoo further teaches the step wherein the connection management component automatically discovers the premise devices (par [0040] and see fig.2).

Regarding Claim 9, Bilger teaches wherein the connection management component will automatically installs the premise devices in the security network (col. 20, lines 1-13).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Bilger in order Naidoo's components to automatically install devices to the security system. One of ordinary skill in the art would have been motivated because it would ease installation of components by automatically installing the device to the security system.

Regarding Claim 11, Naidoo further teaches the step wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices (par [0099]).

Regarding Claim 12, Naidoo further teaches the step wherein the gateway includes a device connect component that includes definitions of the security system components and the premise devices (pars [0080-0081]).

Art Unit: 2451

Regarding Claim 15, Naidoo further teaches the step wherein the gateway is coupled to the premise devices using a wireless coupling (par [0033]).

Regarding Claim 16, Naidoo further teaches the step wherein the gateway is coupled to the security server via the internet (par [0030]).

Regarding Claim 17, Naidoo further teaches the step wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location (par [0043] and see fig.2).

Regarding Claim 18, Naidoo further teaches wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link (par [0043] and see fig.2).

Regarding Claim 19, Naidoo further teaches the step of transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link (par [0043] and see fig.2).



Art Unit: 2451

Regarding Claim 20, Naidoo further teaches the step wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of:

security system components and premise devices, and data received by at least one of security system components and premise devices (pars [0069], and [0080-0081]).

Regarding Claim 21, Naidoo further teaches the step of transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable (par [0043]).

Regarding Claim 22, Naidoo further teaches wherein the secondary communication link includes a broadband coupling (pars [0027] and [0122]).

Regarding Claim 23, Naidoo further teaches the step wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling (par [0043]).

Regarding Claim 24, Naidoo further teaches the step of transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link (pars [0027-0028], [0043], and [0046]).

Art Unit: 2451

Regarding Claim 25, Naidoo further teaches wherein the event data comprises changes in device states of at least one of:

security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices (pars [0069], and [0080-0081]).

Regarding Claim 28, Naidoo further teaches wherein the security server creates modifies and terminates couplings between the gateway and the premise devices (pars [0099-0101]).

Regarding Claim 30, Naidoo further teaches wherein wherein the security server performs creation, modification, deletion and configuration of the premise devices (pars [0099-0101]).

Regarding Claim 31, Naidoo further teaches wherein the security server creates automations, schedules and notification rules associated with the security system components (par [0045]).

Art Unit: 2451

Regarding Claim 32, Naidoo further teaches wherein the security server creates automations, schedules and notification rules associated with the premise devices (pars [0027-0028] and [0045]).

Regarding Claim 33, Naidoo further teaches the step wherein the security server manages access to current and logged state data for the security system components (pars [0049-0050]).

Regarding Claim 34, Naidoo further teaches the step wherein the security server manages access to current and logged state data for the premise devices (pars [0027-0028] and [0049-0050]).

Regarding Claim 35, Naidoo further teaches the step wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices (pars [0027-0028] and [0049-0050]).

Regarding Claim 36, Naidoo further teaches the step wherein the security server manages communications with the security system components (par [0049]).

Regarding Claim 37, Naidoo further teaches the step wherein the security server manages communications with the premise devices (pars [0027-0028] and [0049]).

Art Unit: 2451

Regarding 38, Naidoo further teaches the step wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data (par [0053]).

Regarding 39, Naidoo further teaches the step wherein the notifications include one or more of short message service messages and electronic mail messages (par [0069]).

Regarding Claim 40, Naidoo further teaches the step wherein the event data is event data of the security system components (par [0053]).

Regarding Claim 41, Naidoo further teaches the step wherein the event data is event data of the premise devices (pars [0027-0028] and [0053]).

Regarding Claim 42, Naidoo further teaches the step wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link (pars [0027-0028], [0043], and [0046]).

Regarding Claim 43, Naidoo further teaches the step wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers (par [0059]).

Art Unit: 2451

Regarding Claim 44, the method of claim 1, wherein the premise device is an Internet Protocol device (par [0037]).

Regarding Claim 45, Naidoo further teaches the step wherein the premise device is a camera (pars [0040-0041]).

Regarding Claim 48, Naidoo further teaches the step wherein the premise device is a sensor (pars [0040-0041]).

8. Claims 10 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Tanaka et al. (US 2004/0037295).

Regarding Claim 10, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of Claim 7, *wherein the connection management component automatically configures the premise devices for operation in the security network.*

Tanaka in the field of the same endeavor teaches creating a virtual local area network using a graphical user interface. In particular, Tanaka teaches the server automatically creates configuration information of the switch (see Tanaka: par [0083]).

Therefore, it would have been obvious to a person of ordinary skill in the art at

Art Unit: 2451

the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Tanaka in order for Naidoo server to perform configurations on the device. Tanaka teachings enabled Naidoo/Bilger/Rezvani to create, modify, and delete configuration settings of the switch. One of ordinary skill in the art would have been motivated because allowing for configurations to be created, modified and deleted increase the flexibility of a device by allowing configurations to be created, modified and deleted.

Regarding Claim 29, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani discloses the method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.

Tanaka in the field of the same endeavor teaches creating a virtual local area network using a graphical user interface. In particular, Tanaka teaches the server automatically creates configuration information of the switch and deletes the VLAN link. The server automatically issues command to delete the connection to the switch (see Tanaka; [0083]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Tanaka in order for Naidoo/Bilger/Rezvani server to perform actions on the device configurations. Tanaka teachings enabled Naidoo/Bilger/Rezvani to create, modify, and delete configuration settings of the switch. One of ordinary skill in the art would have been motivated because allowing for configurations to be created, modified and deleted

Art Unit: 2451

increase the flexibility of a device by allowing configurations to be created, modified and deleted.

9. Claims 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over in further view of Naidoo in further view of Bilger in further view of Rezvani and in further view of Patterson (US 2005/0086126).

Regarding Claim 26, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of Claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.

Patterson, in the field of the same endeavor teaches managing and linking network accounts to share access privileges among accounts. In particular, Patterson teaches that the server may create account, upgrade an account, or terminate the upgrading of an account (see Patterson; [0046]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Patterson in order for the server of Naidoo/Bilger/Rezvani to create, upgrade, and terminate accounts. One of ordinary skill would be motivated because Patterson suggest it would be desirable for an environment having different levels of access, a provider may charge higher fees for accounts with higher levels of access. Accordingly, from the provider's standpoint, it is desirable to encourage users to purchase more

Art Unit: 2451

expensive subscriptions, and so the provider often attempts to make the accounts with higher levels of access more appealing to users (see Patterson; [0002]).

10. Claims 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over in further view of Naidoo in further view of Bilger in further view of Rezvani and in further view of Moyer et al. (US 2002/0103898).

Regarding Claim 27, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.

Moyer in the field of the same endeavor teaches Session Initiated Protocol (SIP) to communicate with network capable appliances by leveraging SIP capabilities to directly communicating with the appliances. In particular, Moyer teaches that SIP is an application layer control and signaling protocol used for creating, modifying and terminating communication sessions between participants (see Moyer; [0013]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Moyer in order for Naidoo/Bilger/Rezvani servers to create, modify, and terminate communication between the gateway and the security system utilizing SIP. One of ordinary skill in the art would be motivated because SIP is designed to be independent of the underlying transport layer and it can run on TCP, UDP, or SCTP.



Art Unit: 2451

11. Claim 46-47 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Lingemann (US 2006/0009863).

Regarding claim 46, Naidoo/Bilger/Rezvani the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of claim 1, wherein the network device is a touchscreen.

Lingemann in the field of the same endeavor teaches building an automation system including user interface units with touchscreen. In particular, Lingemann teaches (see Lingemann; fig. 10, [0076]; a touch screen interface unit as illustrated in fig. 10 used for controlling electrical devices).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Lingemann in order for Naidoo's device to incorporate a touchscreen. One of ordinary skill in the art would have been motivated because a touchscreen would provide an ease of interaction by allowing the user to interact with what is displayed directly on the hand, where it is displayed, rather than indirect with a mouse or touchpad.

Regarding Claim 47, Naidoo/Bilger/Rezvani discloses the method of claim 24, wherein the network device is a device controller that controls an attached device (see Lingemann; fig. 10, [0076]; a touch screen interface unit as illustrated in fig. 10 used for

Art Unit: 2451

controlling electrical devices).

12. Claim 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Moore et al. (US 2007/0061266).

Regarding Claim 13, Naidoo/Bilger/Rezvani substantially discloses the method of claim 1, wherein the premise local area network is coupled to a wide area network. (see Naidoo; fig. 2; [0047-0048, 0087]; the security gateway is located in the premise which is considered a LAN. The security gateway is also connected to the internet and the security system server located at the data center which is considered to be the WAN).

However, Naidoo/Bilger/Rezvani does not explicitly disclose the premise local area network is coupled to a wide area network via a premise router.

Moore in the field of the same endeavor teaches large-scale, reliable, and secure foundations for distributed databases and content management systems combining unstructured and structured data, and allowing post-input reorganization to achieve a high degree of flexibility. In particular, Moore teaches a router that forward data packets across an internet work through a process known as routing that act as a junction between two networks (see Moore; [0217]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Moore in order for Naidoo/Bilger/Rezvani premise location to include a router that act as

Art Unit: 2451

a junction between two networks. One of ordinary skill in the art would have been motivated because the router would have improved Naidoo/Bilger/Rezvani teachings by enabled data packets to be routed to networks.

Regarding Claim 14, the combined teachings of Naidoo/Bilger/Rezvani and Moore further teach wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network (see Naidoo; fig. 2; [0047-0048, 0087]; the security gateway is located in the premise which is considered a LAN. The security gateway is also connected to the internet and the security system server located at the data center which is considered to be the WAN and Moore use of routers (see Moore; [0217]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Moore in order for Naidoo/Bilger/Rezvani premise location to include a router that act as a junction between two networks. One of ordinary skill in the art would have been motivated because the router would have improved Naidoo/Bilger/Rezvani teachings by enabled data packets to be routed to networks.

13. Claims 49-51 rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo and in further view of Rezvani.

Regarding Claim 49, Naidoo teaches a method comprising:

Art Unit: 2451

forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location (pars [0027-0030], [0047-0048], and [0078-0079], and see figs. 1-2 and 6); and

establishing a coupling between the gateway and a plurality of premise devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the gateway and security network, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (pars [0017], [0027-0030], [0040] [0047-0048], [0078-0079], [0107], and see figs. 1-2 and 6).

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the

Art Unit: 2451

invention was made to modify the teachings of Naidoo with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Applicants are also respectfully reminded that broadly providing an automatic means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art. See MPEP 2144.04(III).

Regarding Claim 50, Naidoo teaches a method comprising:

automatically discovering a security system at a gateway and establishing communications between a gateway and a security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system (pars [0027-0030], [0047-0048], and [0078-0079], and see figs. 1-2 and 6); and

automatically establishing communications between the gateway and a plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating communications and functions of the plurality of network devices and the security system components, wherein objects corresponding to at least one of the security

Art Unit: 2451

system components and the plurality of premise devices are maintained on the security server (pars [0017], [0027-0030], [0040] [0047-0048], [0078-0079], [0107], and see figs.1-2 and 6).

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Applicants are also respectfully reminded that broadly providing an automatic means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art. See MPEP 2144.04(III).

Art Unit: 2451

Regarding Claim 51, Naidoo teaches a method comprising:

forming a security network by automatically discovering a security system at a gateway and establishing communications between the gateway and the security system, the security system including security system components installed at a facility, wherein the gateway is located at a first location, wherein the gateway is coupled to a security server at a second location different from the first location (pars [0017], [0027-0030], [0040], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the security network and a plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the security network (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the plurality of network devices, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (pars [0027-0030], [0040] [0047-0048], [0078-0079], [0107], and see figs.1-2 and 6).

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

However, Rezvani in the field of the same endeavor teaches a registration

Art Unit: 2451

protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Applicants are also respectfully reminded that broadly providing an automatic means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art. See MPEP 2144.04(III).



Art Unit: 2451

***Conclusion***

14. Examiner has cited particular paragraphs, columns, and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY MEJIA whose telephone number is (571)270-3630. The examiner can normally be reached on Mon-Thur 9:30AM-8:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic

Application/Control Number: 12/189,788

Page 29

Art Unit: 2451

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/John Follansbee/  
Supervisory Patent Examiner, Art Unit 2451

/A.M./  
Patent Examiner, Art Unit 2451

<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 1 of 2

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-5,623,601 A	Vu, Hung T.	726/12
*	B	US-6,138,249 A	Nolet, James F.	714/25
*	C	US-2002/0114439 A1	Dunlap, John H.	379/219
*	D	US-2002/0133539 A1	Monday, Paul R.	709/203
*	E	US-2003/0038849 A1	Craven et al.	345/864
*	F	US-2003/0062997 A1	Naidoo et al.	340/531
*	G	US-2003/0147534 A1	Ablay et al.	380/270
*	H	US-2003/0189509 A1	Hayes et al.	341/176
*	I	US-6,686,838 B1	Rezvani et al.	340/506
*	J	US-6,756,998 B1	Bilger, Brent	715/764
*	K	US-2004/0189871 A1	Kurosawa et al.	348/552
*	L	US-2004/0199645 A1	Rouhi, Arash	709/227
*	M	US-7,015,806 B2	Naidoo et al.	340/531

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
N					
O					
P					
Q					
R					
S					
T					

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
U	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
V					
W					
X					

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 2 of 2

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification	
*	A	US-2006/0271695 A1	11-2006	Lavian, Yoel	709/229
*	B	US-2006/0282886 A1	12-2006	Gaug, Mark	726/005
*	C	US-2007/0146484 A1	06-2007	Horton et al.	348/159
*	D	US-2007/0130286 A1	06-2007	Hopmann et al.	709/217
*	E	US-7,249,317 B1	07-2007	Nakagawa et al.	715/209
*	F	US-2007/0192486 A1	08-2007	Wilson et al.	709/225
*	G	US-2007/0216783 A1	09-2007	Ortiz et al.	348/235
*	H	US-2008/0163355 A1	07-2008	Chu, Andrew	726/12
*	I	US-7,827,252 B2	11-2010	Hopmann et al.	709/217
*	J	US-7,884,855 B2	02-2011	Ortiz, Luis M.	348/211.8
	K	US-			
	L	US-			
	M	US-			


**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Index of Claims</b>  	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010	04/26/2011	04/29/2011	12/19/2011				
	1	✓	✓	✓	✓				
	2	✓	✓	✓	✓				
	3	✓	✓	✓	✓				
	4	✓	✓	-	-				
	5	✓	✓	✓	✓				
	6	✓	✓	✓	✓				
	7	✓	✓	✓	✓				
	8	✓	✓	✓	✓				
	9	✓	✓	✓	✓				
	10	✓	✓	✓	✓				
	11	✓	✓	✓	✓				
	12	✓	✓	✓	✓				
	13	✓	✓	✓	✓				
	14	✓	✓	✓	✓				
	15	✓	✓	✓	✓				
	16	✓	✓	✓	✓				
	17	✓	✓	✓	✓				
	18	✓	✓	✓	✓				
	19	✓	✓	✓	✓				
	20	✓	✓	✓	✓				
	21	✓	✓	✓	✓				
	22	✓	✓	✓	✓				
	23	✓	✓	✓	✓				
	24	✓	✓	✓	✓				
	25	✓	✓	✓	✓				
	26	✓	✓	✓	✓				
	27	✓	✓	✓	✓				
	28	✓	✓	✓	✓				
	29	✓	✓	✓	✓				
	30	✓	✓	✓	✓				
	31	✓	✓	✓	✓				
	32	✓	✓	✓	✓				
	33	✓	✓	✓	✓				
	34	✓	✓	✓	✓				
	35	✓	✓	✓	✓				
	36	✓	✓	✓	✓				

<b>Index of Claims</b>  	<b>Application/Control No.</b>  12189788	<b>Applicant(s)/Patent Under Reexamination</b>  BAUM ET AL.
	<b>Examiner</b>  ANTHONY MEJIA	<b>Art Unit</b>  2451

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010	04/26/2011	04/29/2011	12/19/2011				
	37	✓	✓	✓	✓				
	38	✓	✓	✓	✓				
	39	✓	✓	✓	✓				
	40	✓	✓	✓	✓				
	41	✓	✓	✓	✓				
	42	✓	✓	✓	✓				
	43	✓	✓	✓	✓				
	44	✓	✓	✓	✓				
	45	✓	✓	✓	✓				
	46	✓	✓	✓	✓				
	47	✓	✓	✓	✓				
	48	✓	✓	✓	✓				
	49	✓	✓	✓	✓				
	50	✓	✓	✓	✓				
	51	✓	✓	✓	✓				

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(generat\$3 creat\$3) near5 (network) near5 (download\$3 copying) near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:02
L2	0	(form\$3 creat\$3) near5 (network) near5 (copying copies sav\$3 stor\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:04
L3	43	(form\$3 creat\$3) near5 (network) near5 (copying copies sav\$3 stor\$3) near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:04
L4	34972799	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:05
L5	35	3 AND L4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:05
L6	6187	"6" AND (updat\$3) near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:06
L7	1	5 AND (updat\$3) near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:07
L8	10	(updat\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:07

L9	77	(updat\$3 near5 (firmware) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:12
L10	8	(generat\$3 creat\$3) near5 (network) near5 (download\$3 copying) near5 (firmware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:13
L11	0	9 AND 10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:13
L12	42	9 AND 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:26
L13	1003986	"77" AND 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:36
L14	42	9 AND 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:37
L15	33	14 AND (creat\$3 generat\$3 near5 network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:41
S1	2	"20060271695"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:01
S2	18	12/189757	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:01



S3	45868	709/201.ccls. 709/202.ccls. 709/203.ccls. 709/224.ccls. 709/225.ccls. 709/227.ccls. 717/101.ccls. 717/102.ccls. 707/203.ccls. 718/101.ccls. 726/1.ccls. 706/46.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:05
S4	34837379	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:05
S5	39563	S3 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:06
S6	3955	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:06
S7	201056	((generat\$3 creat\$3) near5 (network))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S8	797	S6 AND S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S9	659	S8 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S10	797	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)) AND ((generat\$3 creat\$3) near5 (network))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S11	659	S10 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11

S12	476	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)) AND ((generat\$3 creat\$3) near5 (network)) AND (security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S13	416	S12 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:12
S14	25	(automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors) near5 (security surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:19
S15	23	S14 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:20
S16	3	"7015806".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:24
S17	2	"6756998".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:32
S18	2	"20020103898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 16:49
S19	2	"6686838".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/26 19:18
S20	9	"20030062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:29

S21	15	"2003/0062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:30
S22	2	09/969521	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:41
S23	2	"20090077622"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/14 17:37
S24	2	"7996548".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 14:24
S25	2	"7746233".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 14:25
S26	8851	(security ADJ server (server)) near5 (controls) near5 (components devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:26
S27	1077	(security ADJ server (server)) near5 (controls) near5 (cameras)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:27
S28	34972574	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:27
S29	866	S27 AND S28	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:27

S30	253	S29 AND ("348"/\$3.ccls. "709"/\$3.ccls.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:29
S31	53	S30 AND (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:30
S32	30934	(embedd\$3 install\$3 replac\$3 updat\$3) near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:55
S33	1077	(security ADJ server (server)) near5 (controls) near5 (cameras)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:56
S34	34972574	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:56
S35	866	S33 AND S34	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:56
S36	253	S35 AND ("348"/\$3.ccls. "709"/\$3.ccls.)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:56
S37	53	S36 AND (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:56
S38	14	S32 AND S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 16:56

S39	52	(embedd\$3 install\$3 replac\$3 updat\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:00
S40	0	S39 AND S33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:00
S41	10	(replac\$3 updat\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:01
S42	42	(embedd\$3 install\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:02
S43	0	(embedd\$3 install\$3) near5 (operating ADJ system) near5 (gateway) near5 (control\$4 manag\$3) near5 (components cameras devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:03
S44	0	(embedd\$3 install\$3) near5 (operating ADJ system) near5 (gateway) near5 (cameras)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:04
S45	42	(embedd\$3 install\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:04
S46	36	S45 AND S34	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:04
S47	31	S45 AND (security surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:05

S48	31	S45 AND (security surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:06
S49	0	S45 AND (surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:07
S50	0	((embedd\$3 install\$3) near5 (operating ADJ system) near5 (gateway)) same (surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:07
S51	0	((embedd\$3 install\$3) near5 (operating ADJ system) near5 (gateway)) and (surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:08
S52	0	((updat\$3) near5 (operating ADJ system) near5 (gateway)) and (surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:54
S53	10	((updat\$3) near5 (operating ADJ system) near5 (gateway))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 17:54
S54	82	(gateway) near5 (stor\$3 sav\$3 copying copies) near5 (operating ADJ system (os))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:17
S55	67	S54 AND S34	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:17
S56	4150	(gateway) near5 (updat\$3 patch)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:19

S57	3	S56 AND S55	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:19
S58	4	(gateway) near5 (stor\$3 sav\$3 copying copies) near5 (operating ADJ system (os)) near5 (cameras devices clients)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:20
S59	8	(gateway) near5 (stor\$3 sav\$3 embedd\$3) near5 (operating ADJ systems (os)) near5 (cameras devices clients)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:23
S60	5	S59 AND (updat\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:25
S61	95	(gateway) near5 (control\$4 manag\$3) near5 (cameras surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:39
S62	964	(gateway) near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:39
S63	0	S61 AND S62	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:39
S64	22	S61 AND (software ADJ updates)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:39
S65	297	(gateway central) near5 (control\$4 manag\$3) near5 (cameras surveillance) AND (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:42

S66	254	S65 AND S34	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:43
S67	6839	(updat\$3) near5 (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:55
S68	2	S66 AND S67	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 18:55
S69	10	(updat\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:06
S70	2	(dynamically dynamic automatically self) near5 (updat\$3) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:11
S71	21	12/189757	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:20
S72	775	(dynamically dynamic automatically self) near5 (updat\$3) near5 ((firmware) operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:21
S73	804	(gateway central server) near5 (control\$4 manag\$3) near5 (cameras surveillance) AND (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:22
S74	4205	(gateway central server) near5 (control\$4 manag\$3) near5 (cameras surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:22



S75	0	S72 AND S74	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:22
S76	0	S72 AND S73	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:23
S77	4	S72 AND "348"/\$3.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:23
S78	1	(dynamically dynamic automatically self) near5 (updat\$3) near5 (firmware) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:25
S79	0	(seamlessly automatically) near5 (updat\$3) near5 (firmware) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:26
S80	437	(seamlessly automatically) near5 (updat\$3) near5 (firmware)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:27
S81	45024	S80 AMD S74	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:27
S82	0	S80 AND S74	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:27
S83	0	S80 AND S33	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:28

S84	12	(dynamically dynamic automatically self) near5 (updat\$3) near5 (firmware software driver) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:28
S85	2	(dynamically dynamic automatically self) near5 (updat\$3) near5 (firmware software driver) near5 ((surveillance monitoring camera) ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/15 19:29
S86	1	(form\$3 creat\$3) near5 (network) near5 (operating ADJ system) near5 (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 12:58
S87	1022	(form\$3 creat\$3) SAME (network) SAME (operating ADJ system) SAME (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 12:59
S88	297	(gateway central) near5 (control\$4 manag\$3) near5 (cameras surveillance) AND (operating ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:00
S89	0	S87 AND S88	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:00
S90	2559	(gateway central) near5 (control\$4 manag\$3) near5 (cameras surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:00
S91	0	S87 AND S90	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/19 13:00


## EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

L16	9	(generat\$3 creat\$3) near5 (network) near5 (download \$3 copying cop\$3 updat\$3) near5 ((firmware) (operating ADJ system)). CLM.	US-PGPUB; USPAT; UPAD	OR	ON	2011/12/19 13:46
L17	2177	709/200.ccls.	US-PGPUB; USPAT; UPAD	OR	ON	2011/12/19 13:46
L18	0	16 AND 17	US-PGPUB; USPAT; UPAD	OR	ON	2011/12/19 13:47

**12/ 19/ 2011 2:47:31 PM**

**C:\ Documents and Settings\ amejia\ My Documents\ EAST\ Workspaces\ 12189757.w sp**

<b>Search Notes</b>  	<b>Application/Control No.</b>  12189788	<b>Applicant(s)/Patent Under Reexamination</b>  BAUM ET AL.
	<b>Examiner</b>  ANTHONY MEJIA	<b>Art Unit</b>  2451

SEARCHED			
Class	Subclass	Date	Examiner
709	201, 202, 203, 224, 225, 227	12/19/2011	A.M.
717	101, 102	12/19/2011	A.M.
707	203	12/19/2011	A.M.
718	101	12/19/2011	A.M.
726	1	12/19/2011	A.M.
706	46	12/19/2011	A.M.

SEARCH NOTES		
Search Notes	Date	Examiner
EAST Class Limited w/Text Search (See Search History)	12/19/2011	A.M.
EAST Text Search (See Search History)	12/19/2011	A.M.
EAST Assignee Search (See Search History)	08/23/2010	A.M.
EAST Inventor Search (See Search History)	08/23/2010	A.M.

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

/A. M./ Examiner.Art Unit 2451	
-----------------------------------	--

**REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL  
(Submitted Only via EFS-Web)**

Application Number	12189788	Filing Date	2008-08-12	Docket Number (if applicable)	ICON.P001D3	Art Unit	2451
First Named Inventor	Marc Baum, et al			Examiner Name	Anthony Mejia		

**This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.**  
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

**SUBMISSION REQUIRED UNDER 37 CFR 1.114**

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_

Other \_\_\_\_\_

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other \_\_\_\_\_

**MISCELLANEOUS**

Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months \_\_\_\_\_  
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

Other \_\_\_\_\_

**FEES**

**The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**

The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No \_\_\_\_\_

**SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED**

Patent Practitioner Signature

Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Richard L. Gregory, Jr./	Date (YYYY-MM-DD)	2011-11-14
Name	Richard L. Gregory, Jr.	Registration Number	42607

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12189788
<b>Filing Date:</b>	12-Aug-2008
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Filer:</b>	Richard L. Gregory/Kim Moore
<b>Attorney Docket Number:</b>	ICON.P001D3

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				
Extension - 3 months with \$0 paid	2253	1	635	635



Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Request for continued examination	2801	1	465	465
<b>Total in USD (\$)</b>				<b>1100</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	11402768
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	98195
<b>Filer:</b>	Richard L. Gregory/Kim Moore
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	14-NOV-2011
<b>Filing Date:</b>	12-AUG-2008
<b>Time Stamp:</b>	17:13:37
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1100
RAM confirmation Number	4725
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / zip (if appl.)	Pages (if appl.)
SecureNet Technologies, LLC Exhibit 1003 Page 898					

1		ICONP001D3_amendment_response_14NOV2011.pdf	2810937 78f02e243e4b7029cd475aebb313985823c ea63d	yes	20
<b>Multipart Description/PDF files in .zip description</b>					
		<b>Document Description</b>	<b>Start</b>	<b>End</b>	
		Amendment After Final	1	1	
		Claims	2	9	
		Applicant Arguments/Remarks Made in an Amendment	10	19	
		Extension of Time	20	20	
<b>Warnings:</b>					
<b>Information:</b>					
2	Request for Continued Examination (RCE)	ICONP001D3_RCE_14NOV2011.pdf	697255 c267328a0585ff53dc08656a2b0d3b0e1d4 18e70	no	3
<b>Warnings:</b>					
<b>Information:</b>					
3	Fee Worksheet (SB06)	fee-info.pdf	32293 76a8021e73d6a2c2054eb2a652766add3be fad49	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			3540485		
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					

**IN THE UNITED STATES PATENT OFFICE**

In Re Application of: )  
 )  
 Marc Baum, et al. ) Examiner: Anthony Mejia  
 ) Art Unit: 2451  
 )  
 Application No.: 12/189,788 )  
 )  
 Filed: August 12, 2008 )  
 )  
 For: FORMING A SECURITY NETWORK )  
 INCLUDING INTEGRATED SECURITY )  
 SYSTEM COMPONENTS AND NETWORK )  
 DEVICES )

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE

Sir:

Applicant respectfully requests consideration of the following amendments and remarks contained herein in response to the Office Action mailed May 13, 2011.

AMENDMENTS

IN THE CLAIMS

1. (Currently amended) A method comprising:
  - coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components;
  - automatically discovering the plurality of security system components at the gateway and establishing communications between the gateway and the plurality of security system components;
  - automatically discovering a plurality of premise devices at the gateway and establishing communications between the gateway and the plurality of premise devices;
  - and
  - forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server.
  
2. (Original) The method of claim 1, comprising controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device.
  
3. (Original) The method of claim 2, wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

Claim 4 (Canceled).

5. (Previously presented) The method of claim 1, comprising using protocols of the security system to discover the security system components, wherein the gateway includes the protocols of the security system.
6. (Previously presented) The method of claim 1, comprising the gateway receiving protocols of the security system from the security server in response to a request, wherein the gateway uses the protocols received to discover the security system components.
7. (Original) The method of claim 1, wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components.
8. (Original) The method of claim 7, wherein the connection management component automatically discovers the premise devices.
9. (Original) The method of claim 7, wherein the connection management component automatically installs the premise devices in the security network.
10. (Original) The method of claim 7, wherein the connection management component automatically configures the premise devices for operation in the security network.
11. (Original) The method of claim 1, wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices.
12. (Original) The method of claim 1, wherein the gateway includes a device connect component that includes definitions of the security system components and the premise devices.

13. (Original) The method of claim 1, wherein the premise local area network is coupled to a wide area network via a premise router.
14. (Original) The method of claim 1, wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network.
15. (Original) The method of claim 1, wherein the gateway is coupled to the premise devices using a wireless coupling.
16. (Original) The method of claim 1, wherein the gateway is coupled to the security server via the internet.
17. (Original) The method of claim 1, wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location.
18. (Original) The method of claim 1, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link.
19. (Original) The method of claim 18, comprising transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link.
20. (Original) The method of claim 19, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

21. (Original) The method of claim 18, comprising transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable.
22. (Original) The method of claim 18, wherein the secondary communication link includes a broadband coupling.
23. (Original) The method of claim 18, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling.
24. (Original) The method of claim 18, comprising transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link.
25. (Original) The method of claim 24, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.
26. (Original) The method of claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.
27. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.
28. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the premise devices.



29. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.
30. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the premise devices.
31. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the security system components.
32. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the premise devices.
33. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the security system components.
34. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the premise devices.
35. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices.
36. (Original) The method of claim 1, wherein the security server manages communications with the security system components.
37. (Original) The method of claim 1, wherein the security server manages communications with the premise devices.
38. (Original) The method of claim 1, wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data.

39. (Original) The method of claim 38, wherein the notifications include one or more of short message service messages and electronic mail messages.
40. (Original) The method of claim 38, wherein the event data is event data of the security system components.
41. (Original) The method of claim 38, wherein the event data is event data of the premise devices.
42. (Original) The method of claim 1, wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link.
43. (Original) The method of claim 1, wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.
44. (Original) The method of claim 1, wherein the premise device is an Internet Protocol device.
45. (Original) The method of claim 1, wherein the premise device is a camera.
46. (Original) The method of claim 1, wherein the premise device is a touchscreen.
47. (Original) The method of claim 1, wherein the premise device is a device controller that controls an attached device.
48. (Original) The method of claim 1, wherein the premise device is a sensor.

49. (Currently amended) A method comprising:

forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location; and

automatically discovering a plurality of premise devices at the gateway and establishing a coupling between the gateway and the plurality of premise devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the gateway and the security network, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server.

50. (Currently amended) A method comprising:

automatically discovering a security system at a gateway and establishing communications between the gateway and the security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system; and

automatically discovering a plurality of network devices at the gateway and establishing communications between the gateway and the plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating into the gateway communications and functions of the plurality of network devices and the plurality of security system components, wherein objects corresponding to at least one of the plurality of security system components and the plurality of network devices are maintained on a remote server.

51. (Currently amended) A method comprising:

forming a security network by automatically discovering a security system at a gateway and establishing communications between the gateway and the security system,

the security system including security system components installed at a facility, wherein the gateway is located at a first location, wherein the gateway is coupled to a security server at a second location different than the first location;

automatically discovering a plurality of network devices at the gateway and establishing communications between the security network and the plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the gateway and the security network; and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the plurality of network devices, wherein objects corresponding to at least one of the security system components and the plurality of network devices are maintained on the security server.

REMARKS

Claims 1-3 and 5-51 were pending in the application. Claims 1-3 and 5-51 were rejected. Claims 1 and 49-51 are amended herein. No new matter is added by the amendments herein.

Request for Continued Examination under 37 C.F.R. 1.114

This response is accompanied by a Request for Continued Examination under 37 C.F.R. 1.114 and the required fee.

Petition For Extension Of Time

A Petition For Extension Of Time Under 37 CFR 1.136(a) is submitted herewith along with the appropriate fee amount for a three (3) month extension of time.

Rejections under 35 U.S.C. §103

Claims 1-3, 5-9, 11, 12, 15-25, 28, 30-45 and 48 were rejected under 35 U.S.C. §103(a) as being anticipated by United States (US) Patent Application Publication No. US 2003/0062997 A1 ("Naidoo") in view of United States Patent No. 6,756,998 ("Bilger") and further in view of United States Patent No. 6,686,838 ("Rezvani"). Applicant respectfully submits that the claims as amended herein are patentably distinct from Naidoo, Bilger and/or Rezvani. Moreover, Naidoo, Bilger and/or Rezvani fail to teach each and every element of claims 1-3, 5-9, 11, 12, 15-25, 28, 30-45 and 48 as presented herein.

The Examiner at page 8 of the Office Action states that Naidoo does not explicitly teach the step of "automatically discovering security system components at the gateway". Applicant agrees.

The Examiner at page 8 of the Office Action states that Naidoo and Bilger do not explicitly teach the step of "automatically discovering a plurality of premise devices at a gateway". Applicant agrees.

Regarding claim 1 as amended herein, Applicant respectfully submits that Naidoo describes a system and method for distributed monitoring and remote verification of conditions surrounding an alarm condition in a security system (abstract). Naidoo

describes that the security system includes a security gateway, which is typically located at the desired premises to be monitored, and a monitoring client, typically located at a central station and operatively coupled to security gateway through a network. Naidoo describes that often, the security gateway is located at the target site, however, on some occasions, some or all components of security gateway may be located remotely, but remain operatively coupled to security sensors and video cameras which are at the premises (paragraph 0028).

Naidoo describes that the security gateway is a processor-based device that functions to detect alarm conditions at a target site and to capture information relating to such alarm conditions (paragraph 0032). Naidoo describes that, upon detection of an alarm condition, the security gateway captures video (usually through an attached video camera) of the target site, and sends the video to security system server in real time (paragraph 0028).

Naidoo describes that a monitoring client is generally a software program that may be used to display some or all of the information provided by security gateway. Monitoring client may be a stand-alone program or integrated into one or more existing software programs. Naidoo describes that one or more operators may then use this information to evaluate whether the alarm condition corresponds to an actual alarm condition and then take additional action, if desired, such as alerting the appropriate authorities (paragraph 0032).

Naidoo describes that the security system includes one or more sensors coupled to security gateway for the purpose of detecting alarm conditions. The security system is not limited to any specific type or model of sensor. Any sensor may be used, depending on the desired type and level of protection. Alarm sensors may be wired directly into an alarm control panel built into the security gateway or they may be wirelessly connected (paragraph 0033). Naidoo describes that the security system also includes one or more video cameras that are operable to capture video data of monitored premises. Naidoo describes that the security gateway may be configured to create an association between one or more sensors and an associated video camera (paragraph 0034).

Regarding claim 1, as amended, Applicant respectfully submits that Naidoo does not disclose coupling a gateway to a local area network located in a first location and a

security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

As set forth above, Naidoo describes that the security gateway is a processor-based device that functions to detect alarm conditions at a target site and to capture information relating to such alarm conditions (paragraph 0032). Naidoo describes that, upon detection of an alarm condition, the security gateway captures video (usually through an attached video camera) of the target site, and sends the video to security system server in real time (paragraph 0028).

Naidoo describes that a monitoring client is generally a software program that may be used to display some or all of the information provided by security gateway. Monitoring client may be a stand-alone program or integrated into one or more existing software programs. Naidoo describes that one or more operators may then use this information to evaluate whether the alarm condition corresponds to an actual alarm condition and then take additional action, if desired, such as alerting the appropriate authorities (paragraph 0032). Therefore, Naidoo simply describes a security gateway that detects alarm conditions at a target site and forwards the detected conditions and related information to a security system server whereupon a monitoring client displays some or all of alarm condition information. Naidoo nowhere teaches coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo. Applicant finds no teaching in Bilger to overcome the deficiencies of Naidoo set forth above.

Applicant respectfully submits that Bilger describes a home automation system

interface and method for interfacing with a system that automatically controls controlled devices throughout a home. A unique architecture of occupancy sensors includes entry/exit sensors for detecting movement through doorways that separate rooms in the home, room motion sensors for detecting room occupancy, spot sensors to detect occupancy of specific locations within the rooms, and house status sensors to detect the status of certain parameters of the home. A central controller communicates with the sensors and controlled objects over a communications network, where the sensors and controlled objects can be added to the system in a 'plug and play manner (abstract).

FIG. 7 A illustrates the preferred configuration for network 14, which includes a control/sensor network 52 wired to each "room" 4 in the house. Control/sensor network 52 is a single set of wires bused throughout the house, preferably while the house is under initial construction. Once the AC power lines are installed but before the walls are completed, the network wiring can be easily installed in just one day, often times using the same holes, conduit and/or junction boxes as the AC lines. The control/sensor network 52 is connected to all the sensors 10 and controlled objects 12, as well as to the central controller 16 (column 9, lines 56-66).

FIG. 7A illustrates a random configuration for control/sensor network 52. FIGS. 7B-7D illustrate alternate configurations for routing control/sensor network 52 through the house. A single set of wires can be woven throughout the house in a straight bus or daisy chain configuration, as illustrated in FIG. 7B. The central controller could have one 15 or more central hubs 58 that have individual communications lines 60 each connected to a single sensor 10 or controlled object 12, as illustrated in FIG. 7C. The advantage of this embodiment is that the sensors 10 and controlled objects 12 can use standard Ethernet twisted pair connectors and hubs, but the drawback is that the system is less versatile, and more costly to wire. Alternately, the control/sensor network 52 could be wireless, where each sensor 10 and controlled object 12 including a transceiver 54 that communicates with one or more central transceivers 56 of the central controller 16 (as illustrated in FIG. 7D), or with other transceivers 54 in a token bus configuration (as illustrated in FIG. 7E). Lastly, control/sensor network 52 could be a powerline based system (e.g. X-10 system), where the sensors 10 controlled objects 12 and central controller 16 communicate with each other over the existing AC power lines in the house



(column 10, lines 9-31). None of these embodiments teach coupling a gateway to a local area network located in a first location and a security server in a second location (emphasis added). Therefore, Bilger clearly does not teach coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo in view of Bilger. Applicant finds no teaching in Rezvani to overcome the deficiencies of Naidoo in view of Bilger.

Applicant respectfully submits that Rezvani describes systems and methods for providing registration at a remote site that may include, for example, a monitoring module that may communicate with a remote site (abstract). Devices at one or more locations may interface with the monitoring modules. Rezvani describes that one or more monitoring modules and their associated interfaced devices may be referred to as "installations." Devices may include, for example, video cameras, still cameras, motion sensors, audible detectors, any suitable household appliances, or any other suitable device. Rezvani describes that monitoring modules may be stand-alone devices, software applications, any suitable combination of software and hardware, or any other suitable architecture (column 1, lines 41-50).

Rezvani describes that monitoring modules may communicate with one or more remote sites via a suitable communications network using any suitable communications protocol. The monitoring modules and remote sites may use a registration protocol to transmit registration information. The registration information may get stored in a database at the remote site (column 1, lines 51-56).

Rezvani describes that an installation, any of its components, or both may be associated with a particular user account (column 1, lines 59-60). Association of an installation, installation elements, or both with corresponding user accounts may take place at the remote site. The remote site may make the association using any suitable

database construct that may serve to cross reference the installation, installation elements, or both with user accounts (column 1, line 65 to column 2, line 3).

Rezvani describes that devices may be automatically detected by a monitoring module (column 2, lines 37-38). Rezvani describes that as new devices are added to a registered monitoring module, the monitoring module may automatically (i.e., without any user interaction) detect the presence of the new devices and automatically notify remote site of the presence of the new devices. Remote site may, in turn, add the new devices to the database (column 21, lines 5-11).

Although Rezvani discloses the automatic detection of devices, the detected device information is directed to and registered at a remote site. Rezvani teaches automatically detecting a device at an installation, extracting registration information from the device, communicating the registration information to a remote site that does not have requisite registration information associated with the device using a communications network, registering the device with the remote site based on the registration information, and associating the device at the remote site with a user account based on the registration information (claim 1, column 21, lines 41-53). Rezvani therefore teaches the automatic detection and extraction of registration information from devices at a first location (an installation), the communication of the registration information to a remote location, registration of devices at the remote location using the extracted information and the association of the devices at the remote site with a user account. However, the association of devices with a user account does not disclose (and Rezvani does not otherwise teach) coupling a gateway to a local area network located in a first location and a security server in a second location and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, wherein objects corresponding to at least one of the security system components and the plurality of premise devices are maintained on the security server (emphasis added).

For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani.

As claims 2-3, 5-9, 11, 12, 15-25, 28, 30-45 and 48 depend from amended claim 1 and include further limitations thereon, and since amended claim 1 is patentable over

Naidoo in view of Bilger and further in view of Rezvani, Applicant submits that claims 2-3, 5-9, 11, 12, 15-25, 28, 30-45 and 48 are patentable over by Naidoo in view of Bilger and further in view of Rezvani.

Claims 10 and 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Tanaka et al., US Patent Application Publication number US 2004/0037295 A1 ("Tanaka").

At page 17 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the connection management component automatically configures the premise devices for operation in the security network". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claims 10 and 29 which depend from amended claim 1, Applicant does not find any teaching in Tanaka that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 10 and 29 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Tanaka and respectfully requests that the rejection be withdrawn and allowance thereof.

Claim 26 was rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Patterson, US Patent Application Publication number US 2005/0086126 A1 ("Patterson").

At page 19 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the security server creates, modifies and terminates users corresponding to the security system". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claim 26 which depends from amended claim 1, Applicant does not find any

teaching in Patterson that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claim 26 is patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Patterson and respectfully requests that the rejection be withdrawn and allowance thereof.

Claim 27 was rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moyer et al., US Patent Application Publication number US 2002/0103898 A1 ("Moyer").

At page 20 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the security server creates, modifies and terminates couplings between the gateway and the security system components". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claim 27 which depends from amended claim 1, Applicant does not find any teaching in Moyer that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claim 27 is patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moyer and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 46-47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Lingemann, US Patent Application Publication number US 2006/0009863 A1 ("Lingemann").

At pages 20-21 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "wherein the network device is a touchscreen". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore,

Attorney Docket No. ICON.P001D3

regarding claims 46-47 which depend from amended claim 1, Applicant does not find any teaching in Lingemann that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 46-47 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Lingemann and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 13-14 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moore et al., US Patent Application Publication number US 2007/0061266 A1 ("Moore").

At page 22 of the Office Action, the Examiner states that Naidoo/Bilger/Rezvani does not explicitly disclose "the premise local area network is coupled to a wide area network via a premise router". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo in view of Bilger and further in view of Rezvani does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo in view of Bilger and further in view of Rezvani. Furthermore, regarding claims 13-14 which depend from amended claim 1, Applicant does not find any teaching in Moore that overcomes the deficiencies in Naidoo in view of Bilger and further in view of Rezvani described above. For at least these reasons, Applicant submits that claims 13-14 are patentable over Naidoo in view of Bilger, further in view of Rezvani and further in view of Moore and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 49-51 were rejected as being unpatentable over Naidoo in view of Rezvani.

Applicant respectfully submits that for the reasons already set forth above, amended claim 1 is patentable over Naidoo in view of Rezvani.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 49 and, as such, amended claim 49 is patentable over Naidoo in view of Rezvani. For at least these reasons, Applicant submits that amended claim 49 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and

allowance therefore.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo in view of Rezvani does not teach or suggest each and every limitation of amended claim 50 and, as such, amended claim 50 is patentable over Naidoo in view of Rezvani. For at least these reasons, Applicant submits that amended claim 50 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and allowance therefore.

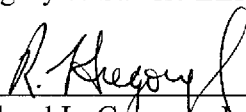
Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo in view of Rezvani does not teach or suggest each and every limitation of amended claim 51 and, as such, amended claim 51 is patentable over Naidoo in view of Rezvani. For at least these reasons, Applicant submits that amended claim 51 is patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and allowance therefore.

### Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully submit that the rejections under 35 U.S.C. §103 have been overcome, and their withdrawal is respectfully requested. Applicants submit that claims 1-3 and 5-51 are in condition for allowance. The allowance of the claims is earnestly requested. If in the opinion of Examiner Mejia a telephone conference would expedite the prosecution of the subject application, or if there are any issues that remain to be resolved prior to allowance of the claims, Examiner Mejia is encouraged to call Rick Gregory at 408.821.8080.

Date: November 14, 2011

Respectfully submitted,  
Gregory & Sawrie LLP



Richard L. Gregory, Jr., Reg. No. 42,607  
Telephone: 408.821.8080

Gregory & Sawrie LLP  
2018 Bissonnet Street  
Houston, Texas 77005  
Fax: 713-364-1397

Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> <b>FY 2009</b> <i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i>		Docket Number (Optional) ICON.P001D3	
Application Number 12/189,788		Filed August 12, 2008	
For Forming A Security Network Including Integrated Security System Components and Network Devices			
Art Unit 2451		Examiner MEJIA, Anthony	
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application. The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):			
		<u>Fee</u>	<u>Small Entity Fee</u>
<input type="checkbox"/>	One month (37 CFR 1.17(a)(1))	\$130	\$65 \$ _____
<input type="checkbox"/>	Two months (37 CFR 1.17(a)(2))	\$490	\$245 \$ _____
<input checked="" type="checkbox"/>	Three months (37 CFR 1.17(a)(3))	\$1110	\$555 \$ <u>635</u>
<input type="checkbox"/>	Four months (37 CFR 1.17(a)(4))	\$1730	\$865 \$ _____
<input type="checkbox"/>	Five months (37 CFR 1.17(a)(5))	\$2350	\$1175 \$ _____
<input checked="" type="checkbox"/>	Applicant claims small entity status. See 37 CFR 1.27.		
<input type="checkbox"/>	A check in the amount of the fee is enclosed.		
<input checked="" type="checkbox"/>	Payment by credit card. Form PTO-2038 is attached.		
<input type="checkbox"/>	The Director has already been authorized to charge fees in this application to a Deposit Account.		
<input type="checkbox"/>	The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number _____.		
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>			
I am the	<input type="checkbox"/>	applicant/inventor.	
	<input type="checkbox"/>	assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).	
	<input checked="" type="checkbox"/>	attorney or agent of record. Registration Number <u>42,607</u>	
	<input type="checkbox"/>	attorney or agent under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____	
/Richard L. Gregory Jr./		November 14, 2011	
Signature		Date	
Richard L. Gregory Jr.		408-676-8080	
Typed or printed name		Telephone Number	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.			
<input checked="" type="checkbox"/>	Total of <u>1</u> forms are submitted.		

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/189,788</b>	Filing Date <b>08/12/2008</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =	OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL		TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT	<b>11/14/2011</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 50	Minus ** 51	= 0	X \$30 =	0	OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus ***4	= 0	X \$125 =	0	OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE	<b>0</b>	OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	X \$ =		OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE


\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
/DONNA SMALLS LOGAN/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



<b>Application Number</b> 	<b>Application/Control No.</b> 12/189,788	<b>Applicant(s)/Patent under Reexamination</b> BAUM ET AL.

<b>Document Code - DISQ</b>	<b>Internal Document – DO NOT MAIL</b>
-----------------------------	--

<b>TERMINAL DISCLAIMER</b>	<input checked="" type="checkbox"/> <b>APPROVED</b>	<input type="checkbox"/> <b>DISAPPROVED</b>
Date Filed : 03/01/2011	<b>This patent is subject to a Terminal Disclaimer</b>	

<b>Approved/Disapproved by:</b>
Dorethea Lawrence 5 tds approved

U.S. Patent and Trademark Office



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes sub-tables for EXAMINER (MEJIA, ANTHONY), ART UNIT (2451), PAPER NUMBER, NOTIFICATION DATE (05/13/2011), and DELIVERY MODE (ELECTRONIC).

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

- rick@gregorymartensen.com
mike@gregorymartensen.com
vlad@gregorymartensen.com



## **DETAILED ACTION**

### ***Response to Amendment***

1. Acknowledgement is made that Claim 4 has been canceled. Claims 1, 5-6 and 49-51 have been amended in the instant application and now being presented.

### ***Priority***

2. Applicant's claim for the benefit of a prior-filed Application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has complied with the conditions for receiving the benefit of an earlier filing date.

### ***Double Patenting***

3. The rejection presented in the previous Office Action is withdrawn in view of terminal disclaimers filed on **01 March 2011** have been reviewed and are accepted. The terminal disclaimers have been recorded.

### ***Response to Arguments***

4. Applicant's alleged arguments, see pages 10-19 of Remarks, filed, **01 March 2010**, with respect to Claims 1-3, 7-8, 11-12, 15-25, 28, 30-45 and 48-51 rejection under 35 U.S.C. 102(b) and Claims 4-6, 9-10, 26-27, 13-14, and 46-47 rejected under 35 U.S.C. 103 (a) have been fully considered but are not persuasive.

5. As per Claims 1, 49-51 applicants submit that Naidoo does not teach every limitation recited in the claim. Applicants argue that Naidoo simply teaches the

Art Unit: 2451

gateway's use of wireless capabilities and receiving wireless communications. These disclosures of wireless capabilities nowhere teaches: "...automatically discovering a plurality of security system components at the gateway and establishing communications between the gateway and the plurality of security system components, and automatically discovering a plurality of premise devices at the gateway and establishing communications between the gateway and the plurality of premise devices, and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components, and forms a security network by electronically integrating into the gateway communications and functions of the plurality of premise device and the plurality of security components (emphasis added).

As to applicant's arguments above, Examiner disagrees that Naidoo does not explicitly teach the steps of: "... electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise device and the plurality of security components...". Naidoo clearly teaches the step of: "...forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise device and the plurality of security components..."

Naidoo discloses a security system for monitoring a premises by integrating broadband features, including audio and video capabilities, web access and wireless capabilities which is typically located at the desired premises 110 to be monitored, and a monitoring

Art Unit: 2451

client 133, typically located at a central station and operatively coupled to security gateway 115 through a network 120. Often, security gateway 115 is located at the target site. However, on some occasions, some or all components of security gateway 115 may be located remotely, but remain operatively coupled to security sensors 105 and video cameras 112 which are at the premises. The components of security gateway 115 are configured to communicate with one another through system bus 605. In other embodiments, some or all of the components may be directly connected or otherwise operatively coupled to one another (*see* pars [0027-0030], [0047-0048], and [0078-0079], and *see* figs.1-2 and 6).

Examiner agrees that Naidoo does not explicitly teach argued limitations: *automatically discovering security system components and plurality of premise devices at the gateway* as argued by applicant's above. Examiner respectfully reminds Applicants that only the broadest reasonable interpretation in light of the specification and taking into account the meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art is required (MPEP §2111) and applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. *See In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986)

Upon further consideration, Bilger in a similar field of endeavor discloses a home automation system interface for interfacing with a system that automatically controls controlled devices throughout the home including the step of *automatically discovering*

Art Unit: 2451

*security system components at the gateway* (e.g., control objects are plug and play compatible and are automatically recognized by the central controller once connected to the network, col.8, lines 55-67).

The combined teachings of Naidoo and Bilger do not explicitly teach the step of *automatically discovering a plurality of premise devices at a gateway*.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Bilger in order Naidoo's components to automatically install devices to the security system. One of ordinary skill in the art would have been motivated because it would ease installation of components by automatically installing the device to the security system.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art

Art Unit: 2451

would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Applicants are also respectfully reminded that broadly providing an automatic means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art. See MPEP 2144.04(III)

6. As per Claims 4-6, Applicant also does not find any teachings in Rezvani that overcomes the deficiencies in Naidoo as discussed above. Specifically, applicants argue that Rezvani does not disclose the limitation: “...forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and plurality of security system components (emphasis added).

7. As per Claims 9, 10, 29, 26, 27, 46-47, 13-14, applicant’s arguments are the same as above.

As to Applicants arguments above, Applicant’s arguments have been fully considered but are not persuasive for the same reasons as discussed above.



Art Unit: 2451

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-3, 5-9, 11-12, 15-25, 28, 30-45, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo et al. (US 2003/0062997) (hereinafter as Naidoo) in further view of Bilger (US 6,756,998) and in further view of Rezvani et al. (US 6,686,838) (hereinafter as Rezvani).

Regarding Claim 1, Naidoo teaches a method comprising:

coupling a gateway to a local area network located in a first location and a security server in a second location (see figs.1-2), wherein the first location includes a security system comprising:

a plurality of security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the gateway and the security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the gateway and premise devices pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

Art Unit: 2451

forming a security network by electronically integrating, via the gateway, communications and functions of the plurality of premise devices and the security system components, (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

The teachings of Naidoo do not explicitly teach the step of *automatically discovering security system components*.

However, Bilger in a similar field of endeavor discloses a home automation system interface for interfacing with a system that automatically controls controlled devices throughout the home including the step of *automatically discovering security system components at the gateway* (e.g., control objects are plug and play compatible and are automatically recognized by the central controller once connected to the network, col.8, lines 55-67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Bilger in order Naidoo's components to automatically install devices to the security system. One of ordinary skill in the art would have been motivated because it would ease installation of components by automatically installing the device to the security system.

In further the combined teachings of Naidoo and Bilger do not explicitly teach the step of *automatically discovering a plurality of premise devices at a gateway*.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may

Art Unit: 2451

gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Regarding Claim 2, Naidoo further teaches the step of controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device (pars [0040-0041]).

Regarding Claim 3, Naidoo further teaches the step wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices (par [0040] and see fig.2).

Regarding Claim 5, Naidoo-Rezvani-Bilger discloses the method of claim 4, comprising using protocols of the security system to discover the security system

Art Unit: 2451

components, wherein the gateway includes the protocols (see Rezvani; col. 2/lines 27-36; the remote sites may validate received registration protocol messages used during the new object discovery process to discovery new devices).

Regarding Claim 6, Naidoo-Rezvani-Bilger discloses the method of claim 4, comprising requesting and receiving protocols of the security system from the security server, wherein the gateway receives and uses the protocols to discover the security system components (see Rezvani; col. 2, lines 27-36; the remote sites may validate received registration protocol messages used during the new object discovery process to discovery new devices).

Regarding Claim 7, Naidoo further teaches the step wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components (pars [0069], [0079], and [0087]).

Regarding Claim 8, Naidoo further teaches the step wherein the connection management component automatically discovers the premise devices (par [0040] and see fig.2).

Regarding Claim 9, Bilger teaches Cross will automatically install sensor in the selected room (col. 20, lines 1-13).

Art Unit: 2451

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Bilger in order Naidoo's components to automatically install devices to the security system. One of ordinary skill in the art would have been motivated because it would ease installation of components by automatically installing the device to the security system.

Regarding Claim 11, Naidoo further teaches the step wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices (par [0099]).

Regarding Claim 12, Naidoo further teaches the step wherein the gateway includes a device connect component that includes definitions of the security system components and the premise devices (pars [0080-0081]).

Regarding Claim 15, Naidoo further teaches the step wherein the gateway is coupled to the premise devices using a wireless coupling (par [0033]).

Regarding Claim 16, Naidoo further teaches the step wherein the gateway is coupled to the security server via the internet (par [0030]).

Regarding Claim 17, Naidoo further teaches the step wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location (par [0043] and see fig.2).

Regarding Claim 18, Naidoo further teaches wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link (par [0043] and see fig.2).

Regarding Claim 19, Naidoo further teaches the step of transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link (par [0043] and see fig.2).

Regarding Claim 20, Naidoo further teaches the step wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of:

security system components and premise devices, and data received by at least one of security system components and premise devices (pars [0069], and [0080-0081]).

Regarding Claim 21, Naidoo further teaches the step of transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable (par [0043]).

Regarding Claim 22, Naidoo further teaches wherein the secondary communication link includes a broadband coupling (pars [0027] and [0122]).

Regarding Claim 23, Naidoo further teaches the step wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling (par [0043]).

Regarding Claim 24, Naidoo further teaches the step of transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link (pars [0027-0028], [0043], and [0046]).

Regarding Claim 25, Naidoo further teaches wherein the event data comprises changes in device states of at least one of:

security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices (pars [0069], and [0080-0081]).

Regarding Claim 28, Naidoo further teaches wherein the security server creates modifies and terminates couplings between the gateway and the premise devices (pars [0099-0101]).

Regarding Claim 30, Naidoo further teaches wherein wherein the security server performs creation, modification, deletion and configuration of the premise devices (pars [0099-0101]).

Regarding Claim 31, Naidoo further teaches wherein the security server creates automations, schedules and notification rules associated with the security system components (par [0045]).

Regarding Claim 32, Naidoo further teaches wherein the security server creates automations, schedules and notification rules associated with the premise devices (pars [0027-0028] and [0045]).

Regarding Claim 33, Naidoo further teaches the step wherein the security server manages access to current and logged state data for the security system components (pars [0049-0050]).



Art Unit: 2451

Regarding Claim 34, Naidoo further teaches the step wherein the security server manages access to current and logged state data for the premise devices (pars [0027-0028] and [0049-0050]).

Regarding Claim 35, Naidoo further teaches the step wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices (pars [0027-0028] and [0049-0050]).

Regarding 36, Naidoo further teaches the step wherein the security server manages communications with the security system components (par [0049]).

Regarding 37, Naidoo further teaches the step wherein the security server manages communications with the premise devices (pars [0027-0028] and [0049]).

Regarding 38, Naidoo further teaches the step wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data (par [0053]).

Regarding 39, Naidoo further teaches the step wherein the notifications include one or more of short message service messages and electronic mail messages (par [0069]).

Art Unit: 2451

Regarding Claim 40, Naidoo further teaches the step wherein the event data is event data of the security system components (par [0053]).

Regarding Claim 41, Naidoo further teaches the step wherein the event data is event data of the premise devices (pars [0027-0028] and [0053]).

Regarding Claim 42, Naidoo further teaches the step wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link (pars [0027-0028], [0043], and [0046]).

Regarding Claim 43, Naidoo further teaches the step wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers (par [0059]).

Regarding Claim 44, the method of claim 1, wherein the premise device is an Internet Protocol device (par [0037]).

Regarding Claim 45, Naidoo further teaches the step wherein the premise device is a camera (pars [0040-0041]).

Regarding Claim 48, Naidoo further teaches the step wherein the premise device is a sensor (pars [0040-0041]).

8. Claims 10 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Tanaka et al. (US 2004/0037295).

Regarding Claim 10, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of Claim 7, *wherein the connection management component automatically configures the premise devices for operation in the security network.*

Tanaka in the field of the same endeavor teaches creating a virtual local area network using a graphical user interface. In particular, Tanaka teaches the server automatically creates configuration information of the switch (see Tanaka: par [0083]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Tanaka in order for Naidoo server to perform configurations on the device. Tanaka teachings enabled Naidoo/Bilger/Rezvani to create, modify, and delete configuration settings of the switch. One of ordinary skill in the art would have been motivated because allowing for configurations to be created, modified and deleted increase the flexibility of a device by allowing configurations to be created, modified and deleted.

Art Unit: 2451

Regarding Claim 29, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani discloses the method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.

Tanaka in the field of the same endeavor teaches creating a virtual local area network using a graphical user interface. In particular, Tanaka teaches the server automatically creates configuration information of the switch and deletes the VLAN link. The server automatically issues command to delete the connection to the switch (see Tanaka; [0083]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Tanaka in order for Naidoo/Bilger/Rezvani server to perform actions on the device configurations. Tanaka teachings enabled Naidoo/Bilger/Rezvani to create, modify, and delete configuration settings of the switch. One of ordinary skill in the art would have been motivated because allowing for configurations to be created, modified and deleted increase the flexibility of a device by allowing configurations to be created, modified and deleted.

9. Claims 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over in further view of Naidoo in further view of Bilger in further view of Rezvani and in further view of Patterson (US 2005/0086126).

Art Unit: 2451

Regarding Claim 26, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of Claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.

Patterson, in the field of the same endeavor teaches managing and linking network accounts to share access privileges among accounts. In particular, Patterson teaches that the server may create account, upgrade an account, or terminate the upgrading of an account (see Patterson; [0046]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Patterson in order for the server of Naidoo/Bilger/Rezvani to create, upgrade, and terminate accounts. One of ordinary skill would be motivated because Patterson suggest it would be desirable for an environment having different levels of access, a provider may charge higher fees for accounts with higher levels of access. Accordingly, from the provider's standpoint, it is desirable to encourage users to purchase more expensive subscriptions, and so the provider often attempts to make the accounts with higher levels of access more appealing to users (see Patterson; [0002]).

10. Claims 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over in further view of Naidoo in further view of Bilger in further view of Rezvani and in further view of Moyer et al. (US 2002/0103898).

Art Unit: 2451

Regarding Claim 27, Naidoo/Bilger/Rezvani discloses the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.

Moyer in the field of the same endeavor teaches Session Initiated Protocol (SIP) to communicate with network capable appliances by leveraging SIP capabilities to directly communicating with the appliances. In particular, Moyer teaches that SIP is an application layer control and signaling protocol used for creating, modifying and terminating communication sessions between participants (see Moyer; [0013]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Moyer in order for Naidoo/Bilger/Rezvani servers to create, modify, and terminate communication between the gateway and the security system utilizing SIP. One of ordinary skill in the art would be motivated because SIP is designed to be independent of the underlying transport layer and it can run on TCP, UDP, or SCTP.

11. Claim 46-47 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Lingemann (US 2006/0009863).

Regarding claim 46, Naidoo/Bilger/Rezvani the invention substantially, however Naidoo/Bilger/Rezvani does not explicitly disclose the method of claim 1, wherein the

Art Unit: 2451

network device is a touchscreen.

Lingemann in the field of the same endeavor teaches building an automation system including user interface units with touchscreen. In particular, Lingemann teaches (see Lingemann; fig. 10, [0076]; a touch screen interface unit as illustrated in fig. 10 used for controlling electrical devices).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Lingemann in order for Naidoo's device to incorporate a touchscreen. One of ordinary skill in the art would have been motivated because a touchscreen would provide an ease of interaction by allowing the user to interact with what is displayed directly on the hand, where it is displayed, rather than indirect with a mouse or touchpad.

Regarding Claim 47, Naidoo/Bilger/Rezvani discloses the method of claim 24, wherein the network device is a device controller that controls an attached device (see Lingemann; fig. 10, [0076]; a touch screen interface unit as illustrated in fig. 10 used for controlling electrical devices).

12. Claim 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in further view of Bilger in further view of Rezvani and in further view of Moore et al. (US 2007/0061266).

Regarding Claim 13, Naidoo/Bilger/Rezvani substantially discloses the method of

Art Unit: 2451

claim 1, wherein the premise local area network is coupled to a wide area network. (see Naidoo; fig. 2; [0047-0048, 0087]; the security gateway is located in the premise which is considered a LAN. The security gateway is also connected to the internet and the security system server located at the data center which is consider to be the WAN).

However, Naidoo/Bilger/Rezvani does not explicitly disclose the premise local area network is coupled to a wide area network via a premise router.

Moore in the field of the same endeavor teaches large-scale, reliable, and secure foundations for distributed databases and content management systems combining unstructured and structured data, and allowing post-input reorganization to achieve a high degree of flexibility. In particular, Moore teaches a router that forward data packets across an internet work through a process known as routing that act as a junction between two networks (see Moore; [0217]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Moore in order for Naidoo/Bilger/Rezvani premise location to include a router that act as a junction between two networks. One of ordinary skill in the art would have been motivated because the router would have improved Naidoo/Bilger/Rezvani teachings by enabled data packets to be routed to networks.

Regarding Claim 14, the combined teachings of Naidoo/Bilger/Rezvani and Moore further teach wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network (see Naidoo; fig. 2;



Art Unit: 2451

[0047-0048, 0087]; the security gateway is located in the premise which is considered a LAN. The security gateway is also connected to the internet and the security system server located at the data center which is considered to be the WAN and Moore use of routers (see Moore; [0217]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo/Bilger/Rezvani with the teachings of Moore in order for Naidoo/Bilger/Rezvani premise location to include a router that act as a junction between two networks. One of ordinary skill in the art would have been motivated because the router would have improved Naidoo/Bilger/Rezvani teachings by enabled data packets to be routed to networks.

13. Claims 49-51 rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo and in further view of Rezvani.

Regarding Claim 49, Naidoo teaches a method comprising:

forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

establishing a coupling between the gateway and a plurality of premise devices located at the first location, wherein the gateway electronically integrates

Art Unit: 2451

communications and functions of the plurality of premise devices and the security system components into the gateway and security network (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Regarding Claim 50, Naidoo teaches a method comprising:

Art Unit: 2451

automatically discovering a security system at a gateway and establishing communications between a gateway and a security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system (pars [0027-0030], [0047-0048], and [0078-0079], and see figs. 1-2 and 6); and

automatically establishing communications between the gateway and a plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating communications and functions of the plurality of network devices and the security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see fig. 1 and 6).

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the

Art Unit: 2451

invention was made to modify the teachings of Naidoo/Bilger with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Regarding Claim 51, Naidoo teaches a method comprising:

forming a security network by automatically discovering a security system at a gateway and establishing communications between the gateway and the security system, the security system including security system components installed at a facility (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the security network and a plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the security network (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the network devices (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

Art Unit: 2451

Naidoo does not explicitly teach the step of automatically discovering the plurality of network devices at the gateway.

However, Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically registry devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Naidoo with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

***Conclusion***

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

15. Reply to a final rejection or action must include cancellation of, or appeal from the rejection of, each rejected claim. If any claim stands allowed, the reply to a final rejection or action must comply with any requirements or objections as to form (see 1.113). If prosecution in an application is closed, an applicant may request continued examination of the application by filing a submission and the fee set forth in § 1.17(e) prior to the earliest of: (c) A submission as used in this section includes, but is not limited to, an information disclosure statement, an amendment to the written description, claims, or drawings, *new arguments, or new evidence in support of patentability*. If reply to an Office action under 35 USC 132 is outstanding, the submission must meet the reply requirements of § 1.111 (see MPEP 706.07)

Art Unit: 2451

Examiner has cited particular paragraphs, columns, and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY MEJIA whose telephone number is (571)270-3630. The examiner can normally be reached on Mon-Thur 9:30AM-8:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

Application/Control Number: 12/189,788

Page 30

Art Unit: 2451

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KAMAL B DIVECHA/  
Primary Examiner, Art Unit 2451

/A.M./  
Patent Examiner, Art Unit 2451



<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0062997 A1	Naidoo et al.	340/531
*	B	US-6,686,838 B1	Rezvani et al.	340/506
*	C	US-6,756,998 B1	Bilger, Brent	715/764
*	D	US-7,015,806 B2	Naidoo et al.	340/531
*	E	US-2006/0271695 A1	Lavian, Yoel	709/229
*	F	US-2006/0282886 A1	Gaug, Mark	726/005
*	G	US-2009/0077622 A1	Baum et al.	726/1
	H	US-		
	I	US-		
	J	US-		
	K	US-		
	L	US-		
	M	US-		


**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)			
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.


<b>Search Notes</b>  	<b>Application/Control No.</b>  12189788	<b>Applicant(s)/Patent Under Reexamination</b>  BAUM ET AL.
	<b>Examiner</b>  ANTHONY MEJIA	<b>Art Unit</b>  2451

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
709	201, 202, 203, 224, 225, 227	4/29/2011	A.M.
717	101, 102	4/29/2011	A.M.
707	203	4/29/2011	A.M.
718	101	4/29/2011	A.M.
726	1	4/29/2011	A.M.
706	46	4/29/2011	A.M.

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
EAST Class Limited w/Text Search (See Search History)	4/29/2011	A.M.
EAST Text Search (See Search History)	4/29/2011	A.M.
EAST Assignee Search (See Search History)	08/23/2010	A.M.
EAST Inventor Search (See Search History)	08/23/2010	A.M.

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

/A. M./ Examiner.Art Unit 2451	
-----------------------------------	--

<b>Index of Claims</b>  	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010	04/26/2011	04/29/2011					
	1	✓	✓	✓					
	2	✓	✓	✓					
	3	✓	✓	✓					
	4	✓	✓	-					
	5	✓	✓	✓					
	6	✓	✓	✓					
	7	✓	✓	✓					
	8	✓	✓	✓					
	9	✓	✓	✓					
	10	✓	✓	✓					
	11	✓	✓	✓					
	12	✓	✓	✓					
	13	✓	✓	✓					
	14	✓	✓	✓					
	15	✓	✓	✓					
	16	✓	✓	✓					
	17	✓	✓	✓					
	18	✓	✓	✓					
	19	✓	✓	✓					
	20	✓	✓	✓					
	21	✓	✓	✓					
	22	✓	✓	✓					
	23	✓	✓	✓					
	24	✓	✓	✓					
	25	✓	✓	✓					
	26	✓	✓	✓					
	27	✓	✓	✓					
	28	✓	✓	✓					
	29	✓	✓	✓					
	30	✓	✓	✓					
	31	✓	✓	✓					
	32	✓	✓	✓					
	33	✓	✓	✓					
	34	✓	✓	✓					
	35	✓	✓	✓					
	36	✓	✓	✓					

<b>Index of Claims</b>  	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010	04/26/2011	04/29/2011					
	37	✓	✓	✓					
	38	✓	✓	✓					
	39	✓	✓	✓					
	40	✓	✓	✓					
	41	✓	✓	✓					
	42	✓	✓	✓					
	43	✓	✓	✓					
	44	✓	✓	✓					
	45	✓	✓	✓					
	46	✓	✓	✓					
	47	✓	✓	✓					
	48	✓	✓	✓					
	49	✓	✓	✓					
	50	✓	✓	✓					
	51	✓	✓	✓					

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	9	"20030062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:29
L2	15	"2003/0062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:30
L3	2	09/969521	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/29 15:41
S1	2	"20060271695"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:01
S2	18	12/189757	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:01
S3	45868	709/201.ccls. 709/202.ccls. 709/203.ccls. 709/224.ccls. 709/225.ccls. 709/227.ccls. 717/101.ccls. 717/102.ccls. 707/203.ccls. 718/101.ccls. 726/1.ccls. 706/46.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:05
S4	34837379	@ad<="20070612" @rlad<="20070612"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:05
S5	39563	S3 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:06

S6	3955	(automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:06
S7	201056	(generat\$3 creat\$3) near5 (network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S8	797	S6 AND S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S9	659	S8 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:10
S10	797	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)) AND ((generat\$3 creat\$3) near5 (network))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S11	659	S10 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S12	476	((automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors)) AND ((generat\$3 creat\$3) near5 (network)) AND (security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:11
S13	416	S12 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:12
S14	25	(automatically) near5 (locat\$3 discover\$3 find\$3) near5 (components devices sensors) near5 (security surveillance)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:19

S15	23	S14 AND S4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:20
S16	3	"7015806".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:24
S17	2	"6756998".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 15:32
S18	2	"20020103898"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/03/27 16:49
S19	2	"6686838".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/04/26 19:18

**EAST Search History (Interference)**

< This search history is empty >

**4/ 29/ 2011 4:04:11 PM**

**C:\ Documents and Settings\ amejia\ My Documents\ EAST\ Workspaces\ 12189757A.wsp**

**IN THE UNITED STATES PATENT OFFICE**

In Re Application of: )  
 )  
 Marc Baum, et al. ) Examiner: Anthony Mejia  
 ) Art Unit: 2451  
 )  
 Application No.: 12/189,788 )  
 )  
 Filed: August 12, 2008 )  
 )  
 For: FORMING A SECURITY NETWORK )  
 INCLUDING INTEGRATED SECURITY )  
 SYSTEM COMPONENTS AND NETWORK )  
 DEVICES )

---

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE

Sir:

Applicant respectfully requests consideration of the following amendments and remarks contained herein in response to the Office Action mailed September 1, 2010.



## AMENDMENTS

### IN THE CLAIMS

1. (Currently amended) A method comprising:
  - coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a plurality of security system components;
  - automatically discovering the plurality of security system components at the gateway and establishing communications between the gateway and the plurality of security system components;
  - automatically discovering a plurality of premise devices at the gateway and establishing communications between the gateway and the plurality of premise devices;
  - and
  - forming a security network by electronically integrating, ~~via~~ into the gateway, communications and functions of the plurality of premise devices and the plurality of security system components.
  
2. (Original) The method of claim 1, comprising controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device.
  
3. (Original) The method of claim 2, wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

Claim 4 (Canceled).

5. (Currently amended) The method of claim 41, comprising using protocols of the security system to discover the security system components, wherein the gateway includes the protocols of the security system.
6. (Currently amended) The method of claim 41, comprising the gateway receiving protocols of the security system from the security server in response to a request, wherein the gateway uses the protocols received to discover the security system components.
7. (Original) The method of claim 1, wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components.
8. (Original) The method of claim 7, wherein the connection management component automatically discovers the premise devices.
9. (Original) The method of claim 7, wherein the connection management component automatically installs the premise devices in the security network.
10. (Original) The method of claim 7, wherein the connection management component automatically configures the premise devices for operation in the security network.
11. (Original) The method of claim 1, wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices.
12. (Original) The method of claim 1, wherein the gateway includes a device connect component that includes definitions of the security system components and the premise devices.

13. (Original) The method of claim 1, wherein the premise local area network is coupled to a wide area network via a premise router.
14. (Original) The method of claim 1, wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network.
15. (Original) The method of claim 1, wherein the gateway is coupled to the premise devices using a wireless coupling.
16. (Original) The method of claim 1, wherein the gateway is coupled to the security server via the internet.
17. (Original) The method of claim 1, wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location.
18. (Original) The method of claim 1, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link.
19. (Original) The method of claim 18, comprising transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link.
20. (Original) The method of claim 19, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

21. (Original) The method of claim 18, comprising transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable.
22. (Original) The method of claim 18, wherein the secondary communication link includes a broadband coupling.
23. (Original) The method of claim 18, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling.
24. (Original) The method of claim 18, comprising transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link.
25. (Original) The method of claim 24, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.
26. (Original) The method of claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.
27. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.
28. (Original) The method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the premise devices.
29. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.

30. (Original) The method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the premise devices.
31. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the security system components.
32. (Original) The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the premise devices.
33. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the security system components.
34. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for the premise devices.
35. (Original) The method of claim 1, wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices.
36. (Original) The method of claim 1, wherein the security server manages communications with the security system components.
37. (Original) The method of claim 1, wherein the security server manages communications with the premise devices.
38. (Original) The method of claim 1, wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data.

39. (Original) The method of claim 38, wherein the notifications include one or more of short message service messages and electronic mail messages.
40. (Original) The method of claim 38, wherein the event data is event data of the security system components.
41. (Original) The method of claim 38, wherein the event data is event data of the premise devices.
42. (Original) The method of claim 1, wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link.
43. (Original) The method of claim 1, wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.
44. (Original) The method of claim 1, wherein the premise device is an Internet Protocol device.
45. (Original) The method of claim 1, wherein the premise device is a camera.
46. (Original) The method of claim 1, wherein the premise device is a touchscreen.
47. (Original) The method of claim 1, wherein the premise device is a device controller that controls an attached device.
48. (Original) The method of claim 1, wherein the premise device is a sensor.
49. (Currently amended) A method comprising:

forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location; and automatically discovering a plurality of premise devices at the gateway and establishing a coupling between the gateway and a the plurality of premise devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the gateway and the security network.

50. (Currently amended) A method comprising:

automatically discovering a security system at a gateway and establishing communications between a the gateway and a the security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system; and

automatically discovering a plurality of network devices at the gateway and establishing communications between the gateway and a the plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating into the gateway communications and functions of the plurality of network devices and the plurality of security system components.

51. (Currently amended) A method comprising:

forming a security network by automatically discovering a security system at a gateway and establishing communications between a the gateway and a the security system, the security system including security system components installed at a facility;

automatically discovering a plurality of network devices at the gateway and establishing communications between the security network and a the plurality of network devices located at the facility, the gateway electronically integrating communications and

functions of the plurality of network devices and the security system components into the gateway and the security network; and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the network devices.



## REMARKS

Claims 1-51 were pending in the application. Claims 1-51 were rejected. Claims 1, 5, 6, and 49-51 are amended herein. Claim 4 is canceled herein without prejudice. No new matter is added by the amendments herein.

### Petition For Extension Of Time

A Petition For Extension Of Time Under 37 CFR 1.136(a) is submitted herewith along with the appropriate fee amount for a three (3) month extension of time.

### Double Patenting Rejections

Claims 1 and 49-51 were provisionally rejected under the judicially created ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 and 60-61 of co-pending Application No. 12/189,785, claims 1 and 52-54 of co-pending Application No. 12/189,780, claims 1 and 60-61 of co-pending Application No. 12/189,757, claims 1 and 96-98 of co-pending Application No. 12/198,039 and claims 1 and 71-73 of co-pending Application No. 12/198,023.

Applicant submits herewith timely filed Terminal Disclaimers to obviate each of the double patenting rejections. Applicant submits that the Terminal Disclaimers overcome the double patenting rejections and requests withdrawal thereof. Applicant maintains however that the claims of the present application and the claims of co-pending Application Nos. 12/189,785, 12/189,780, No. 12/189,757, 12/198,039 and 12/198,023 are not identical and are patentably distinct from one another since they include non-obvious differences.

### Rejections under 35 U.S.C. §102

Claims 1-3, 7, 8, 11, 12, 15-25, 28, 30-45, and 48-51 were rejected under 35 U.S.C. §102(b) as being anticipated by Naidoo et al., United States (US) Patent Application Publication No. US 2003/0062997 A1 ("Naidoo"). Applicant respectfully submits that the claims as amended herein are patentably distinct from Naidoo. Moreover, Naidoo fails to teach each and every element of claims 1-3, 7, 8, 11, 12, 15-25, 28, 30-45, and 48-51 as presented herein.

To be proper, an anticipation rejection requires that a cited reference teach each and every element of the rejected claim(s). As discussed below, it is clearly apparent that Naidoo does not teach each and every element of claims 1-3, 7, 8, 11, 12, 15-25, 28, 30-45, and 48-51 as presented herein.

Regarding claim 1 as amended herein, Applicant respectfully submits that Naidoo describes a system and method for distributed monitoring and remote verification of conditions surrounding an alarm condition in a security system (abstract). Naidoo describes that the security system includes a security gateway, which is typically located at the desired premises to be monitored, and a monitoring client, typically located at a central station and operatively coupled to security gateway through a network. Naidoo describes that often, the security gateway is located at the target site, however, on some occasions, some or all components of security gateway may be located remotely, but remain operatively coupled to security sensors and video cameras which are at the premises (paragraph 0028).

Naidoo describes that the security gateway is a processor-based device that functions to detect alarm conditions at a target site and to capture information relating to such alarm conditions (paragraph 0032). Naidoo describes that, upon detection of an alarm condition, the security gateway captures video (usually through an attached video camera) of the target site, and sends the video to security system server in real time (paragraph 0028).

Naidoo describes that a monitoring client is generally a software program that may be used to display some or all of the information provided by security gateway. Monitoring client may be a stand-alone program or integrated into one or more existing software programs. Naidoo describes that one or more operators may then use this information to evaluate whether the alarm condition corresponds to an actual alarm condition and then take additional action, if desired, such as alerting the appropriate authorities (paragraph 0032).

Naidoo describes that the security system includes one or more sensors coupled to security gateway for the purpose of detecting alarm conditions. The security system is not limited to any specific type or model of sensor. Any sensor may be used, depending on the desired type and level of protection. Alarm sensors may be wired directly into an

alarm control panel built into the security gateway or they may be wirelessly connected (paragraph 0033). Naidoo describes that the security system also includes one or more video cameras that are operable to capture video data of monitored premises. Naidoo describes that the security gateway may be configured to create an association between one or more sensors and an associated video camera (paragraph 0034).

Regarding claim 1, as amended, Applicant respectfully submits that Naidoo does not disclose automatically discovering a plurality of security system components at the gateway and establishing communications between the gateway and the plurality of security system components, and automatically discovering a plurality of premise devices at the gateway and establishing communications between the gateway and the plurality of premise devices, and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components (emphasis added).

Naidoo instead describes a security gateway that detects alarm conditions at a target site and forwards the detected conditions and related information to a security system server. In describing the security gateway's functionality, Naidoo teaches the gateway's use of wireless capabilities. As one example, Naidoo discloses the security gateway's potential use of a fixed wireless network to issue a redundant alarm notification (paragraph 0043). As another example, a control panel component of the security gateway may communicate with wireless sensors (paragraphs 0030 and 0080). As yet another example, the security gateway may be activated or deactivated using wireless remote communications (paragraph 0089). As indicated by these references, Naidoo simply teaches the gateway's use of wireless technologies in collecting and transmitting alarm condition data or simply sending and receiving wireless communications. These disclosures of wireless capabilities nowhere teach automatically discovering a plurality of security system components at the gateway and establishing communications between the gateway and the plurality of security system components, and automatically discovering a plurality of premise devices at the gateway and establishing communications between the gateway and the plurality of premise devices, and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components (emphasis added).

As already set forth above, Naidoo describes a security gateway that detects alarm conditions at a target site and forwards the detected conditions and related information to a security system server. The security gateway may include one or more sensors and may also include one or more video cameras. Under the system of Naidoo, the security gateway may be configured to create an association between one or more sensors and an associated video camera. This reference to a potential configuration does not define a process (automatic or otherwise) or any set-up procedure (automatic or otherwise) that automatically discovers a plurality of security system components at the gateway and establishes communications between the gateway and the plurality of security system components, and automatically discovers a plurality of premise devices at the gateway and establishes communications between the gateway and the plurality of premise devices, and forms a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components (emphasis added).

For at least these reasons, Applicant respectfully submits that amended claim 1 is not anticipated by Naidoo.

As claims 2, 3, 7, 8, 11, 12, 15-25, 28, 30-45, and 48 depend from amended claim 1 and include further limitations thereon, and since amended claim 1 is not anticipated by Naidoo, Applicant submits that claims 2, 3, 7, 8, 11, 12, 15-25, 28, 30-45, and 48 are not anticipated by Naidoo.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 49 and, as such, amended claim 49 is not anticipated by Naidoo. For at least these reasons, Applicant submits that amended claim 49 is not anticipated by Naidoo and respectfully requests that the rejection be withdrawn and allowance therefore.

Applicant respectfully submits that, for the reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 50 and, as such, amended claim 50 is not anticipated by Naidoo. For at least these reasons, Applicant submits that amended claim 50 is not anticipated by Naidoo and respectfully requests that the rejection be withdrawn and allowance therefore.

Applicant respectfully submits that, for the reasons stated above with reference to

amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 51 and, as such, amended claim 51 is not anticipated by Naidoo. For at least these reasons, Applicant submits that amended claim 51 is not anticipated by Naidoo and respectfully requests that the rejection be withdrawn and allowance therefore.

Rejections under 35 U.S.C. §103

Claims 4-6 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Rezvani et al., US Patent number 6,686,838 ("Rezvani"). Claim 4 is canceled herein without prejudice.

At page 17 of the Office Action, the Examiner states that Naidoo does not explicitly disclose "the method of claim 1, wherein the gateway automatically discovers the security system components". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo. Furthermore, regarding claims 5-6 which depend from amended claim 1, Applicant does not find any teaching in Rezvani that overcomes the deficiencies in Naidoo described above. For at least these reasons, Applicant submits that claims 5-6 are patentable over Naidoo in view of Rezvani and respectfully requests that the rejection be withdrawn and allowance thereof.

Further regarding Examiner's rejection of claims 4-6 based in part on Rezvani, Applicant respectfully submits that Rezvani describes systems and methods for providing registration at a remote site that may include, for example, a monitoring module that may communicate with a remote site (abstract). Devices at one or more locations may interface with the monitoring modules. Rezvani describes that one or more monitoring modules and their associated interfaced devices may be referred to as "installations." Devices may include, for example, video cameras, still cameras, motion sensors, audible detectors, any suitable household appliances, or any other suitable device. Rezvani describes that monitoring modules may be stand-alone devices, software applications, any suitable combination of software and hardware, or any other suitable architecture (column 1, lines 41-50).

Rezvani describes that monitoring modules may communicate with one or more

remote sites via a suitable communications network using any suitable communications protocol. The monitoring modules and remote sites may use a registration protocol to transmit registration information. The registration information may get stored in a database at the remote site (column 1, lines 51-56).

Rezvani describes that an installation, any of its components, or both may be associated with a particular user account (column 1, lines 59-60). Association of an installation, installation elements, or both with corresponding user accounts may take place at the remote site. The remote site may make the association using any suitable database construct that may serve to cross reference the installation, installation elements, or both with user accounts (column 1, lines 65-67 to column 2, lines 1-3).

Rezvani describes that devices may be automatically detected by a monitoring module (column 2, lines 37-38). Rezvani describes that as new devices are added to a registered monitoring module, the monitoring module may automatically (i.e., without any user interaction) detect the presence of the new devices and automatically notify remote site of the presence of the new devices. Remote site may, in turn, add the new devices to the database (column 21, lines 5-11).

Regarding claim 1, as amended, Rezvani does not disclose forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components (emphasis added).

Although Rezvani discloses the automatic detection of devices, the detected device information is directed to and registered at a remote site. Rezvani teaches automatically detecting a device at an installation, extracting registration information from the device, communicating the registration information to a remote site that does not have requisite registration information associated with the device using a communications network, registering the device with the remote site based on the registration information, and associating the device at the remote site with a user account based on the registration information (claim 1, column 21, lines 41-53). Rezvani therefore teaches the automatic detection and extraction of registration information from devices at a first location (an installation). Rezvani further teaches communication of the registration information to a remote location and registration of devices at the remote

location using the extracted information. Rezvani does not teach automatically discovering a plurality of security system components at the gateway and establishing communications between the gateway and the plurality of security system components, and automatically discovering a plurality of premise devices at the gateway and establishing communications between the gateway and the plurality of premise devices, and forming a security network by electronically integrating into the gateway communications and functions of the plurality of premise devices and the plurality of security system components (emphasis added).

For at least these reasons, Applicant respectfully submits that amended claim 1 is patentable over Naidoo in view of Rezvani. As claims 5-6 depend from amended claim 1 and include further limitations thereon, and since amended claim 1 is patentable over Naidoo in view of Rezvani, Applicant submits that claims 5-6 are patentable over Naidoo in view of Rezvani.

Claim 9 was rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Bilger, US Patent number 6,756,998 (“Bilger”).

At page 18 of the Office Action, the Examiner states that Naidoo does not explicitly disclose "the method of claim 7, wherein the connection management component automatically installs the premise devices in the security network". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo. Furthermore, regarding claim 9 which depends from amended claim 1, Applicant does not find any teaching in Bilger that overcomes the deficiencies in Naidoo described above. For at least these reasons, Applicant submits that claim 9 is patentable over Naidoo in view of Bilger and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 10 and 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Tanaka et al., US Patent Application Publication number US 2004/0037295 A1 (“Tanaka”).

At page 19 of the Office Action, the Examiner states that Naidoo does not explicitly disclose "the method of claim 7, wherein the connection management

component automatically configures the premise devices for operation in the security network". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo. Furthermore, regarding claims 10 and 29 which depend from amended claim 1, Applicant does not find any teaching in Tanaka that overcomes the deficiencies in Naidoo described above. For at least these reasons, Applicant submits that claims 10 and 29 are patentable over Naidoo in view of Tanaka and respectfully requests that the rejection be withdrawn and allowance thereof.

Claim 26 was rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Patterson, US Patent Application Publication number US 2005/0086126 A1 ("Patterson").

At page 21 of the Office Action, the Examiner states that Naidoo does not explicitly disclose "the method of claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo. Furthermore, regarding claim 26 which depends from amended claim 1, Applicant does not find any teaching in Patterson that overcomes the deficiencies in Naidoo described above. For at least these reasons, Applicant submits that claim 26 is patentable over Naidoo in view of Patterson and respectfully requests that the rejection be withdrawn and allowance thereof.

Claim 27 was rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Moyer et al., US Patent Application Publication number US 2002/0103898 A1 ("Moyer").

At page 22 of the Office Action, the Examiner states that Naidoo does not explicitly disclose "the method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to



amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo. Furthermore, regarding claim 27 which depends from amended claim 1, Applicant does not find any teaching in Moyer that overcomes the deficiencies in Naidoo described above. For at least these reasons, Applicant submits that claim 27 is patentable over Naidoo in view of Moyer and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 46-47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Lingemann, US Patent Application Publication number US 2006/0009863 A1 (“Lingemann”).

At page 22 of the Office Action, the Examiner states that Naidoo does not explicitly disclose "the method of claim 1, wherein the network device is a touchscreen". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo. Furthermore, regarding claims 46-47 which depend from amended claim 1, Applicant does not find any teaching in Lingemann that overcomes the deficiencies in Naidoo described above. For at least these reasons, Applicant submits that claims 46-47 are patentable over Naidoo in view of Lingemann and respectfully requests that the rejection be withdrawn and allowance thereof.

Claims 13-14 were rejected under 35 U.S.C. §103(a) as being unpatentable over Naidoo in view of Moore et al., US Patent Application Publication number US 2007/0061266 A1 (“Moore”).

At page 24 of the Office Action, the Examiner states that Naidoo does not explicitly disclose "the premise local area network is coupled to a wide area network via a premise router". Applicant agrees.

Applicant respectfully submits that, for reasons stated above with reference to amended claim 1, Naidoo does not teach or suggest each and every limitation of amended claim 1 and, as such, amended claim 1 is patentable over Naidoo. Furthermore, regarding claims 13-14 which depend from amended claim 1, Applicant does not find any teaching in Moore that overcomes the deficiencies in Naidoo described above. For at least these

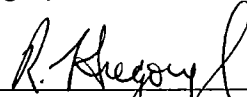
reasons, Applicant submits that claims 13-14 are patentable over Naidoo in view of Moore and respectfully requests that the rejection be withdrawn and allowance thereof.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully submit that the double patenting rejections and the rejections under 35 U.S.C. §102 and §103 have been overcome, and their withdrawal is respectfully requested. Applicants submit that claims 1-3 and 4-51 are in condition for allowance. The allowance of the claims is earnestly requested. If in the opinion of Examiner Mejia a telephone conference would expedite the prosecution of the subject application, or if there are any issues that remain to be resolved prior to allowance of the claims, Examiner Mejia is encouraged to call Rick Gregory at 408.821.8080.

Date: March 1, 2011

Respectfully submitted,  
Gregory & Martensen LLP



Richard L. Gregory, Jr., Reg. No. 42,607  
Telephone: 408.821.8080

Gregory & Martensen LLP  
2018 Bissonnet Street  
Houston, Texas 77005  
Fax: 281.501.1731

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBIVATE A PROVISIONAL DOUBLE PATENTING  
REJECTION OVER A PENDING "REFERENCE" APPLICATION**

Docket Number (Optional)  
ICON.P001D3

In re Application of: iControl Networks, Inc.

Application No.: 12/189,788

Filed: August 12, 2008

For: Forming a Security Network Including Integrated Security System Components and Network Devices

The owner\*, iControl Networks, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number 12/189,785, filed on August 11, 2008, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that: any such patent: granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney or agent of record. Reg. No. 42,607

/Richard L. Gregory Jr./  
Signature

March 1, 2011  
Date

Richard L. Gregory, Jr.  
Typed or printed name

(408) 676-8080  
Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).

Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBIVATE A PROVISIONAL DOUBLE PATENTING  
REJECTION OVER A PENDING "REFERENCE" APPLICATION**

Docket Number (Optional)

ICON.P001D3

In re Application of: iControl Networks, Inc.

Application No.: 12/189,788

Filed: August 12, 2008

For: Forming a Security Network Including Integrated Security System Components and Network Devices

The owner\*, iControl Networks, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 12/189,780, filed on August 11, 2008, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney or agent of record. Reg. No. 42,607

/Richard L. Gregory Jr./

Signature

March 1, 2011

Date

Richard L. Gregory, Jr.

Typed or printed name

(408) 676-8080

Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).

Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING  
REJECTION OVER A PENDING "REFERENCE" APPLICATION**Docket Number (Optional)  
ICON.P001D3

In re Application of: iControl Networks, Inc.

Application No.: 12/189,788

Filed: August 12, 2008

For: Forming a Security Network Including Integrated Security System Components and Network Devices

The owner\*, iControl Networks, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number 12/198,023, filed on August 25, 2008, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that: any such patent: granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney or agent of record. Reg. No. 42,607

/Richard L. Gregory Jr./

Signature

March 1, 2011

Date

Richard L. Gregory, Jr.

Typed or printed name

(408) 676-8080

Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).

Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> <b>FY 2009</b> <i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i>		Docket Number (Optional) <b>ICON.P001D3</b>	
Application Number <b>12/189,788</b>		Filed <b>August 12, 2008</b>	
For <b>Forming a Security Network Including Integrated Security System Components and Network Devices</b>			
Art Unit <b>2451</b>		Examiner <b>Anthony MEJIA</b>	
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.			
The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):			
	<u>Fee</u>	<u>Small Entity Fee</u>	
<input type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$130	\$65	\$ _____
<input type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$490	\$245	\$ _____
<input checked="" type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$1110	\$555	\$ <u>555</u>
<input type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$1730	\$865	\$ _____
<input type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$2350	\$1175	\$ _____
<input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.			
<input type="checkbox"/> A check in the amount of the fee is enclosed.			
<input checked="" type="checkbox"/> Payment by credit card.			
<input type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.			
<input type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number _____.			
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>			
I am the <input type="checkbox"/> applicant/inventor.			
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).			
<input checked="" type="checkbox"/> attorney or agent of record. Registration Number <u>42,607</u>			
<input type="checkbox"/> attorney or agent under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____			
<u>/Richard L. Gregory, Jr./</u>		<u>March 1, 2011</u>	
Signature		Date	
<u>Richard L. Gregory, Jr.</u>		<u>408-676-8080</u>	
Typed or printed name		Telephone Number	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.			
<input checked="" type="checkbox"/> Total of <u>1</u> forms are submitted.			

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12189788
<b>Filing Date:</b>	12-Aug-2008
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Filer:</b>	Richard L. Gregory/Rob Rathbun
<b>Attorney Docket Number:</b>	ICON.P001D3

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				
Extension - 3 months with \$0 paid	2253	1	555	555

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Statutory or terminal disclaimer	2814	5	70	350
<b>Total in USD (\$)</b>				<b>905</b>



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	9563380
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	98195
<b>Filer:</b>	Richard L. Gregory/Rob Rathbun
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	01-MAR-2011
<b>Filing Date:</b>	12-AUG-2008
<b>Time Stamp:</b>	17:24:31
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$905
RAM confirmation Number	4321
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / zip	Pages (if appl.)
SecureNet Technologies, LLC Exhibit 1003 Page 785					

1		ICONP001D3_Amendment_Response.pdf	2669383 <small>3047bc2c02151d67b8e388341cf6f1849ce171db</small>	yes	26
<b>Multipart Description/PDF files in .zip description</b>					
<b>Document Description</b>		<b>Start</b>		<b>End</b>	
Transmittal Letter		1		1	
Amendment/Req. Reconsideration-After Non-Final Reject		2		20	
Terminal Disclaimer Filed		21		21	
Terminal Disclaimer Filed		22		22	
Terminal Disclaimer Filed		23		23	
Terminal Disclaimer Filed		24		24	
Terminal Disclaimer Filed		25		25	
Extension of Time		26		26	
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (PTO-875)	fee-info.pdf	32200 <small>3dd62a32e498b8530c4414b3574473facdd6042</small>	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			2701583		

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

**Transmittal of Documents**

*Certification Under 37 C.F.R. §1.8(a)*

Transmitted via

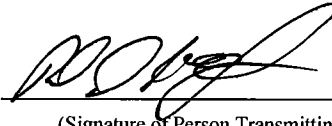
**March 1, 2011**

Date of Transmission

**USPTO EFS**

I hereby certify that this document, and any other accompanying documents referred to herein are being transmitted to the United States Patent Office via EFS in accordance with 37 C.F.R. §1.6(a)(4) on the date indicated above.

***Rob Rathbun***



\_\_\_\_\_  
(Print Name of Person Transmitting Documents)

\_\_\_\_\_  
(Signature of Person Transmitting Documents)

Amendment and Response Under CFR §1.111;  
Five (5) Terminal Disclaimers to Obviate a Provisional Double Patenting  
Rejection Over a Pending "Reference" Application;  
Petition for Three (3) Months Extension of Time;  
Electronic payment of filing fees.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBIVATE A PROVISIONAL DOUBLE PATENTING  
REJECTION OVER A PENDING "REFERENCE" APPLICATION**Docket Number (Optional)  
ICON.P001D3

In re Application of: iControl Networks, Inc.

Application No.: 12/189,788

Filed: August 12, 2008

For: Forming a Security Network Including Integrated Security System Components and Network Devices

The owner\*, iControl Networks, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number 12/198,039, filed on August 25, 2008, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that: any such patent: granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney or agent of record. Reg. No. 42,607

/Richard L. Gregory Jr./  
Signature

March 1, 2011  
Date

Richard L. Gregory, Jr.  
Typed or printed name

(408) 676-8080  
Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).  
Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION**Docket Number (Optional)  
ICON.P001D3

In re Application of: iControl Networks, Inc.

Application No.: 12/189,788

Filed: August 12, 2008

For: Forming a Security Network Including Integrated Security System Components and Network Devices

The owner\*, iControl Networks, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number 12/189,757, filed on August 11, 2008, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that: any such patent: granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney or agent of record. Reg. No. 42,607

/Richard L. Gregory Jr./

Signature

March 1, 2011

Date

Richard L. Gregory, Jr.

Typed or printed name

(408) 676-8080

Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).

Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/189,788</b>	Filing Date <b>08/12/2008</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		OR	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		OR	N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		OR	N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		OR	X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				OR		
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>					OR		
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL		OR	TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	<b>03/01/2011</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 50	Minus	** 51	=	0	OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus	***4	=	0	OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR		
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE	<b>0</b>	OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR		
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /CORALIA BETANCOURT/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



**UNITED STATES PATENT AND TRADEMARK OFFICE**

UNITED STATES DEPARTMENT OF COMMERCE  
**United States Patent and Trademark Office**  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
12/189,788		2451	2455



**Correspondence Address/Fee Address Change**

The following fields have been set to Customer Number 98195 on 08/09/2010

- Correspondence Address
- Maintenance Fee Address
- Power of Attorney Address

The address of record for Customer Number 98195 is:

**98195**  
**Gregory & Martensen LLP**  
**2018 Bissonnet Street**  
**Houston, TX 77005**





UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
12/189,788 08/12/2008 Marc Baum ICON.P001D3 7650

98195 7590 09/01/2010
Gregory & Martensen LLP
2018 Bissonnet Street
Houston, TX 77005

EXAMINER

MEJIA, ANTHONY

ART UNIT PAPER NUMBER

2451

MAIL DATE DELIVERY MODE

09/01/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

**Office Action Summary**

<b>Application No.</b> 12/189,788	<b>Applicant(s)</b> BAUM ET AL.	
<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 12 August 2008.
- 2a)  This action is **FINAL**.
- 2b)  This action is non-final.
- 3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4)  Claim(s) 1-51 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5)  Claim(s) \_\_\_\_\_ is/are allowed.
- 6)  Claim(s) 1-51 is/are rejected.
- 7)  Claim(s) \_\_\_\_\_ is/are objected to.
- 8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9)  The specification is objected to by the Examiner.
- 10)  The drawing(s) filed on 24 November 2008 is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 10/15/2009.
- 4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_

### **DETAILED ACTION**

1. Acknowledgement is made that Claims 1-51 are pending in the instant application and are now being presented.

#### ***Priority***

2. Applicant's claim for the benefit of a prior-filed Application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has complied with the conditions for receiving the benefit of an earlier filing date.

#### ***Double Patenting***

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644

Art Unit: 2451

(CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1 and 49-51 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 and 60-61 of co-pending Application No. 12/189,785.

Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

Claims 1 and 49-51 of the instant application are contain every element of Claim(s) 1 and 60-61 of co-pending Applications Nos. 12/189,785 and thus anticipate the claims of the instant application. Therefore, the Claims of the instant application are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later application claim is not patently distinct from an earlier claim if the later claim is anticipated by the earlier claim.

5. Claims 1 and 49-51 are provisionally rejected on the ground of nonstatutory

Art Unit: 2451

obviousness-type double patenting as being unpatentable over claims 1 and 52-54 of co-pending Application No. 12/189,780.

Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

Claims 1 and 49-51 of the instant application are contain every element of Claim(s) 1 and 52-54 of co-pending Applications Nos. 12/189,780 and thus anticipate the claims of the instant application. Therefore, the Claims of the instant application are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later application claim is not patently distinct from an earlier claim if the later claim is anticipated by the earlier claim.

6. Claims 1 and 49-51 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 and 60-61 of co-pending Application No. 12/189,757.

Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

Claims 1 and 49-51 of the instant application are contain every element of Claim(s) 1 and 60-61 of co-pending Applications Nos. 12/189,757 and thus anticipate the claims of the instant application. Therefore, the Claims of the instant application are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later application claim is not patently distinct from an earlier claim if the later claim is anticipated by the earlier claim.

Art Unit: 2451

7. Claims 1 and 49-51 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 and 96-98 of co-pending Application No. 12/198,039.

Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

Claims 1 and 49-51 of the instant application are contain every element of Claim(s) 1 and 96-98 of co-pending Applications Nos. 12/198,039 and thus anticipate the claims of the instant application. Therefore, the Claims of the instant application are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later application claim is not patently distinct from an earlier claim if the later claim is anticipated by the earlier claim.

8. Claims 1 and 49-51 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 and 71-73 of co-pending Application No. 12/198,023.

Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

Claims 1 and 49-51 of the instant application are contain every element of Claim(s) 1 and 71-73 of co-pending Applications Nos. 12/198,023 and thus anticipate the claims of the instant application. Therefore, the Claims of the instant application are not patently distinct from the earlier patent claims and as such are unpatentable over obvious-type double patenting. A later application claim is not patently distinct from an

Art Unit: 2451

earlier claim if the later claim is anticipated by the earlier claim.

“A later patent claim is not patentably distinct from an earlier patent claim if the later claim obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus)”. ELI LILLY AND COMPANY vs. BARR LABORATORIES INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented. Please note, the above is not a complete list of claims rejected for nonstatutory obviousness-type double patenting. For the sake of brevity, only the independent claims were listed.

### ***Specification***

9. The use of the following trademarks: GE Security™, Honeywell™, DSC/Tyco™, Alarm.com™, NextAlarm™, and uControl™ have been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

***Claim Rejections - 35 USC § 102***

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1-3, 7-8, 11-12, 15-25, 28, 30-45, 48-51 are rejected under 35 U.S.C. 102(b) as being anticipated by Naidoo et al. (US 2003/0062997) (hereinafter as Naidoo).

Regarding Claim 1, Naidoo teaches a method comprising:

coupling a gateway to a local area network located in a first location and a security server in a second location (see figs.1-2), wherein the first location includes a security system comprising:

a plurality of security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the gateway and the security system components (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the gateway and premise devices pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

forming a security network by electronically integrating, via the gateway, communications and functions of the plurality of premise devices and the security



Art Unit: 2451

system components, (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

Regarding Claim 2, Naidoo further teaches the step of controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device (pars [0040-0041]).

Regarding Claim 3, Naidoo further teaches the step wherein the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices (par [0040] and see fig.2).

Regarding Claim 7, Naidoo further teaches the step wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components (pars [0069], [0079], and [0087]).

Regarding Claim 8, Naidoo further teaches the step wherein the connection management component automatically discovers the premise devices (par [0040] and see fig.2).

Art Unit: 2451

Regarding Claim 11, Naidoo further teaches the step wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices (par [0099]).

Regarding Claim 12, Naidoo further teaches the step wherein the gateway includes a device connect component that includes definitions of the security system components and the premise devices (pars [0080-0081]).

Regarding Claim 15, Naidoo further teaches the step wherein the gateway is coupled to the premise devices using a wireless coupling (par [0033]).

Regarding Claim 16, Naidoo further teaches the step wherein the gateway is coupled to the security server via the internet (par [0030]).

Regarding Claim 17, Naidoo further teaches the step wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location (par [0043] and see fig.2).

Regarding Claim 18, Naidoo further teaches wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the

Art Unit: 2451

gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link (par [0043] and see fig.2).

Regarding Claim 19, Naidoo further teaches the step of transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link (par [0043] and see fig.2).

Regarding Claim 20, Naidoo further teaches the step wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of:

security system components and premise devices, and data received by at least one of security system components and premise devices (pars [0069], and [0080-0081]).

Regarding Claim 21, Naidoo further teaches the step of transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable (par [0043]).

Regarding Claim 22, Naidoo further teaches wherein the secondary communication link includes a broadband coupling (pars [0027] and [0122]).

Art Unit: 2451

Regarding Claim 23, Naidoo further teaches the step wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling (par [0043]).

Regarding Claim 24, Naidoo further teaches the step of transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link (pars [0027-0028], [0043], and [0046]).

Regarding Claim 25, Naidoo further teaches wherein the event data comprises changes in device states of at least one of:

security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices (pars [0069], and [0080-0081]).

Regarding Claim 28, Naidoo further teaches wherein the security server creates modifies and terminates couplings between the gateway and the premise devices (pars [0099-0101]).

Art Unit: 2451

Regarding Claim 30, Naidoo further teaches wherein wherein the security server performs creation, modification, deletion and configuration of the premise devices (pars [0099-0101]).

Regarding Claim 31, Naidoo further teaches wherein the security server creates automations, schedules and notification rules associated with the security system components (par [0045]).

Regarding Claim 32, Naidoo further teaches wherein the security server creates automations, schedules and notification rules associated with the premise devices (pars [0027-0028] and [0045]).

Regarding Claim 33, Naidoo further teaches the step wherein the security server manages access to current and logged state data for the security system components (pars [0049-0050]).

Regarding Claim 34, Naidoo further teaches the step wherein the security server manages access to current and logged state data for the premise devices (pars [0027-0028] and [0049-0050]).

Art Unit: 2451

Regarding Claim 35, Naidoo further teaches the step wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices (pars [0027-0028] and [0049-0050]).

Regarding 36, Naidoo further teaches the step wherein the security server manages communications with the security system components (par [0049]).

Regarding 37, Naidoo further teaches the step wherein the security server manages communications with the premise devices (pars [0027-0028] and [0049]).

Regarding 38, Naidoo further teaches the step wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data (par [0053]).

Regarding 39, Naidoo further teaches the step wherein the notifications include one or more of short message service messages and electronic mail messages (par [0069]).

Regarding Claim 40, Naidoo further teaches the step wherein the event data is event data of the security system components (par [0053]).

Art Unit: 2451

Regarding Claim 41, Naidoo further teaches the step wherein the event data is event data of the premise devices (pars [0027-0028] and [0053]).

Regarding Claim 42, Naidoo further teaches the step wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link (pars [0027-0028], [0043], and [0046]).

Regarding Claim 43, Naidoo further teaches the step wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers (par [0059]).

Regarding Claim 44, the method of claim 1, wherein the premise device is an Internet Protocol device (par [0037]).

Regarding Claim 45, Naidoo further teaches the step wherein the premise device is a camera (pars [0040-0041]).

Regarding Claim 48, Naidoo further teaches the step wherein the premise device is a sensor (pars [0040-0041]).

Regarding Claim 49, Naidoo teaches a method comprising:

Art Unit: 2451

forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

establishing a coupling between the gateway and a plurality of premise devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the security network (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

Regarding Claim 50, Naidoo teaches a method comprising:

automatically establishing communications between a gateway and a security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

automatically establishing communications between the gateway and a plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating communications and functions of the plurality of network devices and the security



Art Unit: 2451

system components (pars [0027-0030], [0047-0048], and [0078-0079], and see fig.1 and 6).

Regarding Claim 51, Naidoo teaches a method comprising:

forming a security network by automatically establishing communications between a gateway and a security system, the security system including security system components installed at a facility (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6);

automatically establishing communications between the security network and a plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the security network (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6); and

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the network devices (pars [0027-0030], [0047-0048], and [0078-0079], and see figs.1-2 and 6).

### ***Claim Rejections - 35 USC § 103***

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2451

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in view of Rezvani et al. (US 6,686,838).

Regarding Claim 4, Naidoo discloses the invention substantially, however Naidoo does not explicitly disclose the method of claim 1, wherein the gateway automatically discovers the security system components.

Rezvani in the field of the same endeavor teaches a registration protocol may be used by the monitoring module and the remote site in generating the message communicated during the registration process. The monitoring module may gather and generate various identification information to be included in the registration protocol message used to automatically register devices. In particular, Rezvani teaches new devices may be added to a registered installation and automatically detected and registered by a new object discovery process (see Rezvani; col. 2/line 66-col. 3/line 9).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Rezvani in order to enable Naidoo's gateway to incorporate the functionality of automatic discovery by the process of Rezvani new object discovery process to automatically discover security system components. One of ordinary skill in the art would have been motivated because Rezvani provides an improved technique for registering devices as suggested by Rezvani (see Rezvani; col. 1, lines 32-34).

Art Unit: 2451

Regarding Claim 5, Naidoo-Rezvani discloses the method of claim 4, comprising using protocols of the security system to discover the security system components, wherein the gateway includes the protocols (see Rezvani; col. 2/lines 27-36; the remote sites may validate received registration protocol messages used during the new object discovery process to discovery new devices).

Regarding Claim 6, Naidoo-Rezvani discloses the method of claim 4, comprising requesting and receiving protocols of the security system from the security server, wherein the gateway receives and uses the protocols to discover the security system components (see Rezvani; col. 2, lines 27-36; the remote sites may validate received registration protocol messages used during the new object discovery process to discovery new devices).

14. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in view of Bilger (US 6,756,998).

Regarding Claim 9, Naidoo discloses the invention substantially, however Naidoo does not explicitly discloses the method of claim 7, wherein the connection management component automatically installs the premise devices in the security network.

Bilger in the field of the same endeavor teaches home automation system interface for interfacing with a system that automatically controls controlled devices

Art Unit: 2451

throughout the home. In particular, Bilger teaches Cross will automatically install sensor in the selected room (col. 20, lines 1-13).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Bilger in order Naidoo's components to automatically install devices to the security system. One of ordinary skill in the art would have been motivated because it would ease installation of components by automatically installing the device to the security system.

15. Claims 10 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in view of Tanaka et al. (US 2004/0037295).

Regarding Claim 10, Naidoo discloses the invention substantially, however Naidoo does not explicitly disclose the method of Claim 7, wherein the connection management component automatically configures the premise devices for operation in the security network.

Tanaka in the field of the same endeavor teaches creating a virtual local area network using a graphical user interface. In particular, Tanaka teaches the server automatically creates configuration information of the switch (see Tanaka: par [0083]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Tanaka in order for Naidoo server to perform configurations on the device. Tanaka teachings enabled Naidoo to create, modify, and delete configuration settings of the switch. One of

Art Unit: 2451

ordinary skill in the art would have been motivated because allowing for configurations to be created, modified and deleted increase the flexibility of a device by allowing configurations to be created, modified and deleted.

Regarding Claim 29, Naidoo discloses the invention substantially, however Naidoo discloses the method of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components.

Tanaka in the field of the same endeavor teaches creating a virtual local area network using a graphical user interface. In particular, Tanaka teaches the server automatically creates configuration information of the switch and deletes the VLAN link. The server automatically issues command to delete the connection to the switch (see Tanaka; [0083]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Tanaka in order for Naidoo server to perform actions on the device configurations. Tanaka teachings enabled Naidoo to create, modify, and delete configuration settings of the switch. One of ordinary skill in the art would have been motivated because allowing for configurations to be created, modified and deleted increase the flexibility of a device by allowing configurations to be created, modified and deleted.

16. Claims 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo et al. (US 2003/0062997) in view of Patterson (US 2005/0086126).

Regarding Claim 26, Naidoo discloses the invention substantially, however Naidoo does not explicitly disclose the method of Claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system.

Patterson, in the field of the same endeavor teaches managing and linking network accounts to share access privileges among accounts. In particular, Patterson teaches that the server may create account, upgrade an account, or terminate the upgrading of an account (see Patterson; [0046]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Patterson in order for the server of Naidoo to create, upgrade, and terminate accounts. One of ordinary skill would be motivated because Patterson suggest it would be desirable for an environment having different levels of access, a provider may charge higher fees for accounts with higher levels of access. Accordingly, from the provider's standpoint, it is desirable to encourage users to purchase more expensive subscriptions, and so the provider often attempts to make the accounts with higher levels of access more appealing to users (see Patterson; [0002]).

17. Claims 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in view of Moyer et al. (US 2002/0103898).

Regarding Claim 27, Naidoo discloses the invention substantially, however

Art Unit: 2451

Naidoo does not explicitly disclose the method of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components.

Moyer in the field of the same endeavor teaches Session Initiated Protocol (SIP) to communicate with network capable appliances by leveraging SIP capabilities to directly communicating with the appliances. In particular, Moyer teaches that SIP is an application layer control and signaling protocol used for creating, modifying and terminating communication sessions between participants (see Moyer; [0013]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Moyer in order for Naidoo servers to create, modify, and terminate communication between the gateway and the security system utilizing SIP. One of ordinary skill in the art would be motivated because SIP is designed to be independent of the underlying transport layer and it can run on TCP, UDP, or SCTP.

18. Claim 46-47 is rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo in view of Lingemann (US 2006/0009863).

Regarding claim 46, Naidoo the invention substantially, however Naidoo does not explicitly disclose the method of claim 1, wherein the network device is a touchscreen.

Lingemann in the field of the same endeavor teaches building an automation system including user interface units with touchscreen. In particular, Lingemann

Art Unit: 2451

teaches (see Lingemann; fig. 10, [0076]; a touch screen interface unit as illustrated in fig. 10 used for controlling electrical devices).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Lingemann in order for Naidoo's device to incorporate a touchscreen. One of ordinary skill in the art would have been motivated because a touchscreen would provide an ease of interaction by allowing the user to interact with what is displayed directly on the hand, where it is displayed, rather than indirect with a mouse or touchpad.

Regarding Claim 47, Naidoo-Lingemann discloses the method of claim 24, wherein the network device is a device controller that controls an attached device (see Lingemann; fig. 10, [0076]; a touch screen interface unit as illustrated in fig. 10 used for controlling electrical devices).

19. Claim 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naidoo and in further view of Moore et al. (US 2007/0061266).

Regarding Claim 13, Naidoo substantially discloses the method of claim 1, wherein the premise local area network is coupled to a wide area network. (see Naidoo; fig. 2; [0047-0048, 0087]; the security gateway is located in the premise which is considered a LAN. The security gateway is also connected to the internet and the security system server located at the data center which is consider to be the WAN).



Art Unit: 2451

However, Naidoo does not explicitly disclose the premise local area network is coupled to a wide area network via a premise router.

Moore in the field of the same endeavor teaches large-scale, reliable, and secure foundations for distributed databases and content management systems combining unstructured and structured data, and allowing post-input reorganization to achieve a high degree of flexibility. In particular, Moore teaches a router that forward data packets across an internet work through a process known as routing that act as a junction between two networks (see Moore; [0217]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Moore in order for Naidoo premise location to include a router that act as a junction between two networks. One of ordinary skill in the art would have been motivated because the router would have improved Naidoo teachings by enabled data packets to be routed to networks.

Regarding Claim 14, the combined teachings of Naidoo and Moore further teach wherein the gateway is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network (see Naidoo; fig. 2; [0047-0048, 0087]; the security gateway is located in the premise which is considered a LAN. The security gateway is also connected to the internet and the security system server located at the data center which is considered to be the WAN and Moore use of routers (see Moore; [0217]).

Art Unit: 2451

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Naidoo with the teachings of Moore in order for Naidoo premise location to include a router that act as a junction between two networks. One of ordinary skill in the art would have been motivated because the router would have improved Naidoo teachings by enabled data packets to be routed to networks.

### ***Conclusion***

Examiner has cited particular paragraphs, columns, and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANTHONY MEJIA whose telephone number is (571)270-3630. The examiner can normally be reached on Mon-Thur 9:30AM-8:00PM EST.

Art Unit: 2451

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A.M./  
Patent Examiner, Art Unit 2451

/KAMAL B DIVECHA/

Primary Examiner, Art Unit 2451

<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 1 of 3

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,353,891 B1	03-2002	Borella et al.	726/12
*	B	US-2002/0112051 A1	08-2002	Ullman, Lorin Evan	709/224
*	C	US-2002/0112182 A1	08-2002	Chang et al.	713/201
*	D	US-2003/0009552 A1	01-2003	Benfield et al.	709/224
*	E	US-2003/0009553 A1	01-2003	Benfield et al.	709/224
*	F	US-2003/0041167 A1	02-2003	French et al.	709/238
*	G	US-6,643,652 B2	11-2003	Helgeson et al.	1/1
*	H	US-6,721,747 B2	04-2004	Lipkin, Daniel S.	709/209
*	I	US-2004/0162902 A1	08-2004	Davis, James S.	709/227
*	J	US-2004/0177163 A1	09-2004	Casey et al.	709/249
*	K	US-6,931,445 B2	08-2005	Davis, James S.	709/224
*	L	US-6,959,393 B2	10-2005	Hollis et al.	726/21
*	M	US-7,072,934 B2	07-2006	Helgeson et al.	709/203

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 2 of 3

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,099,944 B1	08-2006	Anschutz et al.	709/227
*	B	US-7,174,564 B1	02-2007	Weatherspoon et al.	726/2
*	C	US-7,222,359 B2	05-2007	Freund et al.	726/3
*	D	US-7,237,267 B2	06-2007	Rayes et al.	726/25
*	E	US-7,305,461 B2	12-2007	Ullman, Lorin Evan	709/223
*	F	US-7,337,217 B2	02-2008	Wang, Dongyan	709/217
*	G	US-7,337,473 B2	02-2008	Chang et al.	726/27
*	H	US-7,343,619 B2	03-2008	Ofek et al.	726/2
*	I	US-7,349,967 B2	03-2008	Wang, Dongyan	709/227
*	J	US-7,367,045 B2	04-2008	Ofek et al.	726/2
*	K	US-7,383,339 B1	06-2008	Meenan et al.	709/227
*	L	US-7,403,838 B2	07-2008	Deen et al.	700/276
*	M	US-7,409,451 B1	08-2008	Meenan et al.	709/227

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Notice of References Cited</b>	Application/Control No. 12/189,788	Applicant(s)/Patent Under Reexamination BAUM ET AL.	
	Examiner ANTHONY MEJIA	Art Unit 2451	Page 3 of 3

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-7,428,585 B1	09-2008	Owens et al.	709/223
*	B US-7,480,713 B2	01-2009	Ullman, Lorin Evan	709/224
*	C US-7,480,724 B2	01-2009	Zimler et al.	709/229
*	D US-7,509,687 B2	03-2009	Ofek et al.	726/30
*	E US-2007/0061266	03-2007	Moore et al.	705/051
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Index of Claims</b>  	<b>Application/Control No.</b> 12189788	<b>Applicant(s)/Patent Under Reexamination</b> BAUM ET AL.
	<b>Examiner</b> ANTHONY MEJIA	<b>Art Unit</b> 2451

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010							
	1	✓							
	2	✓							
	3	✓							
	4	✓							
	5	✓							
	6	✓							
	7	✓							
	8	✓							
	9	✓							
	10	✓							
	11	✓							
	12	✓							
	13	✓							
	14	✓							
	15	✓							
	16	✓							
	17	✓							
	18	✓							
	19	✓							
	20	✓							
	21	✓							
	22	✓							
	23	✓							
	24	✓							
	25	✓							
	26	✓							
	27	✓							
	28	✓							
	29	✓							
	30	✓							
	31	✓							
	32	✓							
	33	✓							
	34	✓							
	35	✓							
	36	✓							

<b>Index of Claims</b>  	<b>Application/Control No.</b>  12189788	<b>Applicant(s)/Patent Under Reexamination</b>  BAUM ET AL.
	<b>Examiner</b>  ANTHONY MEJIA	<b>Art Unit</b>  2451

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>


N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	08/23/2010							
	37	✓							
	38	✓							
	39	✓							
	40	✓							
	41	✓							
	42	✓							
	43	✓							
	44	✓							
	45	✓							
	46	✓							
	47	✓							
	48	✓							
	49	✓							
	50	✓							
	51	✓							



<b>Search Notes</b>  	<b>Application/Control No.</b>  12189788	<b>Applicant(s)/Patent Under Reexamination</b>  BAUM ET AL.
	<b>Examiner</b>  ANTHONY MEJIA	<b>Art Unit</b>  2451

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
709	201, 202, 203, 224, 225, 227	8/23/2010	A.M.
717	101, 102	8/23/2010	A.M.
707	203	8/23/2010	A.M.
718	101	8/23/2010	A.M.
726	1	8/23/2010	A.M.
706	46	8/23/2010	A.M.

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
EAST Class Limited w/Text Search (See Search History)	8/23/2010	A.M.
EAST Text Search (See Search History)	08/23/2010	A.M.
EAST Assignee Search (See Search History)	08/23/2010	A.M.
EAST Inventor Search (See Search History)	08/23/2010	A.M.

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

/A. M./ Examiner.Art Unit 2451	
-----------------------------------	--



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7650

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/189,788	08/12/2008	707	2451	ICON.P001D3
	<b>RULE</b>			

**APPLICANTS**

Marc Baum, San Jose, CA;  
 Paul J. Dawes, Woodside, CA;  
 Mike Kinney, Foster city, CA;  
 Reza Raji, Menlo Park, CA;  
 David Swenson, Glyndon, MN;  
 Aaron Wood, Boulder Creek, CA;

**\*\* CONTINUING DATA \*\*\*\*\***

This application is a DIV of 12/189,757 08/11/2008 which claims benefit of 60/968,005 08/24/2007 and claims benefit of 60/987,359 11/12/2007 and claims benefit of 60/987,366 11/12/2007 and claims benefit of 61/019,162 01/04/2008 and claims benefit of 61/019,167 01/04/2008 and claims benefit of 61/023,489 01/25/2008 and claims benefit of 61/023,493 01/25/2008 and claims benefit of 61/023,496 01/25/2008 and claims benefit of 61/087,967 08/11/2008 and is a CIP of 11/084,232 03/16/2005 and is a CIP of 11/761,718 06/12/2007 PAT 7,711,796 and is a CIP of 11/761,745 06/12/2007 and is a CIP of 12/019,554 01/24/2008 and is a CIP of 12/019,568 01/24/2008

**\*\* FOREIGN APPLICATIONS \*\*\*\*\***

**\*\* IF REQUIRED, FOREIGN FILING LICENSE GRANTED \*\* \*\* SMALL ENTITY \*\***

Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Met after Allowance	<b>STATE OR COUNTRY</b>	<b>SHEETS DRAWINGS</b>	<b>TOTAL CLAIMS</b>	<b>INDEPENDENT CLAIMS</b>
35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Initials	CA	14	51	4
Verified and Acknowledged <u>/ANTHONY MEJIA/</u> Examiner's Signature					

**ADDRESS**

Gregory & Martensen LLP  
 2018 Bissonnet Street  
 Houston, TX 77005  
 UNITED STATES

**TITLE**

Forming A Security Network Including Integrated Security System Components and Network Devices

<b>FILING FEE</b>	FEES: Authority has been given in Paper	<input type="checkbox"/> All Fees
		<input type="checkbox"/> 1.16 Fees (Filing)
		<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)

<b>RECEIVED</b> 1380	No. _____ to charge/credit DEPOSIT ACCOUNT	<input type="checkbox"/> 1.18 Fees (Issue)
	No. _____ for following:	<input type="checkbox"/> Other _____
		<input type="checkbox"/> Credit

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	9	"20030062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/23 09:36
L3	3976	(router) SAME (premise office warehouse home) SAME (gateway)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/23 11:02
L4	35473	709/225.ccls. 709/227.ccls. 709/224.ccls. 709/203.ccls. 726/1.ccls. 706/46.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/23 11:03
L5	303	3 AND L4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/23 11:03
L6	30578954	@ad<="20050316" @rlad<="20050316"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/23 11:03
L7	217	5 AND L6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/23 11:03
L8	151	7 AND (security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/23 11:04
L9	39	7 AND (security ADJ system)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/23 11:14

S1	17	12/189757	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/18 20:31
S2	137	("20020029276"   "20020083342"   "20020095490"   "20020103927"   "20020111698"   "20020143923"   "20020180579"   "20020184301"   "20030051009"   "20030062997"   "20030115345"   "20030132018"   "20030174648"   "20030187920"   "20030210126"   "20040003241"   "20040015572"   "20050079855"   "20050169288"   "20050197847"   "20050216302"   "20060181406"   "20070052675"   "20070286210"   "20070286369"   "20080180240"   "20080183842"   "20090240787"   "0416910"   "0451529"   "5519878"   "5991795"   "6198475"   "6219677"   "6286038"   "6288716"   "6331122"   "6363417"   "6370436"   "6377861"   "6400265"   "6467084"   "6493020"   "6496927"   "6529723"   "6542075"   "6563800"   "6574234"   "6580950"   "6587736"   "6591094"   "6601086"   "6609127"   "6615088"   "6643669"   "6648682"   "6661340"   "6721689"   "6965313"   "7113090"   "7148810"   "7349761"   "7430614"   "7440434"   "7469294"   "7526762"   "7634519").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 02:06

S3	116	("20020083342"   "20020103927"   "20020111698"   "20020143923"   "20020180579"   "20020184301"   "20030051009"   "20030132018"   "20030187920"   "20030197847"   "20030210126"   "20040003241"   "20040015572"   "20050079855"   "20050169288"   "20050216302"   "20050216580"   "20060181406"   "20070286210"   "20080180240"   "20080183842"   "5519878"   "5991795"   "6198475"   "6219677"   "6286038"   "6288716"   "6331122"   "6363417"   "6370436"   "6377861"   "6400265"   "6467084"   "6493020"   "6496927"   "6529723"   "6542075"   "6563800"   "6574234"   "6580950"   "6587736"   "6591094"   "6601086"   "6609127"   "6615088"   "6648682"   "6661340"   "6721689"   "6965313"   "7015806"   "7113090"   "7349761"   "7469294"   "7526762"   "D416910"   "D451529"   "D464328"   "D464948").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 02:09
S4	144	("20020083342"   "20020095490"   "20020103927"   "20020111698"   "20020118107"   "20020143923"   "20020180579"   "20020184301"   "20030051009"   "20030062997"   "20030115345"   "20030132018"   "20030174648"   "20030187920"   "20030197847"   "20030210126"   "20040003241"   "20040015572"   "20050038326"   "20050079855"   "20050169288"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 02:10

		"20050216302"   "20050216580"   "20060181406"   "20070052675"   "20070106124"   "20070286210"   "20070286369"   "20080183842"   "20090240787"   "5519878"   "5991795"   "6198475"   "6219677"   "6286038"   "6288716"   "6331122"   "6363417"   "6370436"   "6377861"   "6400265"   "6462663"   "6467084"   "6493020"   "6496927"   "6529723"   "6542075"   "6563800"   "6574234"   "6580950"   "6587736"   "6591094"   "6601086"   "6609127"   "6615088"   "6643669"   "6648682"   "6661340"   "6721689"   "6965313"   "7015806"   "7113090"   "7148810"   "7349761"   "7430614"   "7440434"   "7469294"   "7526762"   "7634519"   "D416910"   "D451529"   "D464328"   "D464948").PN.				
S6	28	((MARC) near2 (BAUM)).INV.	US-PGPUB; USPAT	OR	ON	2010/06/19 02:33
S7	8	((MIKE) near2 (KINNEY)).INV.	US-PGPUB; USPAT	OR	ON	2010/06/19 02:34
S9	21	((PAUL) near2 (DAWES)).INV.	US-PGPUB; USPAT	OR	ON	2010/06/19 02:35
S10	22	((REZA) near2 (RAJI)).INV.	US-PGPUB; USPAT	OR	ON	2010/06/19 02:36
S11	49	((DAVID) near2 (SWENSON)). INV.	US-PGPUB; USPAT	OR	ON	2010/06/19 02:36
S12	20	((AARON) near2 (WOOD)). INV.	US-PGPUB; USPAT	OR	ON	2010/06/19 02:36
S13	17	(iControl near Networks).AS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 02:37
S15	30558155	@ad<="20050316" @rlad<="20050316"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 02:39

S16	34268	709/225.ccls. 709/227.ccls. 709/224.ccls. 709/203.ccls. 726/1.ccls. 706/46.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 02:44
S17	26558	S15 AND S16	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 02:44
S18	117	("20010016501"   "20060009863"   "20060206220"   "20060271695"   "20070061266"   "20070142022"   "20070256105"   "4754261"   "4833449"   "4993059"   "5907279"   "6060994"   "6134591"   "6281790"   "6351829"   "6385772"   "6400265"   "6621827"   "6658091"   "6661340"   "6686838"   "6690411"   "6693545"   "6738824"   "6756998"   "6778085"   "6781509"   "6798344"   "6891838"   "6928148"   "6930599"   "6943681"   "6965313"   "6970183"   "6972676"   "6975220"   "6990591"   "7030752"   "7032002"   "7039391"   "7079020"   "7080046"   "7085937"   "7103152"   "7106176"   "7113090"   "7113099"   "7120232"   "7120233"   "7130383"   "7149798"   "7183907"   "7218217"   "7250854"   "7254779"   "7262690").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 02:50
S19	4336	(gateway) AND (wireless remotely) AND (security ADJ system) AND (location)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 03:05
S20	63	(gateway) SAME (wireless remotely) SAME (security ADJ system) SAME (location)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 03:06



S21	8	S20 AND S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 03:06
S22	53	S20 AND S15	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 03:06
S23	9	"20030062997"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 12:35
S24	29	11/084232	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/06/19 14:54
S25	1	12/189788	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2010/08/21 02:39

**8/23/2010 11:51:43 AM**

**C:\Documents and Settings\amejia\My Documents\EAST Workspaces\12189757.wsp**

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned

**U.S. PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		4,754,261		Marino, Francis C.	06-28-1988	
		4,833,449	A	Gaffigan, Robert J.	05-23-1989	
		4,993,059	A	Smith, et al.	02-12-1991	
		5,907,279	A	Bruins, et al.	05-25-1999	
		6,060,994		Chen, Scanner	05-09-2000	
		6,134,591		Nickles, Alfred E.	10-17-2000	
		6,281,790		Kimmel, et al.	08-28-2001	
		6,351,829		Dupont, et al.	02-26-2002	
		6,385,772		Courtney, Jonathan D.	05-07-2002	
		6,400,265	B1	Saylor, et al.	06-04-2002	
		6,621,827		Rezvani, et al.	09-16-2003	
		6,658,091		Naidoo, et al.	12-03-2003	
		6,661,340		Saylor, et al.	12-09-2003	
		6,686,838		Rezvani, et al.	02-03-2004	
		6,690,411		Naidoo, et al.	02-10-2004	
		6,693,545		Brown, et al.	02-17-2004	
		6,738,824	B1	Blair, Dana	05-18-2004	
		6,756,998		Bilger, Brent	06-29-2004	
		6,778,085		Faulkner, et al.	08-17-2004	
		6,781,509		Oppedahl, et al.	08-24-2004	

**FOREIGN PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				

Examiner Signature	/Anthony Mejia/	Date Considered	08/23/2010
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned

**U.S. PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		6,798,344		Faulkner, et al.	09-28-2004	
		6,891,838		Petite, et al.	05-10-2005	
		6,928,148		Simon, et al.	08-09-2005	
		6,930,599		Naidoo, et al.	08-16-2005	
		6,943,681		Rezvani, et al.	09-13-2005	
		6,965,313		Saylor, et al.	11-15-2005	
		6,970,183		Monroe, David A.	11-29-2005	
		6,972,676		Kimmel, et al.	12-06-2005	
		6,975,220		Foodman et al.	12-13-2005	
		6,990,591		Pearson, Sterling Michael	01-24-2006	
		7,030,752		Tyroler, Dan	04-18-2006	
		7,032,002		Rezvani, et al.	04-18-2006	
		7,039,391		Rezvani, et al.	05-02-2006	
		7,079,020		Stilp, Louis A.	07-18-2006	
		7,080,046		Rezvani, et al.	07-18-2006	
		7,085,937		Rezvani, et al.	08-01-2006	
		7,103,152		Naidoo, et al.	09-05-2006	
		7,106,176		La, et al.	09-12-2006	
		7,113,090	B1	Saylor, et al.	09-26-2006	
		7,113,099		Tyroler, et al	09-26-2006	

**FOREIGN PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				

Examiner Signature	/Anthony Mejia/	Date Considered	08/23/2010
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2442
	First Named Inventor: Marc Baum	Examiner Name: not assigned

**U.S. PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		7,120,232		Naidoo, et al.	10-10-2006	
		7,120,233		Naidoo, et al.	10-10-2006	
		7,130,383	B2	Naidoo, et al.	10-31-2006	
		7,149,798		Rezvani, et al.	12-12-2006	
		7,183,907		Simon, et al.	02-27-2007	
		7,218,217		Adonailo, et al.	05-15-2007	
		7,250,854		Rezvani, et al.	07-31-2007	
		7,254,779		Rezvani, et al.	08-07-2007	
		7,262,690		Heaton, et al.	08-28-2007	
		2001/0016501	A1	King, Joseph D.	08-23-2001	
		2006/0009863	A1	Lingemann, Ronald R.	01-12-2006	
		2006/0111095	A1	Weigand, David L.	05-25-2006	
		2006/0206220	A1	Amundson, John B.	09-14-2006	
		2006/0271695	A1	Lavian, Yoel	11-30-2006	
		2007/0061266	A1	Moore, et al.	03-15-2007	
		2007/0142022	A1	Madonna, et al.	06-21-2007	
		2007/0256105	A1	Tabbe, Joseph A.	11-01-2007	

**FOREIGN PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				

Examiner Signature	/Anthony Mejia/	Date Considered	08/23/2010
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form 1449/PTO	Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Filing Date: August 12, 2008	Art Unit: 2442
	First Named Inventor: Marc Baum	Examiner Name: not assigned

**NON PATENT LITERATURE DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc ), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		Form PCT/ISA/220, ICON.P001WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P001WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P001WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P002WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P002WO, "PCT International Search Report," 2 pgs	
		Form PCT/ISA/237, ICON.P002WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P003WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P003WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P003WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P005WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P005WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P005WO, "PCT Written Opinion of the International Searching Authority," 7 pgs.	

Examiner Signature	/Anthony Mejia/	Date Considered	08/23/2010
--------------------	-----------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609 Draw line through citation if not in conformance and not considered Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned

**U.S. PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		4,754,261		Marino, Francis C.	06-28-1988	
		4,833,449	A	Gaffigan, Robert J.	05-23-1989	
		4,993,059	A	Smith, et al.	02-12-1991	
		5,907,279	A	Bruins, et al.	05-25-1999	
		6,060,994		Chen, Scanner	05-09-2000	
		6,134,591		Nickles, Alfred E.	10-17-2000	
		6,281,790		Kimmel, et al.	08-28-2001	
		6,351,829		Dupont, et al.	02-26-2002	
		6,385,772		Courtney, Jonathan D.	05-07-2002	
		6,400,265	B1	Saylor, et al.	06-04-2002	
		6,621,827		Rezvani, et al.	09-16-2003	
		6,658,091		Naidoo, et al.	12-03-2003	
		6,661,340		Saylor, et al.	12-09-2003	
		6,686,838		Rezvani, et al.	02-03-2004	
		6,690,411		Naidoo, et al.	02-10-2004	
		6,693,545		Brown, et al.	02-17-2004	
		6,738,824	B1	Blair, Dana	05-18-2004	
		6,756,998		Bilger, Brent	06-29-2004	
		6,778,085		Faulkner, et al.	08-17-2004	
		6,781,509		Oppedahl, et al.	08-24-2004	

**FOREIGN PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned

**U.S. PATENT DOCUMENTS**

Exam Initial*	Cite No. <sup>1</sup>	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number	Kind Code <sup>2</sup> (If known)			
		6,798,344		Faulkner, et al.	09-28-2004	
		6,891,838		Petite, et al.	05-10-2005	
		6,928,148		Simon, et al.	08-09-2005	
		6,930,599		Naidoo, et al.	08-16-2005	
		6,943,681		Rezvani, et al.	09-13-2005	
		6,965,313		Saylor, et al.	11-15-2005	
		6,970,183		Monroe, David A.	11-29-2005	
		6,972,676		Kimmel, et al.	12-06-2005	
		6,975,220		Foodman et al.	12-13-2005	
		6,990,591		Pearson, Sterling Michael	01-24-2006	
		7,030,752		Tyroler, Dan	04-18-2006	
		7,032,002		Rezvani, et al.	04-18-2006	
		7,039,391		Rezvani, et al.	05-02-2006	
		7,079,020		Stilp, Louis A.	07-18-2006	
		7,080,046		Rezvani, et al.	07-18-2006	
		7,085,937		Rezvani, et al.	08-01-2006	
		7,103,152		Naidoo, et al.	09-05-2006	
		7,106,176		La, et al.	09-12-2006	
		7,113,090	B1	Saylor, et al.	09-26-2006	
		7,113,099		Tyroler, et al	09-26-2006	

**FOREIGN PATENT DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T <sup>6</sup>
		Office <sup>3</sup>	Number <sup>4</sup>	Kind Code <sup>5</sup> (If known)				

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered Include copy of this form with next communication to applicant.





Substitute Form 1449/PTO		Attorney Docket No.: ICON.P001D3	Application Number: 12/189,788
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>		Filing Date: August 12, 2008	Art Unit: 2442
		First Named Inventor: Marc Baum	Examiner Name: not assigned

**NON PATENT LITERATURE DOCUMENTS**

Exam. Initial*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc ), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		Form PCT/ISA/220, ICON.P001WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P001WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P001WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P002WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P002WO, "PCT International Search Report," 2 pgs	
		Form PCT/ISA/237, ICON.P002WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P003WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P003WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P003WO, "PCT Written Opinion of the International Searching Authority," 6 pgs.	
		Form PCT/ISA/220, ICON.P005WO, "PCT Notification of Transmittal of The International Search Report and the Written Opinion of the International Searching Authority, or the Declaration," 1 pg.	
		Form PCT/ISA/210, ICON.P005WO, "PCT International Search Report," 2 pgs.	
		Form PCT/ISA/237, ICON.P005WO, "PCT Written Opinion of the International Searching Authority," 7 pgs.	

Examiner Signature	Date Considered
--------------------	-----------------

**\*EXAMINER:** Initial if reference considered, whether or not citation is in conformance with MPEP 609 Draw line through citation if not in conformance and not considered Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.**

PATENT COOPERATION TREATY

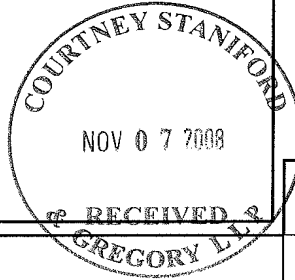
From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:  
 RICHARD L. GREGORY  
 COURTNEY STANIFORD & GREGORY LLP  
 P.O. BOX 9686  
 SAN JOSE, CA 95157

NOTIFICATION OF TRANSMITTAL OF  
 THE INTERNATIONAL SEARCH REPORT AND  
 THE WRITTEN OPINION OF THE INTERNATIONAL  
 SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)



Applicant's or agent's file reference ICON.P001WO	Date of mailing (day/month/year) 04 NOV 2008
International application No. PCT/US 08/72831	International filing date (day/month/year) 11 August 2008 (11.08.2008)
Applicant ICNTROL NETWORKS, INC.	

- The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.  
**Filing of amendments and statement under Article 19:**  
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):  
**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.  
**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35  
**For more detailed instructions,** see the notes on the accompanying sheet.
- The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
- With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
  - the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.
  - no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.
- 4. Reminders**  
 Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.  
 The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.  
 Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.  
 In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.  
 See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ICON.P001WO	<b>FOR FURTHER ACTION</b>	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 08/72831	International filing date ( <i>day/month/year</i> ) 11 August 2008 (11.08.2008)	(Earliest) Priority Date ( <i>day/month/year</i> ) 10 August 2007 (10.08.2007)
Applicant ICONTROL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of   5   sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

the international application in the language in which it was filed.

a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b.  This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c.  With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2.  **Certain claims were found unsearchable** (see Box No. II).

3.  **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

the text is approved as submitted by the applicant.

the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

the text is approved as submitted by the applicant.

the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No.   1  

as suggested by the applicant.

as selected by this Authority, because the applicant failed to suggest a figure.

as selected by this Authority, because this figure better characterizes the invention.

b.  none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 08/72831

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G08B 23/00 (2008.04)

USPC - 340/539.11

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
USPC - 340/539.11

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
USPC - 340/500, 340/501, 340/531, 340/539.1, 340/539.11, 340/539.13

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
Dialog Classic (Chinese Patent Abstracts in English, Derwent World Patents Index, European Patents Full Text, French Patents, Japanese Patent Abstracts in English, U.S. Patents Full Text/1976 to present, WIPO/PCT Patents Full Text), Google Scholar; Terms searched: cellular, gateway, network radio frequency, rf, router....

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7,113,090 B1 (Saylor et al.) 26 September 2006 (26.09.2006); all of this reference, e.g.: Figs. 2, 3, 5, 11; col. 2, ln. 32-37 and ln. 56-67; col. 3, ln. 11-13; col. 3, ln. 65 to col. 4, ln. 15 and 16-21; col. 6, ln. 33-37; col. 6, ln. 65 to col. 7, ln. 3; col. 7, ln. 33-39 and 45-46; col. 11, ln. 26-27; col. 12, ln. 42-53; col. 14, ln. 19; col. 25, ln. 41-42; col. 29, ln. 21 and 52-61; col. 31, ln. 56-60, col. 34, ln. 45-47	1-61
A	US 6,400,265 B1 (Saylor et al.) 04 June 2002 (04.06.2002)	1-61
A	US 4,833,449 A (Gaffigan) 23 May 1989 (23.05.1999)	1-61
A	US 2001/0016501 A1 (King) 23 August 2001 (23.08.2001)	1-61
A	US 4,993,059 A (Smith et al.) 12 February 1991 (12.02.1991)	1-61
A	US 5,907,279 A (Bruins et al.) 25 May 1999 (25.05.1999)	1-61

Further documents are listed in the continuation of Box C.

\* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

26 October 2008 (26.10.2008)

Date of mailing of the international search report

04 NOV 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents  
P.O. Box 1450, Alexandria, Virginia 22313-1450  
Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300  
PCT OSP: 571-272-7774

# PATENT COOPERATION TREATY

From the  
INTERNATIONAL SEARCHING AUTHORITY

## PCT

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

To: RICHARD L. GREGORY COURTNEY STANIFORD & GREGORY LLP P.O. BOX 9686 SAN JOSE, CA 95157
--

Date of mailing (day/month/year)	<b>04 NOV 2008</b>
-------------------------------------	--------------------

Applicant's or agent's file reference ICON.P001WO	<b>FOR FURTHER ACTION</b> See paragraph 2 below
--	--

International application No. PCT/US 08/72831	International filing date (day/month/year) 11 August 2008 (11.08.2008)	Priority date (day/month/year) 10 August 2007 (10.08.2007)
--	---	---

International Patent Classification (IPC) or both national classification and IPC IPC(8) - G08B 23/00 (2008.04) USPC - 340/539.11
---

Applicant ICONTROL NETWORKS, INC.
--------------------------------------

<p>1. This opinion contains indications relating to the following items:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Box No. I Basis of the opinion</li> <li><input type="checkbox"/> Box No. II Priority</li> <li><input type="checkbox"/> Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</li> <li><input type="checkbox"/> Box No. IV Lack of unity of invention</li> <li><input checked="" type="checkbox"/> Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</li> <li><input type="checkbox"/> Box No. VI Certain documents cited</li> <li><input type="checkbox"/> Box No. VII Certain defects in the international application</li> <li><input type="checkbox"/> Box No. VIII Certain observations on the international application</li> </ul> <p>2. <b>FURTHER ACTION</b></p> <p>If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.</p> <p>If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.</p> <p>For further options, see Form PCT/ISA/220.</p> <p>3. For further details, see notes to Form PCT/ISA/220.</p>
---

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion  26 October 2008 (26.10.2008)	Authorized officer:  Lee W. Young  <small>PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774</small>
---	--	--

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 08/72831

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
  - the international application in the language in which it was filed.
  - a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
  
2.  This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))
  
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:
  - a. type of material
    - a sequence listing
    - table(s) related to the sequence listing
  
  - b. format of material
    - on paper
    - in electronic form
  
  - c. time of filing/furnishing
    - contained in the international application as filed
    - filed together with the international application in electronic form
    - furnished subsequently to this Authority for the purposes of search
  
4.  In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
  
5. Additional comments:

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US 08/72831

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**1. Statement**

Novelty (N)	Claims	NONE	YES
	Claims	1-61	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-61	NO
Industrial applicability (IA)	Claims	1-61	YES
	Claims	NONE	NO

**2. Citations and explanations:**

Claims 1-61 lack novelty under PCT Article 33(2) as being anticipated by US 7,113,090 B1 (Saylor et al.).

Regarding claim 1, Saylor et al. discloses a system comprising: a gateway (Fig. 3-item 312 "radio modem") located at a first location (Fig. 2-item 310 "home"); a connection management component coupled to the gateway (Fig. 3 - item 314 "control panel"), the connection management component automatically establishing a wireless coupling with a security system installed at the first location (Fig. 3-item 314 "control panel"), the security system including security system components (Fig. 11-item 1112 "sensors: contacts, motion, etc"), wherein the connection management component forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling (Fig. 3); and a security server at a second location different from the first location, wherein security server is coupled to the gateway (Fig. 3-item 130 "central security server").

Regarding claim 2, Saylor et al. discloses the system of claim 1, wherein the gateway (Fig. 2 - item 222 "radio modem") is connected to a local area network at the first location (Fig. 2 - item 222 "radio modem" is connected via a wireless local area network as shown by "AC/60Hz" to items 212 "panic button", 214 "motion" and 216 "contact"), and the local area network is coupled to a wide area network via a router at the first location (Fig. 2-item 220 "control panel" is coupled to a wide area network shown by "~900Mhz"; col. 4, ln. 7-11 "...the Security Control Panel is simply a messaging hub which receives messages from the sensors ...and which in turn, routes those messages to the Centralized Security Control Panel.")

Regarding claim 3, Saylor et al. discloses the system of claim 1, wherein the gateway (Fig. 2 - item 222 "radio modem") is coupled to a wide area network (Fig. 2-item 222 "radio modem" is coupled to a wide area network shown by "~900Mhz") and is coupled to a local area network at the first location via the connection management component and a router at the first location (Fig. 2 - item 222 "radio modem" is coupled to a local area network as shown by "AC/60Hz" via a connection management component, i.e., item 220 "control panel" and via a wireless router as shown in Fig. 3 by the radio waves between item 220 "control panel" and items 212 "panic button", 214 "motion" and 216 "contact").

Regarding claim 4, Saylor et al. discloses the system of claim 1, wherein the gateway is coupled to the security server via the internet (col. 7, ln. 33-39-"[c]ontrol panel 220 may send a signal via radio modem 222 to radio receiver system 230...Radio receiver system 230 may then communicate with central security server 130 via a TCP/IP connection.").

Regarding claim 5, Saylor et al. discloses the system of claim 1, comprising an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user (col. 2, ln. 32-37: "[a] personalize web interface (e.g., Internet, wireless web, PDA web, etc.) may also be provided through which a user and authorized individuals may view current and historical security device status. A user may initiate contact with a web interface to conveniently view and monitor data for registered alarm sensors...)

Regarding claim 6, Saylor et al. discloses the system of claim 1, comprising a portal coupled to the gateway, wherein the portal provides access to the communications and the functions of the security network via remote client devices (col.12, ln. 46 "[a] user may also access the network via a voice portal").

Regarding claim 7, Saylor et al. discloses the system of claim 6, comprising an interface coupled to the security network, wherein the interface allows control of the functions of the security network from the remote client devices (col.12, ln. 46 "[a] user may also access the network via a voice portal where information may be communicated to the user in a voice message. For example, a user may access a personal status page...The personal status page may include...equipment control module 630...").

Regarding claim 8, Saylor et al. discloses the system of claim 6, wherein the remote client devices include one or more of personal computers (col.7, ln. 45-46: "personal computer 242"), personal digital assistants (col. 11, ln. 27: "PDA"), cellular telephones (col. 11, ln. 26-"cell phone"), and mobile computing devices (col. 11, ln. 26: "pager").

--continued in Supplemental Box--

**Supplemental Box**

**In case the space in any of the preceding boxes is not sufficient.**

Continuation of:

- Box V, Part 2 (citations and explanations)

Regarding claim 9, Saylor et al. discloses the system of claim 1, wherein the gateway including the connection management component automatically discovers the security system components (col. 6, ln. 65 to col. 7, ln. 1-3: "Each of the sensors (or group of sensors) may be equipped with a transmitter and the control panel may be equipped with a receiver. A control panel of the present invention may receive regular status information from the sensors and may be alerted when a sensor detects an alarm situation".)

Regarding claim 10, Saylor et al. discloses the system of claim 9, wherein the gateway includes protocols of the security system from the security server and uses the protocols to discover the security system components (col. 25, ln. 41-42).

Regarding claim 11, Saylor et al. discloses the system of claim 9, wherein the gateway requests and receives protocols of the security system from the security server, wherein the gateway uses the protocols received to discover the security system components (col. 25, ln. 41-42).

Regarding claim 12, Saylor et al. discloses the system of claim 1, wherein the gateway including the connection management component automatically establishes and controls the communications with the security system components (col. 2, ln. 60-67).

Regarding claim 13, Saylor et al. discloses the system of claim 1, wherein the gateway including the connection management component automatically establishes a coupling with the security system including the security system components (col. 4, ln. 16-21).

Regarding claim 14, Saylor et al. discloses the system of claim 1, wherein the gateway includes a rules component that manages rules of interaction between the gateway and the security system components (col. 25, ln. 41-42).

Regarding claim 15, Saylor et al. discloses the system of claim 1, wherein the gateway includes a device connect component that includes definitions of the security system components (col. 25, ln. 41-42).

Regarding claim 16, Saylor et al. discloses the system of claim 1, wherein the security system (Fig. 2-items 212 "panic button", 214 "motion" and 216 "contact" is coupled to a central monitoring station (Fig. 2-item 130 "central security server") via a primary communication link (Fig. 2-"A/C 60 Hz"), wherein the gateway (Fig. 2-item 22 "radio modem") is coupled to the central monitoring station (Fig. 2-item 130 "central security server") via a secondary communication link that is different than the primary communication link (Fig. 2-"~900Hz"), wherein the central monitoring station is located at a third location different from the first location and the second location (col. 6, ln. 33-37).

Regarding claim 17, Saylor et al. discloses the system of claim 16, wherein the gateway transmits event data of the security system components to the central monitoring station over the secondary communication link (col. 4, ln. 6-15).

Regarding claim 18, Saylor et al. discloses the system of claim 17, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components (col. 4, ln. 6-15).

Regarding claim 19, Saylor et al. discloses the system of claim 16, wherein the secondary communication link includes a broadband coupling (col. 4, ln. 21 "broadband").

Regarding claim 20, Saylor et al. discloses the system of claim 16, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling (col. 31, ln. 59 "GSM/GPRS").

Regarding claim 21, Saylor et al. discloses the system of claim 16, wherein the gateway (Fig. 2-item 222 "radio modem) transmits messages comprising event data of the security system components to remote client devices over the secondary communication link (col. 7, ln. 34-35).

Regarding claim 22, Saylor et al. discloses the system of claim 21, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components (col. 7, ln. 35-36).

Regarding claim 23, Saylor et al. discloses the system of claim 16, wherein the gateway receives control data for control of the security system components from remote client devices via the secondary communication link (col. 31, ln. 56-60).

Regarding claim 24, Saylor et al. discloses the system of claim 1, wherein the security network comprises network devices coupled to the gateway via a wireless coupling (Fig. 2-item 218 "home automation modules").

Regarding claim 25, Saylor et al. discloses the system of claim 24, wherein the gateway including the connection management component automatically discovers the network devices (col. 6, ln. 65 to col. 7, ln. 3: "Each of the sensors (or group of sensors) may be equipped with a transmitter and the control panel may be equipped with a receiver. A control panel of the present invention may receive regular status information from the sensors and may be alerted when a sensor detects an alarm situation".)

Regarding claim 26, Saylor et al. discloses the system of claim 24, wherein the gateway including the connection management component automatically installs the network devices in the security network (col. 6, ln. 65 to col. 7, ln. 1-3: "Each of the sensors (or group of sensors) may be equipped with a transmitter and the control panel may be equipped with a receiver. A control panel of the present invention may receive regular status information from the sensors and may be alerted when a sensor detects an alarm situation".)

--continued in Supplemental Box--



WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US 08/72831

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

- preceding supplemental box -

Regarding claim 27, Saylor et al. discloses the system of claim 24, wherein the gateway including the connection management component automatically configures the network devices for operation in the security network (col. 29, ln. 52-61).

Regarding claim 28, Saylor et al. discloses the system of claim 24, wherein the gateway (Fig. 2-item 222 "radio modem") controls communications between the network devices (Fig. 2-item 218 "home automation modules", the security system components (Fig. 2, item 214 "motion" and item 216 "contact", and the security server (Fig. 2-item 130 "central security server").

Regarding claim 29, Saylor et al. discloses the system of claim 24, wherein the gateway including the connection management component transmits event data of the network devices to remote client devices over at least one of a plurality of communication links (col. 3, ln. 11-13 "[t]he information may be conveyed via one or more preferred modes of communication (e.g., wireless communication, broadband, landline, etc.).

Regarding claim 30, Saylor et al. discloses the system of claim 29, wherein the gateway receives control data for control of the network devices from remote client devices via at least one of the plurality of communication links (col.12, ln. 43-46 and 48-53 and "[a] user of the present invention may access a web site (or other user interface) through the Internet or other communication means...For example, a user may access a personal status page where information may be observed and analyzed. The personal status page may include various modules and functions, which may include a current status report module 610 person reports module 620, equipment control module 630, and other modules and functions.").

Regarding claim 31, Saylor et al. discloses the system of claim 29, wherein the event data comprises changes in device states of the network devices, data of the network devices, and data received by the network devices (col.12, ln. 43-46 and 48-53 and "[a] user of the present invention may access a web site (or other user interface) through the Internet or other communication means...For example, a user may access a personal status page where information may be observed and analyzed. The personal status page may include various modules and functions, which may include a current status report module 610 person reports module 620, equipment control module 630, and other modules and functions.").

Regarding claim 32, Saylor et al. discloses the system of claim 24, wherein the security system (Fig. 2: "home") is coupled to a central monitoring station (Fig. 2-item 130 "central security server") via a primary communication link (Fig. 2: "~900Mhz"), wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link (col. 4, ln. 16-21).

Regarding claim 33, Saylor et al. discloses the system of claim 32, wherein the gateway transmits event data of the network devices to the central monitoring station over the secondary communication link (col. 4, ln. 16-21).

Regarding claim 34, Saylor et al. discloses the system of claim 32, wherein the secondary communication link includes a broadband coupling (col. 4, ln. 21 "broadband").

Regarding claim 35, Saylor et al. discloses the system of claim 32, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling (col. 31, ln. 59 "GSM/GPRS").

Regarding claim 36, Saylor et al. discloses the system of claim 32, wherein the gateway transmits messages comprising event data of the network devices to remote client devices over the secondary communication link (col. 7, ln. 34-35).

Regarding claim 37, Saylor et al. discloses the system of claim 24, wherein the security server creates, modifies and terminates couplings between the gateway and the network devices (col. 4, ln. 6-15).

Regarding claim 38, Saylor et al. discloses the system of claim 24, wherein the security server performs creation, modification, deletion and configuration of the network devices (col. 3, ln. 65 to col. 4, ln. 15).

Regarding claim 39, Saylor et al. discloses the system of claim 24, wherein the security server creates automations, schedules and notification rules associated with the network devices (col. 3, ln. 65 to col. 4, ln. 15).

Regarding claim 40, Saylor et al. discloses the system of claim 24, wherein the security server manages access to current and logged state data for the network devices (col. 3, ln. 65 to col. 4, ln. 15).

Regarding claim 41, Saylor et al. discloses the system of claim 24, wherein the security server manages access to current and logged state data for couplings between the gateway and the network devices (col. 3, ln. 65 to col. 4, ln. 15).

Regarding claim 42, Saylor et al. discloses the system of claim 24, wherein the security server manages communications with the network devices (col. 3, ln. 65 to col. 4, ln. 15).

Regarding claim 43, Saylor et al. discloses the system of claim 24, wherein the network device is an Internet Protocol device (col. 2, ln. 56-59).

Regarding claim 44, Saylor et al. discloses the system of claim 24, wherein the network device is a camera (col 14, ln. 19).

Regarding claim 45, Saylor et al. discloses the system of claim 24, wherein the network device is a touchscreen (col. 29, ln. 21).

--continued in Supplemental Box--

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US 08/72831

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

- preceding supplemental box -

Regarding claim 46, Saylor et al. discloses the system of claim 24, wherein the network device is a device controller that controls an attached device (col. 2, ln. 56-59).

Regarding claim 47, Saylor et al. discloses the system of claim 24, wherein the network device is a sensor (Fig. 11-item 1112 "sensors").

Regarding claim 48, Saylor et al. discloses the system of claim 1, wherein the security server creates, modifies and terminates users corresponding to the security system (col. 2, ln. 31-35).

Regarding claim 49, Saylor et al. discloses the system of claim 1, wherein the security server creates, modifies and terminates couplings between the gateway and the security system components (col. 4, ln. 6-15).

Regarding claim 50, Saylor et al. discloses the system of claim 1, wherein the security server performs creation, modification, deletion and configuration of the security system components (col. 4, ln. 6-15).

Regarding claim 51, Saylor et al. discloses the system of claim 1, wherein the security server creates automations, schedules and notification rules associated with the security system components (col. 4, ln. 6-15).

Regarding claim 52, Saylor et al. discloses the system of claim 1, wherein the security server manages access to current and logged state data for the security system components (col. 4, ln. 6-15).

Regarding claim 53, Saylor et al. discloses the system of claim 1, wherein the security server manages access to current and logged state data for couplings between the gateway and the security system components (col. 4, ln. 6-15).

Regarding claim 54, Saylor et al. discloses the system of claim 1, wherein the security server manages communications with the security system components (col. 4, ln. 6-15).

Regarding claim 55, Saylor et al. discloses the system of claim 1, wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data (Fig. 5).

Regarding claim 56, Saylor et al. discloses the system of claim 55, wherein the notifications include one or more of short message service messages (Fig. 11-item 1124 "pager") and electronic mail messages (Fig. 11-item 1122 "e-mail").

Regarding claim 57, Saylor et al. discloses the system of claim 55, wherein the event data is event data of the security system components (col. 4, ln. 6-15).

Regarding claim 58, Saylor et al. discloses the system of claim 1, wherein the security server transmits event data of the security system components to a central monitoring station of the security system over the secondary communication link (col. 4, ln. 6-15).

Regarding claim 59, Saylor et al. discloses the system of claim 1, wherein the security system components include one or more of sensors (col. 2, ln. 36 "alarm sensors"), cameras (col. 10, ln. 33 "video cameras") input/output (I/O) devices, and accessory controllers.

Regarding claim 60, Saylor et al. discloses a security network comprising: a gateway (Fig. 3-item 312 "radio modem") including a connection management component (Fig. 3 - item 314 "control panel") located at a first location (Fig. 2-item 310 "home"), the connection management component automatically establishing a wireless coupling with a security system installed at the first location (Fig. 2 "A/C 60 Hz"), the security system including security system components Fig. 2-item 214 "motion" and item 216 "contact"), wherein the connection management component forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling (Fig. 2); and a security server at a second location different from the first location, wherein security server is coupled to the gateway and includes a plurality of security network applications (Fig. 2-item 130 "central security server" and col. 34, ln. 45-47 "[c]entral security server 1630 may receive monitor data from the various remote devices for compiling, processing and/or responding").

Regarding claim 61, Saylor et al. discloses a security network comprising: a gateway (Fig. 3-item 312 "radio modem") including a connection management component (Fig. 3 - item 314 "control panel") located at a first location (Fig. 2-item 310 "home"); a wireless coupling between the gateway and a security system installed at the first location (Fig. 2 "A/C 60 Hz"), wherein the security system includes a plurality of security system components that are proprietary to the security system (Fig. 2-item 214 "motion" and item 216 "contact"), the connection management component automatically establishing the wireless coupling with the security system components and forming a security network that integrates communications and functions of the security system components into the security network (Fig. 2); and an interface coupled to the gateway, the interface providing communications with the security network and control of the functions of the security network from a remote client device (col. 12, ln. 42-53).

Claims 1-61 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used by industry.

PATENT COOPERATION TREATY

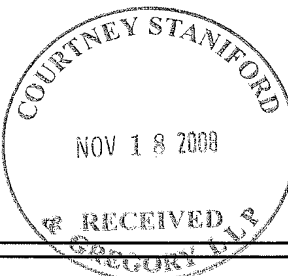
From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

To:  
 RICHARD L. GREGORY  
 COURTNEY STANIFORD & GREGORY LLP  
 P.O. BOX 9686  
 SAN JOSE, CA 95157



Applicant's or agent's file reference ICON.P002WO	Date of mailing (day/month/year)
International application No. PCT/US 08/74260	International filing date (day/month/year) 25 August 2008 (25.08.2008)
Applicant IControl Networks, Inc.	
<b>FOR FURTHER ACTION</b> See paragraphs 1 and 4 below	

- The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.  
**Filing of amendments and statement under Article 19:**  
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):  
**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.  
**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35  
**For more detailed instructions, see the notes on the accompanying sheet.**
- The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
- With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
  - the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.
  - no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.
- 4. Reminders**  
 Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.  
 The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.  
 Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.  
 In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.  
 See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer:  Lee W. Young  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ICON.P002WO	<b>FOR FURTHER ACTION</b>	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 08/74260	International filing date ( <i>day/month/year</i> ) 25 August 2008 (25.08.2008)	(Earliest) Priority Date ( <i>day/month/year</i> ) 24 August 2007 (24.08.2007)
Applicant iControl Networks, Inc.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

the international application in the language in which it was filed.

a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b.  This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c.  With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2.  **Certain claims were found unsearchable** (see Box No. II).

3.  **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

the text is approved as submitted by the applicant.

the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

the text is approved as submitted by the applicant.

the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 1

as suggested by the applicant.

as selected by this Authority, because the applicant failed to suggest a figure.

as selected by this Authority, because this figure better characterizes the invention.

b.  none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 08/74260

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 15/173, H04N 7/16 (2008.04)

USPC - 709/238; 725/143

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

USPC: 709/238; 725/143

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

USPC: 709/201, 208, 223, 238, 256; 707/1, 10; 725/25, 74, 86, 105, 135, 143, 153; search terms below

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Delphion [German (Applications - Full text), German (Granted - Full text), European (Applications - Full text), European (Granted - Full text), INPADOC, Abstracts of Japan, US (Granted - Full text), WIPO PCT Publications (Full text), US (Applications - Full text)]; Google Scholar; Google Patents; security system, gateway

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/0271695 A1 (Lavian) 30 November 2006 (30.11.2006), abstract, para [0008], [0011]-[0014], [0035], [0075].	1-73
Y	US 7,130,383 B2 (Naidoo et al.) 31 October 2006 (31.10.2006), abstract, abstract; col 6, ln 24-33, col 8, ln 7-12, col 20, ln 10-21.	1-73
Y	US 6,738,824 B1 (Blair) 18 May 2004 (18.05.2004), abstract, col 1, ln 12-30, col 2, ln 54-67, col 5, ln 22-36.	33-47

Further documents are listed in the continuation of Box C.

\* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

06 November 2008 (06.11.2008)

Date of mailing of the international search report

13 NOV 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents  
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300  
PCT OSP: 571-272-7774

**PATENT COOPERATION TREATY**

From the  
INTERNATIONAL SEARCHING AUTHORITY

**PCT**

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

To:  
RICHARD L. GREGORY  
COURTNEY STANIFORD & GREGORY LLP  
P. O. BOX 9686  
SAN JOSE, CA 95157

Date of mailing  
(day/month/year) **13 NOV 2008**

Applicant's or agent's file reference  
ICON.P002WO

**FOR FURTHER ACTION**  
See paragraph 2 below

International application No.  
PCT/US 08/74260

International filing date (day/month/year)  
25 August 2008 (25.08.2008)

Priority date (day/month/year)  
24 August 2007 (24.08.2007)

International Patent Classification (IPC) or both national classification and IPC  
IPC(8) - G06F 15/173, H04N 7/16 (2008.04)  
USPC - 709/238; 725/143

Applicant IControl Networks, Inc.

**I. This opinion contains indications relating to the following items:**

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

**2. FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

**3. For further details, see notes to Form PCT/ISA/220.**

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion  06 November 2008 (06.11.2008)	Authorized officer:  Lee W. Young  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	---	--

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 08/74260

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
  - the international application in the language in which it was filed
  - a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2.  This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:
  - a. type of material
    - a sequence listing
    - table(s) related to the sequence listing
  - b. format of material
    - on paper
    - in electronic form
  - c. time of filing/furnishing
    - contained in the international application as filed
    - filed together with the international application in electronic form
    - furnished subsequently to this Authority for the purposes of search
4.  In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US 08/74260

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	<u>1-73</u>	YES
	Claims	<u>None</u>	NO
Inventive step (IS)	Claims	<u>None</u>	YES
	Claims	<u>1-73</u>	NO
Industrial applicability (IA)	Claims	<u>1-73</u>	YES
	Claims	<u>None</u>	NO

2. Citations and explanations:

Claims 1-32 and 48-73 lack an inventive step under PCT Article 33(3) as being obvious over US 2006/0271695 A1 (Lavian) in view of US 7,130,383 B2 to Naidoo et al. (hereinafter 'Naidoo').

As to claim 1, Lavian teaches a system comprising a gateway located at a first location (abstract; para [0011]-[0012]); a video engine coupled to the gateway, the video engine automatically establishing a coupling with a camera device installed at the first location (fig 1; para [0012]; peripheral devices such as a camera connected to gateway; para [0008]; video camera/images; para [0013]-[0014]; video engine can be interpreted to include camera device, or can be interpreted to be additional peripheral devices such as a separate computing device), wherein the video engine forms a segregated network with the camera device via the coupling (para [0008]: 'video images through a secure channel, on a point to point basis'; see also para [0035]); and a security server located at a second location different from the first location (abstract: application server; para [0013]-[0014]), the security server coupled to the gateway, the security server and the video engine communicating to control routing of a video stream from the camera device to a requesting client device, the requesting client device remote to the first location and the second location (para [0012]-[0014]: authorized web user receiving video stream from camera via application server; para [0075]: remote user device). Lavian does not explicitly teach a first location, a second location different from first location. However, it would have been obvious to one of skill in the art to provide a security server system at a location different from the location of a gateway to provide for additional reliability and security. Also, Naidoo additionally teaches remote monitoring system wherein a user is in a geographically separate location than the security system and a gateway that may be located at any location (abstract; col 6, ln 24-33). See also Naidoo teaching video engine (col 8, ln 7-12; col 20, ln 10-21). It would have been obvious to combine Naidoo with Lavian in order to provide a reliable, secure, and dynamic method for a remote user to access and monitor a security system.

As to claims 2-3, Lavian further teaches wherein the gateway is connected to a local area network at the first location, and the local area network is coupled to a wide area network via a router at the first location (para [0011], [0034]), wherein the gateway is coupled to a wide area network and is coupled to a local area network at the first location via the connection management component and a router at the first location (para [0011], [0034]). See also Naidoo (col 14, ln 15-26).

As to claim 4, Lavian further teaches wherein the gateway is coupled to the security server via the internet (abstract, para [0032]).

As to claims 5-7, Lavian further teaches wherein the routing is Universal Plug and Play port forwarding, wherein the routing is relay server routing, wherein the routing is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing (para [0057]-[0059]: router; para [0067]).

As to claims 8-9, Lavian further teaches wherein the video stream is encrypted (para [0013], [0070]), wherein the gateway encrypts the video stream received from the camera device (para [0013], [0070]). See also Naidoo (col 16, ln 11-12).

As to claim 10, Naidoo further teaches wherein the video stream is a Motion Picture Experts Group (MPEG) -4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream (col 8, ln 7-12; col 20, ln 10-21).

As to claims 11-13, Lavian further teaches wherein the requesting client device initiates and establishes a Transmission Control Protocol (TCP) connection with the security server (abstract; para [0013], [0032]), wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device (abstract; para [0013], [0032]), wherein the routing is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing (para [0057]-[0059]: router; para [0067], [0082]).

As to claim 14, Naidoo further teaches wherein the video stream is a Motion Picture Experts Group (MPEG) -4 (MPEG-4) over Hypertext Transfer Protocol (HTTP) video stream (col 8, ln 7-12; col 18, ln 25-29; col 20, ln 10-21). See also Lavian (abstract).

As to claim 15-16, Lavian further teaches wherein the requesting client device initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the security server (abstract; para [0013], [0032]), wherein the security server initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device (abstract; para [0013], [0032]).

(See Supplemental Box)



WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 08/74260

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Citations and Explanations:

As to claim 17, Naidoo further teaches wherein the video stream is a Motion Joint Photographic Experts Group (JPEG) (MJPEG) video stream (col 8, In 7-12; col 20, In 10-21).

As to claims 18-19, Lavian further teaches wherein the requesting client device initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the security server (abstract, para [0013], [0032]), wherein the security server initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device (abstract; para [0013], [0032]).

As to claims 20-21, Naidoo further teaches wherein a format of the video stream is automatically selected by at least one of the gateway and the security server (col 20, In 10-21), wherein the format is one of Motion Picture Experts Group (MPEG) -4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) format, a MPEG-4 over Hypertext Transfer Protocol (HTTP) format, and a Motion Joint Photographic Experts Group (JPEG) (MJPEG) format (col 8, In 7-12; col 20, In 10-21). See also Lavian (para [0011]: gateway control; [0063]: suitable format).

As to claims 22-25, Lavian further teaches wherein the format is selected based on a capability of the requesting client device (para [0063]), wherein the format is selected based on a capability of the camera device (para [0063], [0032]), wherein the format is selected based on an authentication requirement of the requesting client device (para [0013]-[0014], [0063]), wherein the format is selected based on a privacy requirement of the requesting client device (para [0013]-[0014], [0063]).

As to claims 26-27, Lavian further teaches wherein the format is selected based on a determined capability of a network coupling the gateway to the requesting client device, wherein the determined capability is determined by at least one of the gateway and the security server (para [0011], [0013], [0063]), wherein the determined capability is relative success among a plurality of routings of the video stream (para [0011], [0013], [0063]).

As to claims 28-29, Lavian further teaches wherein the determined capability is relative success of Universal Plug and Play port forwarding (para [0011], [0082]), wherein the determined capability is relative success of Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing (para [0011], [0082], [0057]-[0059]).

As to claims 30-32, Lavian further teaches wherein the determined capability is bandwidth availability of the requesting client device (para [0011], [0063]), wherein the determined capability is processing capability of the requesting client device (para [0063]), wherein the determined capability is bandwidth availability of the camera device (para [0063], [0032]).

As to claim 48, Lavian further teaches wherein the requesting client device include one or more of a personal computer, a personal digital assistant, a cellular telephone, and a mobile computing device (abstract; para [0063]).

As to claim 49, Lavian further teaches wherein the gateway performs audio streaming between a first device and a second device, wherein the first device is located behind the gateway at the first location and the second device is located outside the gateway at a remote location (para [0032]; see also abstract; para [0011], [0013]).

As to claims 50-53, Lavian further teaches wherein the gateway performs a data transfer between a first device and a second device, wherein the first device is located behind the gateway at the first location and the second device is located outside the gateway at a remote location (para [0011]; see also abstract; para [0012]-[0013], [0081]), wherein the data transfer uses Transmission Control Protocol (TCP) (abstract; para [0013], [0032]), wherein the data transfer uses User Datagram Protocol (UDP) (abstract; para [0013], [0032]), wherein the data transfer uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) (abstract; para [0013], [0032], [0081]).

As to claims 54-58, Lavian further teaches wherein the gateway is coupled via a wireless coupling to a security system installed at the first location, the security system including security system components, wherein the gateway forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling (abstract; para [0011]-[0013]), an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user (abstract; para [0045], [0072]), wherein the gateway automatically discovers the security system components (abstract; para [0011]-[0013]), wherein the gateway includes protocols of the security system from the security server and uses the protocols to discover the security system components (para [0011], [0013], [0081]), wherein the gateway requests and receives protocols of the security system from the security server, wherein the gateway uses the protocols received to discover the security system components (abstract; para [0011], [0013], [0081]).

As to claims 59-62, Lavian further teaches wherein the gateway automatically establishes and controls the communications with the security system components (abstract; para [0011], [0013]), wherein the gateway automatically establishes a coupling with the security system including the security system components (abstract; para [0011], [0013]), wherein the gateway manages rules of interaction between the gateway and the security system components (para [0011], [0032]), wherein the gateway includes definitions of the security system components (para [0011]-[0012], [0032]). See also Naidoo (abstract; col 17, In 13-20; col 16, In 5-15).

As to claim 63, Lavian further teaches wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location (para [0088]-[0089]; see also abstract; fig 5; para [0035]). See also Naidoo (col 17, In 15-20: teaching a secondary pathway).

(See Supplemental Box)

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US 08/74260

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Citations and Explanations:

As to claims 64-67, Lavian further teaches wherein the gateway transmits event data of the security system components to the central monitoring station over the secondary communication link (para [0047]), wherein the event data comprises changes in device states of the security system components (para [0047], [0098]), data of the security system components, and data received by the security system components (para [0047], [0098]), wherein the secondary communication link includes a broadband coupling (abstract), wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling (para [0035]).

As to claims 68-70, Lavian further teaches wherein the gateway transmits messages comprising event data of the security system components to the requesting client device over the secondary communication link (para [0011], [0098]), wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components (para [0047], [0098]), wherein the gateway receives control data for control of the security system components from the requesting client device via the secondary communication link (para [0011], [0035], [0060]). See also Naidoo (col 17, ln 15-20: teaching a secondary pathway).

As to claim 71, Lavian teaches a system comprising a gateway including a video engine located at a first location (fig 1; para [0011]-[0012]: peripheral devices such as a camera connected to gateway; para [0008]: video camera/images; para [0013]-[0014]: video engine can be interpreted to include camera device, or can be interpreted to be additional peripheral devices such as a separate computing device), the gateway coupled to a local area network (LAN) of the first location, the video engine automatically establishing a coupling with a camera device installed at the first location (fig 1; para [0012]: peripheral devices such as a camera connected to gateway; para [0008]: video camera/images; para [0013]-[0014]: video engine can be interpreted to include camera device, or can be interpreted to be additional peripheral devices such as a separate computing device; see also para [0081] teaching communication of peripheral devices), wherein the video engine forms a segregated network with the camera device via the coupling (para [0008]: 'video images through a secure channel, on a point to point basis'); and a security server located at a second location different from the first location, wherein the security server is coupled to the gateway using a wide area network (WAN) (abstract: application server; para [0013]-[0014]), the security server and the video engine communicating to control routing of a video stream from the camera device to a requesting client device, the requesting client device remote to the first location and the second location (para [0012]-[0014]: authorized web user receiving video stream from camera via application server; para [0075]: remote user device). Lavian does not explicitly teach a first location, a second location different from first location. However, it would have been obvious to one of skill in the art to provide a security server system at a location different from the location of a gateway to provide for additional reliability and security. Also, Naidoo additionally teaches remote monitoring system wherein a user is in a geographically separate location than the security system and a gateway that may be located at any location (abstract; col 6, ln 24-33). See also Naidoo teaching video engine (col 8, ln 7-12; col 20, ln 10-21), LAN and WAN (col 14, ln 15-20). It would have been obvious to combine Naidoo with Lavian in order to provide a reliable, secure, and dynamic method for a remote user to access and monitor a security system.

As to claim 72, Lavian teaches a system comprising a gateway located at a first location, the gateway coupled to a local area network (LAN) of the first location; a video engine coupled to the gateway, the video engine automatically establishing a coupling with a camera device installed at the first location (abstract; fig 1; para [0011]- [0012]: peripheral devices such as a camera connected to gateway; para [0008]: video camera/images; para [0013]-[0014]: video engine can be interpreted to include camera device, or can be interpreted to be additional peripheral devices such as a separate computing device; see also para [0081] teaching communication of peripheral devices), wherein the video engine forms a segregated network with the camera device via the coupling (para [0008]: 'video images through a secure channel, on a point to point basis'; see also para [0035]); and a security server located at a second location different from the first location, wherein the security server is coupled to the gateway using a wide area network (WAN) (abstract: application server; para [0013]-[0014]), the security server and the video engine communicating to control routing of a video stream from the camera device to a requesting client device, the requesting client device remote to the first location and the second location (para [0012]-[0014]: authorized web user receiving video stream from camera via application server; para [0075]: remote user device). Lavian does not explicitly teach automatically establishing a coupling with a camera device. However, automatic discovery and detection of peripheral devices in a network are well known in the art, in addition, Lavian further teaches communication of devices in a home automation system. Hence, it would have been obvious to provide automatic coupling in order to provide fast and reliable connections in a network system. Lavian does not explicitly teach a first location, a second location different from first location. However, it would have been obvious to one of skill in the art to provide a security server system at a location different from the location of a gateway to provide for additional reliability and security. Also, Naidoo additionally teaches remote monitoring system wherein a user is in a geographically separate location than the security system and a gateway that may be located at any location (abstract; col 6, ln 24-33). See also Naidoo teaching video engine (col 8, ln 7-12; col 20, ln 10-21), LAN and WAN (col 14, ln 15-20). It would have been obvious to combine Naidoo with Lavian in order to provide a reliable, secure, and dynamic method for a remote user to access and monitor a security system.

(See Supplemental Box)

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Citations and Explanations:

As to claim 73, Lavian teaches a system comprising a gateway including a video engine located at a first location, the gateway coupled to a local area network (LAN) of the first location, the video engine automatically establishing a coupling with a camera device installed at the first location (abstract; fig 1; para [0011]-[0012]; peripheral devices such as a camera connected to gateway; para [0008]; video camera/images; para [0013]-[0014]; video engine can be interpreted to include camera device, or can be interpreted to be additional peripheral devices such as a separate computing device; see also para [0081] teaching communication of peripheral devices), wherein the video engine forms a segregated network with the camera device via the coupling (para [0008]: 'video images through a secure channel, on a point to point basis'; see also para [0035]); a security server located at a second location different from the first location (abstract: application server; para [0013]-[0014]), wherein the security server is coupled to the gateway using a wide area network (WAN), the security server and the video engine communicating to (abstract; para [0011]-[0014], [0075]); an interface coupled to the gateway and the security server (abstract; para [0013], [0034]), the interface receiving requests from a requesting client device for a video stream from the camera device and providing the video stream from the camera device to the requesting client device, the requesting client device remote to the first location and the second location (para [0012]-[0014]: authorized web user receiving video stream from camera via application server; para [0075]: remote user device). Lavian does not explicitly teach automatically establishing a coupling with a camera device. However, automatic discovery and detection of peripheral devices in a network are well known in the art, in addition, Lavian further teaches communication of devices in a home automation system. Hence, it would have been obvious to provide automatic coupling in order to provide fast and reliable connections in a network system. Lavian does not explicitly teach a first location, a second location different from first location. However, it would have been obvious to one of skill in the art to provide a security server system at a location different from the location of a gateway to provide for additional reliability and security. Also, Naidoo additionally teaches remote monitoring system wherein a user is in a geographically separate location than the security system and a gateway that may be located at any location (abstract; col 6, ln 24-33). See also Naidoo teaching video engine (col 8, ln 7-12; col 20, ln 10-21), LAN and WAN (col 14, ln 15-20). It would have been obvious to combine Naidoo with Lavian in order to provide a reliable, secure, and dynamic method for a remote user to access and monitor a security system.

Claims 33-47 lack an inventive step under PCT Article 33(3) as being obvious over Lavian in view of Naidoo and in further view of US 6,738,824 B1 (Blair).

As to claim 33, Lavian further teaches wherein the format of the video stream is automatically selected according to a priority (para [0011], [0013], [0063]). Neither Lavian nor Naidoo explicitly teach a priority. However, priorities for various data transfers in a network system are well known in the art. In addition, Blair teaches priority levels in a network system (abstract; col 1, ln 12-30; col 2, ln 54-67; col 5, ln 22-36). Hence, it would have been obvious to combine Blair with Lavian and Naidoo to have priorities for various data in order to ensure that transmitted data is relevant and reliable when sent to the end user.

As to claims 34-37, Naidoo further teaches wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a first priority, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a second priority, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a third priority, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol (HTTP) video stream has a fourth priority (col 8, ln 7-12; col 20, ln 10-21; col 16, ln 11-12). See also Lavian para (abstract; para [0011], [0013], [0032], [0042], [0070]). See also Blair (abstract; col 1, ln 12-30; col 2, ln 54-67; col 5, ln 22-36).

As to claims 38-42, Naidoo further teaches wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream has a fifth priority, wherein the gateway encrypts the video stream from the camera device, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a sixth priority, wherein the gateway encrypts the video stream from the camera device, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a seventh priority, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has an eighth priority, wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has a ninth priority, wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein one of the gateway and the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing (col 8, ln 7-12; col 20, ln 10-21; col 16, ln 11-12). See also Lavian para (abstract; para [0011], [0013], [0032], [0042], [0070]). See also Blair (abstract; col 1, ln 12-30; col 2, ln 54-67; col 5, ln 22-36).

As to claims 43-47, Naidoo further teaches wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has a tenth priority, wherein the security server facilitates Hypertext Transfer Protocol (HTTP) routing, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has an eleventh priority, wherein one of the gateway and the security server facilitates Hypertext Transfer Protocol (HTTP) routing, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol (HTTP) video stream has a twelfth priority, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a thirteenth priority, wherein the security server facilitates routing, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a fourteenth priority, wherein one of the gateway and the security server facilitates routing (col 8, ln 7-12; col 20, ln 10-21; col 16, ln 11-12). See also Lavian para (abstract; para [0011], [0013], [0032], [0042], [0070]). See also Blair (abstract; col 1, ln 12-30; col 2, ln 54-67; col 5, ln 22-36).

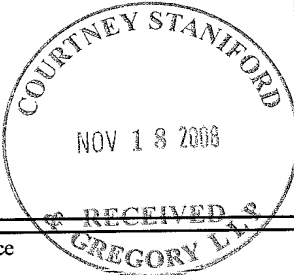
Claims 1-73 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.

**PATENT COOPERATION TREATY**

From the INTERNATIONAL SEARCHING AUTHORITY

**PCT**

To:  
 RICHARD L. GREGORY  
 COURTNEY STANIFORD & GREGORY LLP  
 P.O. BOX 9686  
 SAN JOSE, CA 95157



NOTIFICATION OF TRANSMITTAL OF  
 THE INTERNATIONAL SEARCH REPORT AND  
 THE WRITTEN OPINION OF THE INTERNATIONAL  
 SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference ICON.P003WO	Date of mailing (day/month/year) <b>FOR FURTHER ACTION</b> See paragraphs 1 and 4 below
International application No. PCT/US 08/74246	International filing date (day/month/year) <b>25 August 2008 (25.08.2008)</b>
Applicant <b>ICONTROL NETWORKS, INC.</b>	

1.  The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

**Filing of amendments and statement under Article 19:**  
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

**For more detailed instructions,** see the notes on the accompanying sheet.

2.  The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3.  **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.


4. **Reminders**  
 Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	---

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ICON.P003WO	<b>FOR FURTHER ACTION</b>	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 08/74246	International filing date ( <i>day/month/year</i> ) 25 August 2008 (25.08.2008)	(Earliest) Priority Date ( <i>day/month/year</i> ) 24 August 2007 (24.08.2007)
Applicant ICONTROL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of  9  sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

the international application in the language in which it was filed.

a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b.  This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c.  With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2.  **Certain claims were found unsearchable** (see Box No. II).

3.  **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

the text is approved as submitted by the applicant.

the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

the text is approved as submitted by the applicant.

the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No.  1

as suggested by the applicant.

as selected by this Authority, because the applicant failed to suggest a figure.

as selected by this Authority, because this figure better characterizes the invention.

b.  none of the figures is to be published with the abstract.

**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/US 08/74246

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC(8) - G06F 3/041 (2008.04)  
 USPC - 345/173  
 According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**  
 Minimum documentation searched (classification system followed by classification symbols)  
 IPC(8): G06F 3/041 (2008.04)  
 USPC: 345/173

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
 USPC: 345/173, 418, 156; 379/29; 709/201, 217, 223, 220 (text search)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
 WEST(USPT,PGPB,EPAB,JPAB,USOCR); Freepatentsonline.com, DialogWeb (databases 2, 65), Google; Search terms used:  
 thermostat controller touchscreen priority loadbalancing account login automation PLC network interface wireless 802 11 IP surveillance security


**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/0142022 A1 (Madonna et al.) 21 June 2007 (21.06.2007), Fig. 1, 2 para [0040]-[0065], [0082]-[0087], [091]-[0099], [0108]-[0123]	1-61
A	US 2006//0009863 A1 (Lingemann) 12 January 2006 (12.01.2006), entire document	1-61
A	US 2006/0206220 A1 (Amundson) 14 September 2006 (14.09.2006), entire document	1-61

Further documents are listed in the continuation of Box C.

\* Special categories of cited documents:  
 "A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier application or patent but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed  
 "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search 02 November 2008 (02.11.2008)	Date of mailing of the international search report <b>14 NOV 2008</b>
--	--

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774 
---	---

**PATENT COOPERATION TREATY**

From the  
INTERNATIONAL SEARCHING AUTHORITY

**PCT**

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

To:  
RICHARD L. GREGORY  
COURTNEY STANIFORD & GREGORY LLP  
P.O. BOX 9686  
SAN JOSE, CA 95157

Date of mailing  
(day/month/year) **14 NOV 2008**

Applicant's or agent's file reference <b>ICON.P003WO</b>		<b>FOR FURTHER ACTION</b> See paragraph 2 below	
International application No. <b>PCT/US 08/74246</b>	International filing date (day/month/year) <b>25 August 2008 (25.08.2008)</b>	Priority date (day/month/year) <b>24 August 2007 (24.08.2007)</b>	
International Patent Classification (IPC) or both national classification and IPC <b>IPC(8) - G06F 3/041 (2008.04)</b> <b>USPC - 345/173</b>			
Applicant <b>ICONTROL NETWORKS, INC.</b>			

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application


2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion <b>02 November 2008 (02.11.2008)</b>	Authorized officer: <b>Lee W Young</b>  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7174
---	--	---

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 08/74246

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
  - the international application in the language in which it was filed.
  - a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
  
2.  This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
  
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:
  - a. type of material
    - a sequence listing
    - table(s) related to the sequence listing
  
  - b. format of material
    - on paper
    - in electronic form
  
  - c. time of filing/furnishing
    - contained in the international application as filed
    - filed together with the international application in electronic form
    - furnished subsequently to this Authority for the purposes of search
  
4.  In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
  
5. Additional comments:



**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US 08/74246

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**1. Statement**

Novelty (N)	Claims	NONE	YES
	Claims	1-61	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-61	NO
Industrial applicability (IA)	Claims	1-61	YES
	Claims	NONE	NO

**2. Citations and explanations:**

Claims 1-61 lack novelty under PCT Article 33(2) as being anticipated by US 2007/0142022 A1 to Madonna et al. (hereinafter 'Madonna').

Regarding claim 1, Madonna teaches a device comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; and a plurality of interfaces coupled to the processor and presented to a user via the touchscreen, wherein the plurality of interfaces include a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]), wherein the network interface allows the user to transfer content to and from a wide area network (WAN) coupled to the LAN; and a remote server coupled to the touchscreen, the remote server managing at least one of the touchscreen and the security system (a remote touchscreen service communicates between the home network and the Internet, cellular or satellite network; para [0053], [0058], [0060], [0062], [0106]).

Regarding claim 2, Madonna teaches the remote server allows a user to configure content of the touchscreen (para [0064], [0065], [0069], [0070], [0087]).

Regarding claim 3, Madonna teaches the remote server provides user portals that enable content and information displayed on the touchscreen to be displayed on other devices (para [0047], [0059], [0093]).

Regarding claim 4, Madonna teaches the other devices include at least one of HTML browsers, WEB/WAP phones, and desktop widgets (a remote touchscreen service communicates between the home network and the Internet, cellular or satellite network; para [0053], [0058], [0060], [0062], [0106]).

Regarding claim 5, Madonna teaches the security system is managed via applications entirely within the touchscreen (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 6, Madonna teaches the touchscreen includes a wireless transceiver for communicating with security system components of the security system (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 7, Madonna teaches the touchscreen plays live video from a camera, wherein the camera is an Internet Protocol (IP) camera (para [0051], [0059], [0097], [0119], [0106]).

Regarding claim 8, Madonna teaches the camera is at the first location (para [0051], [0059], [0097], [0119], [0106]).

Regarding claim 9, Madonna teaches the camera is at a second location managed by the remote server (para [0051], [0059], [0097], [0119], [0106]).

Regarding claim 10, Madonna teaches the live video is accessed through internet content widgets (para [0093], [0094], [0097], [0108]).

Regarding claim 11, Madonna teaches the live video is IP video (para [0060], [0062], [0093]-[0097]).

Regarding claim 12, Madonna teaches the live video is MPEG-4 video (para [0099]).

Regarding claim 13, Madonna teaches the live video is Motion JPEG (MJPEG) video (para [0099]).

Regarding claim 14, Madonna teaches devices are added to the security system through the touchscreen (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 15, Madonna teaches devices are added to a user account on the remote server through the touchscreen (user service component profile; para [0055], [0069], [0085], [0123]).

--SEARCH CONTINUED IN SUPPLEMENTAL BOX--

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US 08/74246

**Supplemental Box**

**In case the space in any of the preceding boxes is not sufficient.**

Continuation of:  
Box No. V. 2. Citations and explanations:

Regarding claim 16, Madonna teaches device information and device data are transmitted to from the devices to the remote server (user service component profile; para [0055], [0069], [0085], [0123]).

Regarding claim 17, Madonna teaches the device information includes at least one of device name and device type, wherein the device data includes at least one of device state and battery state (user service component profile with device discovery service; para [0055], [0069], [0085], [0123]).

Regarding claim 18, Madonna teaches device information and device data are associated with a user account by the remote server (user service component profile; para [0055], [0065], [0069], [0085], [0123]).

Regarding claim 19 Madonna teaches the devices are automatically detected by the touchscreen and added to a user account on the remote server through the touchscreen (user service component profile with device discovery service; para [0055], [0069], [0085], [0123]).

Regarding claim 20, Madonna teaches the coupling with the LAN is over 802.11 (Wi-Fi para [0050], [0091]).

Regarding claim 21, Madonna teaches the touchscreen integrates the content with the access and control of the security system (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 22, Madonna teaches the content includes interactive content in the form of internet widgets (para [0093], [0094], [0097], [0108]).

Regarding claim 23, Madonna teaches the network interface allows the user to transfer at least one of content and internet widgets to and from the LAN (para [0093], [0094], [0097], [0108]).

Regarding claim 24, Madonna teaches the network interface allows the user to control functions of peripheral devices of the first location coupled to the LAN (user service component profile; para [0055], [0069], [0085], [0123]).

Regarding claim 25, Madonna teaches the plurality of interfaces are configurable (user service component profile; para [0055], [0069], [0085], [0123]).

Regarding claim 26, Madonna teaches the network interface provides the user with communication and control of a plurality of network devices coupled to the LAN (user service component profile; para [0055], [0069], [0085], [0123]).

Regarding claim 27, Madonna teaches the network interface provides the user with communication and control of a plurality of security system components, wherein the security system comprises the plurality of security system components (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 28, Madonna teaches the WAN is the internet and the network interface is a web browser (a remote touchscreen service communicates between the home network and the Internet, cellular or satellite network; para [0053], [0058], [0060], [0062], [0106]).

Regarding claim 29 Madonna teaches the touchscreen integrates at least one of a security system control panel and an internet browser (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 30, Madonna teaches an application engine coupled to the processor, wherein the application engine controls a plurality of applications executing under the processor (para [0053], [0055], [0057], [0064], [0082]).

Regarding claim 31, Madonna teaches the plurality of applications includes a security application and a content application, wherein the security application provides the security interface and the content application provides the network interface (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 32, Madonna teaches the plurality of applications provides interactivity with a plurality of devices via the plurality of interfaces (Fig. 1; para [0047], [0059], [0093]).

Regarding claim 33, Madonna teaches the plurality of devices are coupled to the processor. (Fig. 2; para [0050], [0051]).

Regarding claim 34, Madonna teaches the plurality of devices are coupled to the processor via a wireless coupling (Wi-Fi para [0050], [0091]).

Regarding claim 35, Madonna teaches the plurality of devices include a plurality of devices of the security system (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 36, Madonna teaches the plurality of devices include a plurality of devices of the LAN (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 37, Madonna teaches the plurality of devices include a plurality of devices of the WAN (para [0047], [0059], [0093]).

--SEARCH CONTINUED IN NEXT SUPPLEMENTAL BOX--

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US 08/74246

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Box No. V. 2. Citations and explanations:

Regarding claim 38, Madonna teaches the plurality of applications are accessed and loaded directly via the WAN (para [0055], [0064]).

Regarding claim 39 Madonna teaches the touchscreen includes the plurality of applications (Fig. 1; para [0053], [0055], [0064]).

Regarding claim 40, Madonna teaches the plurality of applications includes a resident application that manages interactions between the plurality of applications (Fig. 1; para [0053], [0055], [0064]).

Regarding claim 41, Madonna teaches the resident application manages interactions between the plurality of devices (Fig. 1; para [0053], [0055], [0064]).

Regarding claim 42, Madonna teaches the resident application determines a priority of each application of the plurality of applications and manages the plurality of applications according to the priority (task allocation and loadsharing using high-level applications; para [0056], [0059]).

Regarding claim 43, Madonna teaches the resident application allows a first application having a first priority to override a second application having a second priority when the first priority is higher than the second priority (task allocation and loadsharing using high-level applications; para [0056], [0059]).

Regarding claim 44, Madonna teaches a first application engine coupled to the processor, wherein the first application engine executes a security application that provides the security interface (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]).

Regarding claim 45, Madonna teaches a second application engine coupled to the processor, wherein the second application engine executes a content application that provides the network interface (a remote touchscreen service communicates between the home network and the Internet, cellular or satellite network; para [0053], [0058], [0060], [0062], [0106]).

Regarding claim 46, Madonna teaches a core engine coupled to the processor, the core engine controlling dynamic provisioning of the plurality of applications and the content (task allocation and loadsharing using high-level applications; para [0053], [0055], [0056], [0057], [0059], [0064], [0082]).

Regarding claim 47, Madonna teaches the core engine manages images received from a plurality devices of at least one of the security system and the LAN.

Regarding claim 48, Madonna teaches the images include video (para [0059], [0106]).

Regarding claim 49 Madonna teaches the processor is coupled to the WAN via a broadband coupling (para [0060]).

Regarding claim 50, Madonna teaches the processor is coupled to the WAN via a cellular data coupling (para [0060]).

Regarding claim 51, Madonna teaches the plurality of interfaces provides interactivity with a plurality of devices via the plurality of interfaces (para [0041], [0044], [0047]).

Regarding claim 52, Madonna teaches a device of the plurality of devices is an Internet Protocol device (para [0051], [0059], [0097], [0119], [0106]).

Regarding claim 53, Madonna teaches a device of the plurality of devices is a camera (para [0041], [0051], [0059], [0097], [0119], [0106]).

Regarding claim 54, Madonna teaches a device of the plurality of devices is another touchscreen (touchscreen controller linking; para [0051]).

Regarding claim 55, Madonna teaches a device of the plurality of devices is a device controller that controls an attached device (Fig. 1; para [0040], [0050]-[0053]).

Regarding claim 56, Madonna teaches the device controller is a thermostat (HVAC; para [0042], [0106]).

Regarding claim 57, Madonna teaches the device controller is an energy meter (HVAC or heating management; para [0042], [0049], [0106]).

Regarding claim 58, Madonna teaches a device of the plurality of devices is a sensor (para [0041], [0042]).

Regarding claim 59 Madonna teaches the network interface allows a user to control functions of peripheral devices coupled to other touchscreens located at remote locations (para [0040]-[0044], [0106]).

--SEARCH CONTINUED IN NEXT SUPPLEMENTAL BOX--

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US 08/74246

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Box No. V. 2. Citations and explanations:

Regarding claim 60, Madonna teaches a device comprising: a touchscreen at a first location, wherein the touchscreen includes a processor coupled to a local area network (LAN) and a security system at the first location; and a plurality of applications coupled to the processor, the plurality of applications displaying a plurality of interfaces to a user via the touchscreen, the plurality of interfaces including a security interface and a network interface, wherein the security interface provides the user with control of functions of the security system and access to data collected by the security system (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]), wherein the network interface allows the user to transfer content to and from a remote network coupled to the LAN; and a remote server coupled to the touchscreen, the remote server managing at least one of the touchscreen and the security system (a remote touchscreen service communicates between the home network and the Internet, cellular or satellite network; para [0053], [0058], [0060], [0062], [0106]).

Regarding claim 61, Madonna teaches a device comprising: an input/output (I/O) device at a first location, the I/O device comprising a processor coupled to a local area network (LAN) and a security system at the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system; a security application coupled to the processor, the security application providing a security interface for control of functions of the security system, the security interface presented to a user via the I/O device (a touch screen home security remote controller interface device; Fig. 1; para [0040], [0050], [0051], [0106]); a content application coupled to a processor, the content application providing a network interface for access to networked content of a remote wide area network (WAN), the network interface presented to a user via the I/O device, wherein the I/O device is coupled to the WAN via the LAN; and a remote server coupled to the I/O device, the remote server managing at least one of the I/O device and the security system (a remote touchscreen service communicates between the home network and the Internet, cellular or satellite network; para [0053], [0058], [0060], [0062], [0106]).

Claims 1-61 have industrial applicability as defined by PCT Article 33(4), because the subject matter can be made or used in industry.

PATENT COOPERATION TREATY

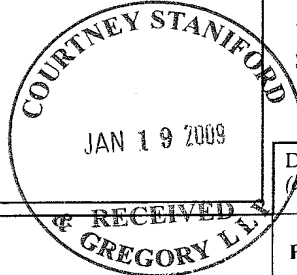
From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:  
 RICHARD L. GREGORY  
 COURTNEY STANIFORD & GREGORY LLP  
 P.O. BOX 9686  
 SAN JOSE, CA 95157

NOTIFICATION OF TRANSMITTAL OF  
 THE INTERNATIONAL SEARCH REPORT AND  
 THE WRITTEN OPINION OF THE INTERNATIONAL  
 SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)



Applicant's or agent's file reference ICON.P005WO	Date of mailing (day/month/year)
International application No. PCT/US 08/83254	<b>FOR FURTHER ACTION</b> See paragraphs 1 and 4 below  International filing date (day/month/year) 12 November 2008 (12.11.2008)
Applicant: ICNTROL NETWORKS, INC.	

1.  The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

**Filing of amendments and statement under Article 19:**

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

**For more detailed instructions,** see the notes on the accompanying sheet.

2.  The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3.  **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices

no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis 1 and 90bis 3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II. National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer:  Lee W. Young  PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference ICON.P005WO	<b>FOR FURTHER ACTION</b>	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 08/83254	International filing date ( <i>day/month/year</i> ) 12 November 2008 (12.11.2008)	(Earliest) Priority Date ( <i>day/month/year</i> ) 12 November 2007 (12.11.2007)
Applicant ICONTROL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of:

the international application in the language in which it was filed.

a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b.  This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c.  With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2.  **Certain claims were found unsearchable** (see Box No. II).

3.  **Unity of invention is lacking** (see Box No. III).

4. With regard to the **title**,

the text is approved as submitted by the applicant

the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

the text is approved as submitted by the applicant.

the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 1

as suggested by the applicant.

as selected by this Authority, because the applicant failed to suggest a figure

as selected by this Authority, because this figure better characterizes the invention

b.  none of the figures is to be published with the abstract.

**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/US 08/83254

<p><b>A. CLASSIFICATION OF SUBJECT MATTER</b>                  IPC(8) - G06F 17/00 (2009 01)                  USPC - 726/14                  According to International Patent Classification (IPC) or to both national classification and IPC</p>		
<p><b>B. FIELDS SEARCHED</b>                  Minimum documentation searched (classification system followed by classification symbols)                  IPC(8): G06F 17/00 (2009 01)                  USPC: 726/14</p>		
<p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched                  USPC: 726/2-5,14 (view text search terms below)</p>		
<p>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)                  pubWEST(PGPB,USPT,EPAB,JPAB; PLUR=YES); DialogWeb; Google Scholar; Google Patent; Text search terms: security, home, business, touchscreen, security, network, content, interactivity, management, presentation, PC, laptop, PDA, mobile, phone, telephone, smartphone cell, broadband, gateway, wireless, coupling, security, LAN ...</p>		
<p><b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b></p>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/0256105 A1 (TABE) 01 November 2007 (01.11.2007) entire document, especially Abstract, FIGS 3 and 13; and para [0044], [0054]-[0055], [0061], [0063]-[0066], [0080], [0084]-[0085], [0088]-[0089], [0091]-[0094], [0096], [0100], [0123], [0133], [0138], [0144], [0150]-[0151], [0159], [0163], [0166], [0171], [0177]-[0178], [0186], [0197], [0199] and [0201]	1-19, 21-80 ----- 20
Y	US 2006/0111095 A1 (WEIGAND) 25 May 2006 (25.05.2006) entire document especially Abstract, para [0011], [0019]	20
A	US 2007/0061266 A1 (MOORE, et al.) 15 March 2007 (15.03.2007) entire document	1-80
<p><input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/></p>		
<p>* Special categories of cited documents:</p>		
"A"	document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E"	earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed	
<p>Date of the actual completion of the international search 06 January 2009 (06.01.2009)</p>		<p>Date of mailing of the international search report 14 JAN 2009</p>
<p>Name and mailing address of the ISA/US                  Mail Stop PCT, Attn: ISA/US, Commissioner for Patents                  P O Box 1450 Alexandria, Virginia 22313-1450                  Facsimile No. 571-273-3201</p>		<p>Authorized officer: Lee W. Young                  PCT Helpdesk: 571-272-4300                  PCT OSP: 571-272-7774</p>

**PATENT COOPERATION TREATY**

From the  
INTERNATIONAL SEARCHING AUTHORITY

**PCT**

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

To:  
RICHARD L. GREGORY  
COURTNEY STANIFORD & GREGORY LLP  
P.O. BOX 9686  
SAN JOSE, CA 95157

Date of mailing  
(day/month/year) 14 JAN 2009

Applicant's or agent's file reference  
ICON.P005WO

**FOR FURTHER ACTION**  
See paragraph 2 below

International application No.  
PCT/US 08/83254

International filing date (day/month/year)  
12 November 2008 (12.11.2008)

Priority date (day/month/year)  
12 November 2007 (12.11.2007)

International Patent Classification (IPC) or both national classification and IPC  
IPC(8) - G06F 17/00 (2009.01)  
USPC - 726/14

Applicant ICONTROL NETWORKS, INC.

1 This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis 1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

**2. FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3 For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/US  
Mail Stop PCT Attn: ISA/US  
Commissioner for Patents  
P O. Box 1450, Alexandria, Virginia 22313-1450  
Facsimile No. 571-273-3201

Date of completion of this opinion  
06 January 2009 (06.01.2009)

Authorized officer:  
Lee W Young  
PCT Helpdesk: 571-272-4300  
PCT OSP: 571-272-7774



WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No

PCT/US 08/83254

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

- the international application in the language in which it was filed  
 a translation of the international application into \_\_\_\_\_ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2.  This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. type of material

- a sequence listing  
 table(s) related to the sequence listing

b. format of material

- on paper  
 in electronic form

c. time of filing/furnishing

- contained in the international application as filed  
 filed together with the international application in electronic form  
 furnished subsequently to this Authority for the purposes of search

4.  In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished

5. Additional comments:

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US 08/83254

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	20	YES
	Claims	1-19, 21-80	NO
Inventive step (IS)	Claims	NONE	YES
	Claims	1-80	NO
Industrial applicability (IA)	Claims	1-80	YES
	Claims	NONE	NO

2. Citations and explanations:

Claims 1-19 and 21-80 lack novelty under PCT Article 33(2) as being anticipated by US 2007/0256105 A1 (Tabe).

As to claim 1, Tabе teaches a system comprising: a gateway located at a first location (para [0091]); a takeover component coupled to the gateway, the takeover component automatically extracting security data of a security system from a first controller coupled to the security system, the security system including security system components (para [0171]); and a connection management component coupled to the gateway, the connection management component automatically forming a security network that includes a second controller coupled to the security system components and the gateway, wherein the second controller replaces the first controller, wherein the gateway uses the security data extracted from the first controller to integrate communications and functions of the security system components into the security network (Fig 13, para [0080]).

As to claim 2, Tabе teaches the takeover component automatically transfers the security data extracted from the first controller to the second controller (para [0171]).

As to claim 3, Tabе teaches the takeover component automatically loads the security data extracted from the first controller in the second controller (para [0171]).

As to claim 4, Tabе teaches the gateway automatically enrolls the security system components in the second controller using the security data (para [0091]).

As to claim 5, Tabе teaches a security server at a second location different from the first location, wherein the security server is coupled to the gateway (para [0091]).

As to claim 6, Tabе teaches the security server receives the security data from the gateway (para [0084] - distribution of security data).

As to claim 7, Tabе teaches the security server stores the security data. (para [0093]).

As to claim 8, Tabе teaches the gateway automatically loads the security data in the second controller (para [0084] - distribution of security data).

As to claim 9, Tabе teaches the gateway automatically queries the security server for the security data (para [0084]).

As to claim 10, Tabе teaches the gateway receives the security data from the security server in response to the query (para [0084], [0091]).

As to claim 11, Tabе teaches the gateway is coupled to the security server via the internet (para [0085], [0091]).

As to claim 12, Tabе teaches the security server creates, modifies and terminates users corresponding to the security system (para [0092]).

As to claim 13, Tabе teaches the security server creates, modifies and terminates couplings between the gateway and the security system components (para [0092]).

As to claim 14, Tabе teaches the security server performs creation, modification, deletion and configuration of the security system components (para [0096]).

As to claim 15, Tabе teaches the security server creates automations, schedules and notification rules associated with the security system components (para [0201] - notifies the host).

- Please See Continuation Sheet -

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No

PCT/US 08/83254

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Box V.2 Citations and explanations:

As to claim 16, Tabe teaches the security server manages access to current and logged state data for the security system components (para [0088] - logs inbound/outbound communication signals, [0094] - monitors the state of the system components).

As to claim 17, Tabe teaches the security server manages access to current and logged state data for couplings between the gateway and the security system components (para [0088], [0094]).

As to claim 18, Tabe teaches the security server manages communications with the security system components (para [0084] - distribution of security data)

As to claim 19, Tabe teaches the security server generates and transfers notifications to remote client devices, the notifications comprising event data (para [0044]).

As to claim 21 Tabe teaches the event data is event data of the security system components (para [0089] - detection events).

As to claim 22, Tabe teaches the gateway automatically controls transfer of the security data into the second controller (para [0091]).

As to claim 23, Tabe teaches the gateway automatically instructs the second controller to enter an installation mode (para [0091])

As to claim 24, Tabe teaches the gateway automatically loads the security data into the second controller when the second controller is in the installation mode (para [0091], [0186]).

As to claim 25, Tabe teaches the first controller is a control panel of the security system, the control panel controlling the security system components (para [0177] - distribution panel)

As to claim 26, Tabe teaches the second controller is a wireless control panel of the security system, the wireless control panel controlling the security system components (para [0171] - wired/wireless, [0177]).

As to claim 27, Tabe teaches the takeover component comprises a radio frequency (RF) transceiver (para [0171] - RF link).

As to claim 28 Tabe teaches the RF transceiver is compatible with the first controller (para [0171]).

As to claim 29, Tabe teaches the takeover component forms a wireless coupling with the first controller (para [0171] - wired/wireless).

As to claim 30, Tabe teaches the gateway locates and identifies wireless components of the security system components (para [0091], [0144])

As to claim 31, Tabe teaches the gateway manages the wireless components (para [0091], [0150]).

As to claim 32, Tabe teaches the gateway is a communication relay that relays the security data between the second controller and the wireless components (para [0091], [0197])

As to claim 33, Tabe teaches the security data comprises sensor identification data (para [0178] - electronic image sensors).

As to claim 34, Tabe teaches the security data comprises security system component data (para [0171]).

As to claim 35, Tabe teaches the security data comprises security system component data for each wireless component of the security system components (para [0171]).

As to claim 36, Tabe teaches the security data comprises security system component zone data for each wired component of the security system components (para [0171]).

As to claim 37, Tabe teaches the security data comprises security zone data of each zone of the first location (para [0064] - spatial locations).

As to claim 38, Tabe teaches the security data comprises security zone names of each zone of the first location (para [0064] - spatial locations, [0100] - uniquely identifies the system components and detection types)

As to claim 39, Tabe teaches the gateway is connected to a local area network at the first location, and the local area network is coupled to a wide area network via a router at the first location (para [0055], [0091]).

- Please See Continuation Sheet -

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US 08/83254

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Box V 2. Citations and explanations:

As to claim 40, Tabe teaches the gateway is coupled to a wide area network and is coupled to a local area network at the first location via the connection management component and a router at the first location (Fig. 13, para [0063], [0080], [0091]).

As to claim 41, Tabe teaches an interface coupled to the security network, wherein the interface allows control of functions of the security network by a user (para [0186] - home occupants).

As to claim 42, Tabe teaches a portal coupled to the gateway, wherein the portal provides access to communications and functions of the security network via remote client devices (para [0044], [0066], [0091]).

As to claim 43, Tabe teaches an interface coupled to the security network, wherein the interface allows control of the functions of the security network from the remote client devices (para [0044]).

As to claim 44, Tabe teaches the remote client devices include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices (para [0044]).

As to claim 45, Tabe teaches the gateway automatically discovers the security system components (para [0091], [0123] - detection).

As to claim 46, Tabe teaches the gateway includes protocols of the security system and uses the protocols to discover the security system components (para [0091], [0133]).

As to claim 47, Tabe teaches the gateway requests and receives protocols of the security system from a security server at a second location, wherein the gateway uses the protocols received to discover the security system components (para [0091], [0133], [0138]).

As to claim 48, Tabe teaches the gateway automatically establishes and controls communications with the security system components (para [0091]).

As to claim 49, Tabe teaches the gateway automatically establishes a coupling with the security system including the security system components (para [0091], [0159]).

As to claim 50, Tabe teaches the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a remote location (para [0091], [0166]).

As to claim 51, Tabe teaches the gateway transmits event data of the security system components to the central monitoring station over the secondary communication link (para [0054], [0091], [0166]).

As to claim 52, Tabe teaches the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components (Fig 3, para [0061] - exchange signals).

As to claim 53, Tabe teaches the secondary communication link includes a broadband coupling (para [0084]).

As to claim 54, Tabe teaches the secondary communication link includes a General Packet Radio Service (GPRS) coupling (para [0054]).

As to claim 55, Tabe teaches the gateway transmits messages comprising event data of the security system components to remote client devices over the secondary communication link (para [0044], [0091]).

As to claim 56 Tabe teaches the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components (Fig 3, para [0061]).

As to claim 57, Tabe teaches the gateway receives control data for control of the security system components from remote client devices via the secondary communication link (para [0044], [0091]).

As to claim 58 Tabe teaches the security network comprises network devices coupled to the gateway via a wireless coupling (para [0054], [0091]).

As to claim 59, Tabe teaches the gateway automatically discovers the network devices. (para [0089] - detection, [0091]).

As to claim 60, Tabe teaches the gateway automatically installs the network devices in the security network (para [0091], [0186]).

- Please See Continuation Sheet -

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US 08/83254

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Box V.2. Citations and explanations:

As to claim 61, Tab e teaches the gateway automatically configures the network devices for operation in the security network (para [0091], [0151]).

As to claim 62, Tab e teaches the gateway controls communications between the network devices, the security system components, and the security server (para [0091]).

As to claim 63 Tab e teaches the gateway transmits event data of the network devices to remote client devices over at least one of a plurality of communication links (para [0044]).

As to claim 64, Tab e teaches the gateway receives control data for control of the network devices from remote client devices via at least one of the plurality of communication links (para [0044]).

As to claim 65, Tab e teaches the event data comprises changes in device states of the network devices, data of the network devices, and data received by the network devices (para [0089] - detection events)

As to claim 66, Tab e teaches the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link (para [0091])

As to claim 67 Tab e teaches the gateway transmits event data of the network devices to the central monitoring station over the secondary communication link (para [0091])

As to claim 68, Tab e teaches the network device is an Internet Protocol device (para [0085]).

As to claim 69 Tab e teaches the network device is a camera (para [0178])

As to claim 70, Tab e teaches the network device is a touchscreen (para [0065]).

As to claim 71, Tab e teaches the network device is a device controller that controls an attached device (para [0163]).

As to claim 72, Tab e teaches the network device is a sensor (para [0178]).

As to claim 73, Tab e teaches the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers (para [0178]).

As to claim 74, Tab e teaches a system comprising: a gateway located at a first location (para [0091]); a takeover component coupled to the gateway, the takeover component establishing a wireless coupling with a first controller of a security system installed at the first location, the takeover component automatically extracting security data of the security system from the first controller, the security system including security system components coupled to the first controller (para [0171]); wherein the gateway uses the security data extracted from the controller to automatically form a security network by transferring the security data to a second controller, wherein the second controller is coupled to the security system components and replaces the first controller (para [0123] - detection)

As to claim 75, Tab e teaches a system comprising a gateway located at a first location, the gateway including a takeover component that establishes a wireless coupling with a first controller of a security system installed at the first location, the takeover component automatically extracting security data of the security system from the first controller, the security system including security system components coupled to the first controller, wherein the gateway uses the security data extracted from the controller to automatically form a security network by transferring the security data to a second controller, wherein the second controller is coupled to the security system components and replaces the first controller (para [0091], [0171]).

As to claim 76, Tab e teaches a system comprising: a gateway located at a first location (para [0091]); a takeover component coupled to the gateway, the takeover component establishing a wireless coupling with a first controller of a security system installed at the first location, the takeover component automatically extracting security data of the security system from the first controller, the security system including security system components coupled to the first controller, wherein the gateway uses the security data extracted from the controller to automatically form a security network by transferring the security data to a second controller, wherein the second controller is coupled to the security system components and replaces the first controller (para [0171]); and a security server at a second location different from the first location, wherein the security server is coupled to the gateway. (para [0199]).

As to claim 77 Tab e teaches a system comprising: a gateway located at a first location (para [0091]); and a takeover component coupled to the gateway, the takeover component establishing a wireless coupling with a first controller of a security system installed at the first location, the security system including security system components coupled to the first controller (para [0171]); the takeover component automatically extracting security data of the security system from the first controller (para [0171]); the takeover component automatically transferring the security data extracted from the first controller to a second controller, wherein the second controller is coupled to the security system components and replaces the first controller (para [0171]).

- Please See Continuation Sheet -

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US 08/83254

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:  
Box V.2 Citations and explanations:

As to claim 78, Tabe teaches a system comprising a gateway located at a first location, the gateway including a takeover component that establishes a coupling with a first controller of a security system installed at the first location, the security system including security system components coupled to the first controller, wherein the takeover component automatically extracts security data of the security system from the first controller via the coupling, wherein the gateway automatically transfers the security data extracted from the controller to a second controller, wherein the second controller is coupled to the security system components and replaces the first controller (para [0091], [0171]).

As to claim 79, Tabe teaches a system comprising: a gateway located at a first location (para [0091]); and a takeover component coupled to the gateway, the takeover component establishing a wireless coupling with a first controller of a security system installed at the first location, the security system including security system components coupled to the first controller, wherein the takeover component automatically extracts security data of the security system from the first controller, wherein the takeover component automatically transfers the security data extracted from the controller to a second controller, wherein the second controller is coupled to the security system components and replaces the first controller (para [0171]); and a security server at a second location different from the first location, wherein the security server is coupled to the gateway and stores the security data received from the takeover component (para [0171]).

As to claim 80, Tabe teaches a device comprising a takeover component running under a processor, the takeover component establishing a wireless coupling with a first controller of a security system installed at the first location, the security system including security system components coupled to the first controller, wherein the takeover component automatically extracts security data of the security system from the first controller via the coupling, wherein the takeover component automatically transfers the security data extracted from the controller to a second controller, wherein the second controller is coupled to the security system components and replaces the first controller (para [0171]).

Claim 20 lacks an inventive step under PCT Article 33(3) as being obvious over Tabe in view of US 2006/0111095 A1 (Weigand)

As to claim 20 Tabe teaches the system of claim 19, but fails to explicitly teach wherein the notifications include one or more of short message service messages and electronic mail messages. However, Weigand does teach wherein the notifications include one or more of short message service messages and electronic mail messages (para [0019]). It would have been obvious to one of ordinary skill in the art to combine the entertainment device configured for interactive detection and security vigilant monitoring in communication with a control server of Tabe with the dynamically distributed, portal-based application services network topology for cellular systems of Weigand, because Tabe and Weigand are directed to systems and methods for security systems. Furthermore, users and designers benefit from systems and methods adapted for operating with GSM networks, Short Message Service or Circuit-Switched Data bearer services may be used. In addition, mobile stations may establish packet-switched connections to an application server using General Packet Radio Services bearer services, because such systems/methods allow for facilitating configuration and implementation of application services that are customized or otherwise tailored for each wireless carrier (Weigand, para [0011]).

Claims 1-80 have industrial applicability as defined by PCT Article 33(4) because the subject matter can be made or used in industry.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	6271985
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	53186
<b>Filer:</b>	Richard L. Gregory/Rob Rathbun
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	15-OCT-2009
<b>Filing Date:</b>	12-AUG-2008
<b>Time Stamp:</b>	17:45:07
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		IDS_ICONP001D3_Oct152009.pdf	651756 <small>5eb8671c6837d69ce2496a820ac06a2084d57cd2</small>	yes	7

Multipart Description/PDF files in .zip description			
	Document Description	Start	End
	Miscellaneous Incoming Letter	1	1
	Transmittal Letter	2	3
	Information Disclosure Statement (IDS) Filed (SB/08)	4	7

**Warnings:**

**Information:**

2	NPL Documents	Form_PCTISA220_IJCONP001W O.pdf	160649 500efb126d8f0cf7c85c59cbb405ddbc6c569ff0	no	1
---	---------------	------------------------------------	--	----	---

**Warnings:**

**Information:**

3	NPL Documents	Form_PCTISA210_IJCONP001W O.pdf	236326 9aba62eb40ca218988cf0f4e10b2819dfb80f821	no	2
---	---------------	------------------------------------	--	----	---

**Warnings:**

**Information:**

4	NPL Documents	Form_PCTISA237_IJCONP001W O.pdf	885936 30803517bf06ae9dcba1f60e8ae86df3cac5a2c	no	6
---	---------------	------------------------------------	---	----	---

**Warnings:**

**Information:**

5	NPL Documents	Form_PCTISA220_IJCONP002W O.pdf	158279 ba39a7275d98b3ede1f3f182c69d26c49e7ea431	no	1
---	---------------	------------------------------------	--	----	---

**Warnings:**

**Information:**

6	NPL Documents	Form_PCTISA210_IJCONP002W O.pdf	228940 6005e690b0bbe28bdaf0259ef3d09ab5f32e1d4c	no	2
---	---------------	------------------------------------	--	----	---

**Warnings:**

**Information:**

7	NPL Documents	Form_PCTISA237_IJCONP002W O.pdf	1019984 d8757b37e2c74886b9badd28d8e3f63946eac6a7	no	6
---	---------------	------------------------------------	---	----	---

**Warnings:**

**Information:**

8	NPL Documents	Form_PCTISA220_IJCONP003W O.pdf	151560 1379045b674f45a3450408cb146808db39149b19	no	1
---	---------------	------------------------------------	--	----	---

**Warnings:**



Information:					
9	NPL Documents	Form_PCTISA210_ICONP003W O.pdf	212376 71d0bf19c4851876dde5f235e5ba0577dd3 0c112	no	2
Warnings:					
Information:					
10	NPL Documents	Form_PCTISA237_ICONP003W O.pdf	694605 8fff18b46e66bc8f1b9d781d2e542c8438b2 fcad	no	6
Warnings:					
Information:					
11	NPL Documents	Form_PCTISA220_ICONP005W O.pdf	145314 362375f21590420c047d6eefbb9c49930199 26823	no	1
Warnings:					
Information:					
12	NPL Documents	Form_PCTISA210_ICONP005W O.pdf	209787 05f3ae04d5e61ceeb09c29855b3e23cb00a 8ecad	no	2
Warnings:					
Information:					
13	NPL Documents	Form_PCTISA237_ICONP005W O.pdf	798796 863b2f36e8975bd3ad949ea4b4351e9686c c8fcf	no	7
Warnings:					
Information:					
<b>Total Files Size (in bytes):</b>			5554308		
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					

Attorney Docket No. ICON.P001D3

Patent

**Transmittal of Information Disclosure Statement**

*Certification Under 37 C.F.R. §1.8(a)*

Transmitted via


**October 15, 2009**

Date of Transmission

**USPTO EFS**

I hereby certify that this document, and any other accompanying documents referred to herein are being transmitted to the United States Patent Office via EFS in accordance with 37 C.F.R. §1.6(a)(4) on the date indicated above.

***Rob Rathbun***



\_\_\_\_\_  
(Print Name of Person Transmitting Documents)

\_\_\_\_\_  
(Signature of Person Transmitting Documents)

Submission of Information Disclosure Statement;  
Substitute Form 1449/PTO;  
Twelve (12) Non Patent Literature Documents.

**IN THE UNITED STATES PATENT OFFICE**

In Re Patent Application of:	)		
	)	Examiner:	Not Assigned
First Named Inventor: Marc Baum	)	Art Unit:	2442
	)		
Application No. 12/189,788	)		
	)		
Filed: August 12, 2008	)		
	)		
For: FORMING A SECURITY NETWORK INCLUDING	)		
INTEGRATED SECURITY SYSTEM	)		
<u>COMPONENTS AND NETWORK DEVICES</u>	)		

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Submission of Information Disclosure Statement**

Sir:

Enclosed is a copy of Information Disclosure Citation Form PTO-1449 (Substitute). Copies of any references that are not U.S. Patents or U.S. Patent Publications are also enclosed. It is respectfully requested that the cited documents be considered and that the enclosed Information Disclosure Citation Form PTO-1449 be initialed by the Examiner to indicate such consideration and a copy thereof returned to applicant(s).

This Information Disclosure Statement is being submitted pursuant to 37 C.F.R. § 1.97(b), and no fee should be due for this submission.

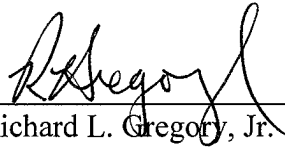
Pursuant to 37 C.F.R. § 1.97(h), the submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability.

Attorney Docket No. ICON.P001D3  
Application No. 12/189,788

**Authorization to Charge Deposit Account**

Please charge our deposit account number 503616 (Attorney Docket Number  
ICON.P001D3) for any fees that may be due for this submission.

Respectfully submitted,  
Courtney Staniford & Gregory LLP



Richard L. Gregory, Jr.  
Reg. No. 42,607

Dated: September 22, 2009

Courtney Staniford & Gregory LLP  
10001 N. De Anza Blvd. Suite 300  
Cupertino, CA 95014  
Telephone No.: (408) 342-1900  
Facsimile No.: (408) 342-1909



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 4 columns: APPLICATION NUMBER (12/189,788), FILING OR 371(C) DATE (08/12/2008), FIRST NAMED APPLICANT (Marc Baum), ATTY. DOCKET NO./TITLE (ICON.P001D3)

CONFIRMATION NO. 7650

PUBLICATION NOTICE

53186
COURTNEY STANIFORD & GREGORY LLP
P.O. BOX 9686
SAN JOSE, CA 95157



Title:Forming A Security Network Including Integrated Security System Components and Network Devices

Publication No.US-2009-0077624-A1
Publication Date:03/19/2009

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 4 columns: APPLICATION NUMBER (12/189,788), FILING OR 371(C) DATE (08/12/2008), FIRST NAMED APPLICANT (Marc Baum), ATTY. DOCKET NO./TITLE (ICON.P001D3)

CONFIRMATION NO. 7650

NEW OR REVISED PPD NOTICE

53186
COURTNEY STANIFORD & GREGORY LLP
P.O. BOX 9686
SAN JOSE, CA 95157



NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 03/19/2009. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Data Management, Application Assistance Unit at (571) 272-4000, or (571) 272-4200, or 1-888-786-0101.

Clear

DEPARTMENT OF DEFENSE  
ACCESS ACKNOWLEDGEMENT / SECRECY ORDER RECOMMENDATION  
FOR PATENT APPLICATION

Application Serial No: DP12189788

Filing Date:

Date Referred: 09/03/2008

I hereby acknowledge that the Department of Defense reviewers has inspected this application in administration of 35 USC 181 on behalf of the Agencies/Commands specified below. DoD reviewers will not divulge any information from this application for any purpose other than administration of 35 USC 181.

Defense Agency	Recommendation	Reviewer Name	Date Reviewed
Army	Secrecy Not Recommended	Herbert Rose	11/20/2008
NSA	Secrecy Not Recommended	Robert Morelli	09/19/2008

<p><i>Type of Recommendations:</i></p> <p><i>SNR: Secrecy Not Recommended</i></p> <p><i>SR: Secrecy Recommended</i></p> <p><i>NC: No Comment</i></p>
--

**Instructions to Reviewers:**

1. All DoD personnel reviewing this application will be listed on this form regardless of whether they are making a secrecy order recommendation.
2. This form will be forwarded to USPTO once all assigned DoD entities have provided their secrecy order recommendation.

**Time for Completion of Review:**

Pursuant to 35 USC 184, the subject matter of this application may be filed in a foreign country for the purpose of filing a patent application without a license anytime after the expiration of six (6) months from filing date unless the application becomes the subject of a secrecy order.

<p><i>The USPTO publishes patent application at 18 months from the earliest claimed filing date. The USPTO will delay the publication of a patent application made available to a defense agency under 35 USC 181 until no earlier than 6 months from the filing date or 90 days from the date of referral to that agency. This application will be cleared for publication 6 months from the filing date or 90 days from the above Date Referred, whichever is later, unless a response is provided to the USPTO regarding the necessary recommendations as to the imposition of a secrecy order.</i></p>
--

**DoD Completion of Review: Final**

Forwarded to USPTO: 12/02/2008 By: Oksana Nesterczuk



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY. DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 12/189,788, 08/12/2008, 2161, 1380, ICON.P001D3, 51, 4

CONFIRMATION NO. 7650

UPDATED FILING RECEIPT

53186
COURTNEY STANIFORD & GREGORY LLP
P.O. BOX 9686
SAN JOSE, CA 95157



Date Mailed: 12/03/2008

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

- Marc Baum, San Jose, CA;
Paul J. Dawes, Woodside, CA;
Mike Kinney, Foster city, CA;
Reza Raji, Menlo Park, CA;
David Swenson, Glyndon, MN;
Aaron Wood, Boulder Creek, CA;

Power of Attorney: The patent practitioners associated with Customer Number 53186

Domestic Priority data as claimed by applicant

This application is a DIV of 12/189,757 08/11/2008 which claims benefit of 60/968,005 08/24/2007 and claims benefit of 60/987,359 11/12/2007 and claims benefit of 60/987,366 11/12/2007 and claims benefit of 61/019,162 01/04/2008 and claims benefit of 61/019,167 01/04/2008 and claims benefit of 61/023,489 01/25/2008 and claims benefit of 61/023,493 01/25/2008 and claims benefit of 61/023,496 01/25/2008 and claims benefit of 61/087,967 08/11/2008 and is a CIP of 11/084,232 03/16/2005 and is a CIP of 11/761,718 06/12/2007 and is a CIP of 11/761,745 06/12/2007 and is a CIP of 12/019,554 01/24/2008 and is a CIP of 12/019,568 01/24/2008

Foreign Applications



**Projected Publication Date:** To Be Determined - pending completion of Security Review

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

Forming A Security Network Including Integrated Security System Components and Network Devices

**Preliminary Class**

707

## **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

**IN THE UNITED STATES PATENT OFFICE**

In Re Patent Application of:	)	
	)	
First Named Inventor: Marc Baum	)	Examiner: Not assigned
	)	
Application No. 12/189,788	)	Art Unit: 2161
	)	
Filed: August 12, 2008	)	
	)	
For: FORMING A SECURITY NETWORK	)	
INCLUDING INTEGRATED SECURITY	)	
SYSTEM COMPONENTS AND NETWORK	)	
DEVICES	)	

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**PRELIMINARY AMENDMENT**

Sir:

Please enter the following amendments before examination of this application.

**IN THE SPECIFICATION**

Please amend the inventorship of the application to be the following:

Marc Baum

Paul J. Dawes

Mike Kinney

Reza Raji

David Swenson

Aaron Wood

Please amend page 2, lines 5 and 6 to be the following:

This application ~~claims the benefit~~ is a divisional application of United States (US) Patent Application Number ~~60/955,172~~12/189,757, filed ~~August 10, 2007~~August 11, 2008.

**IN THE DRAWINGS**

Please amend the drawings as follows.

Please replace sheets 1-13 of the drawings with the replacement sheets enclosed herewith.

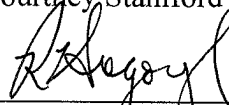
**REMARKS**

Applicants respectfully request entry of the foregoing amendments before examination of the application. Applicants state that no new matter is added by the replacement drawings.

**Authorization to Charge Deposit Account**

The Commissioner is authorized to charge any additional fees which may be required in connection with this Preliminary Amendment, including petition fees and extension of time fees, to Deposit Account Number 503616 (Attorney Docket Number ICON.P001D3).

Respectfully submitted,  
Courtney Staniford & Gregory & LLP



Richard L. Gregory, Jr.  
Reg. No. 42,607

Date: November 24, 2008

Customer Number 53186  
P.O. Box 9686  
San Jose, CA 95157  
Tel: 408-342-1900  
Fax: 408-342-1909

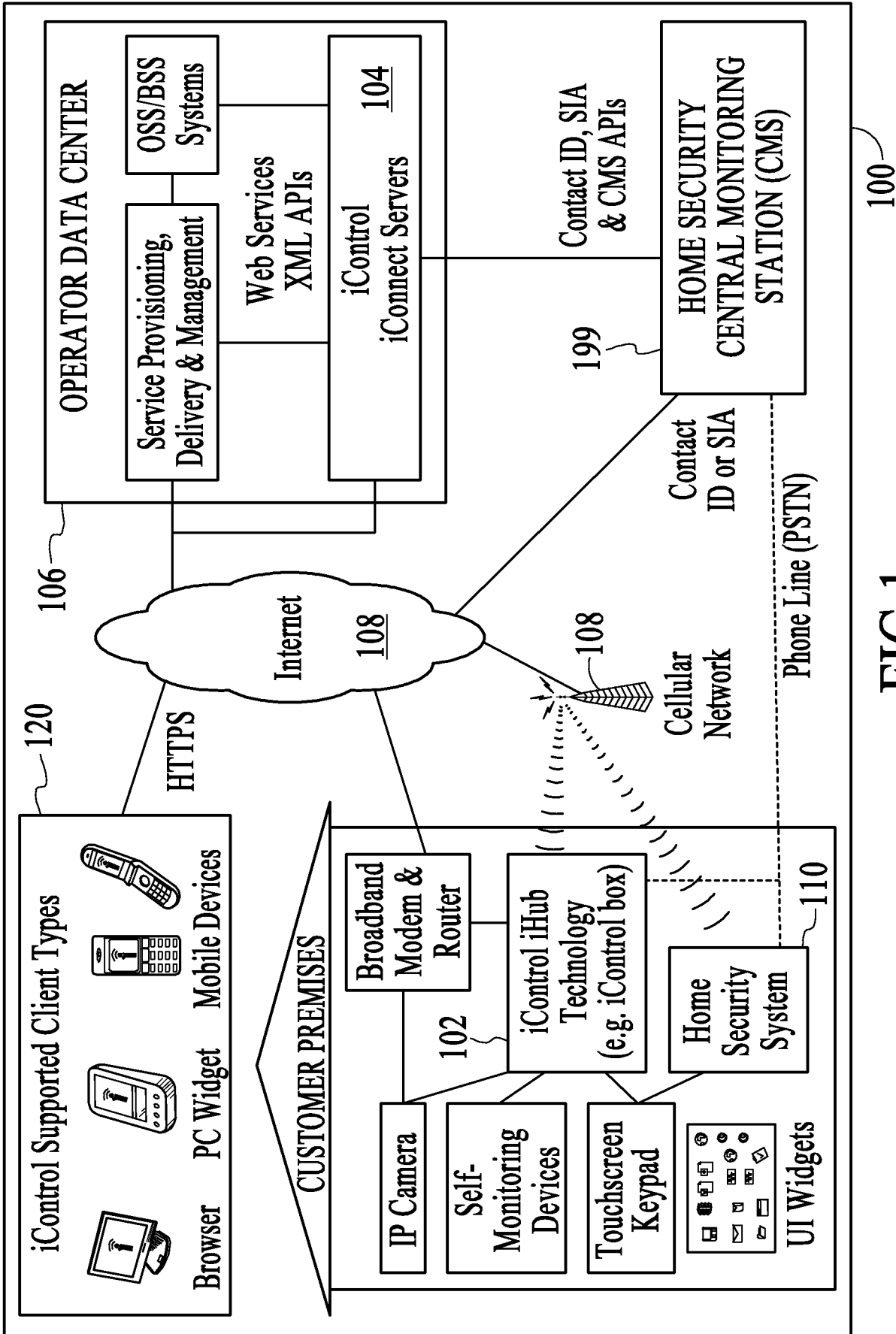


FIG. 1

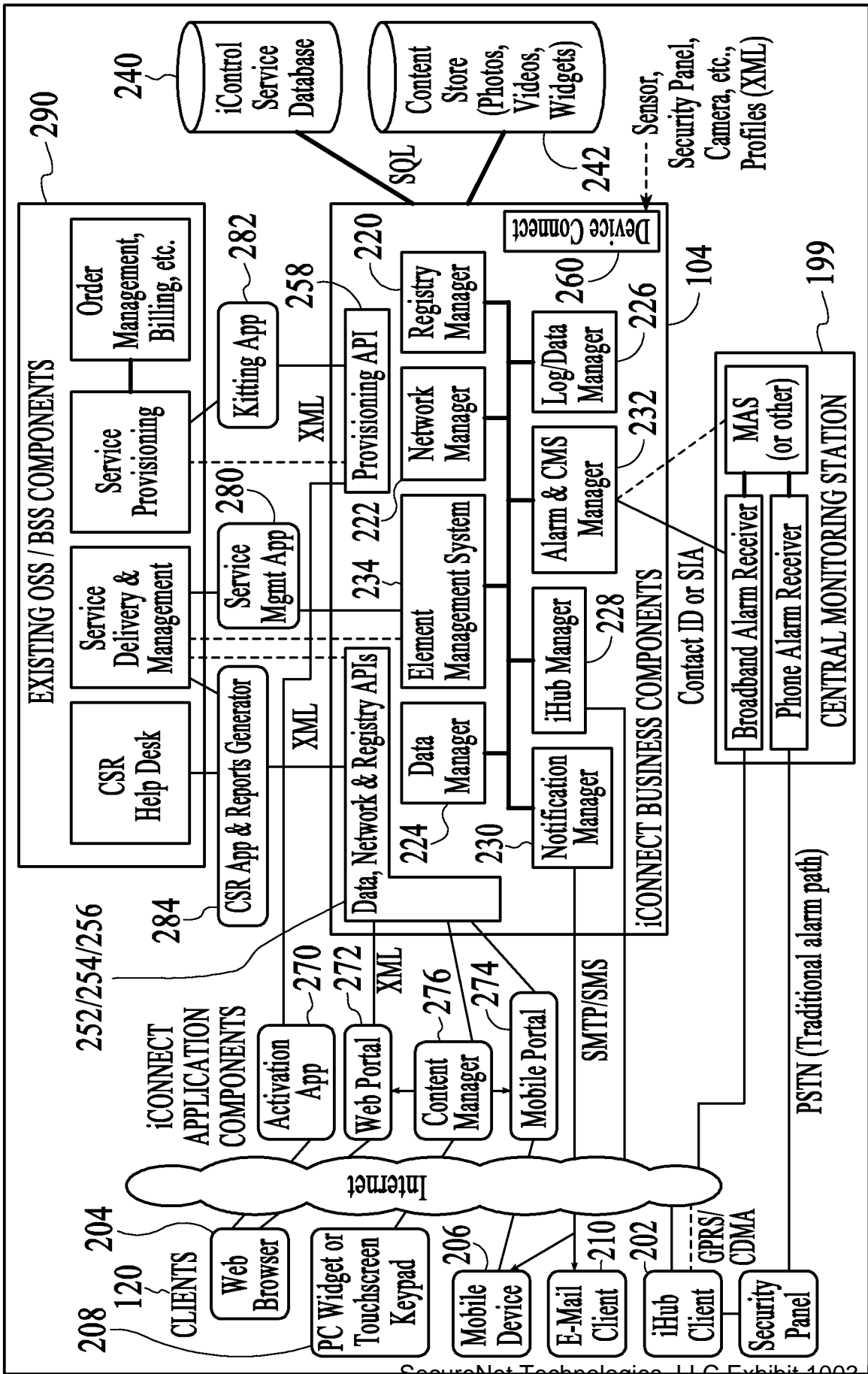


FIG.2



102

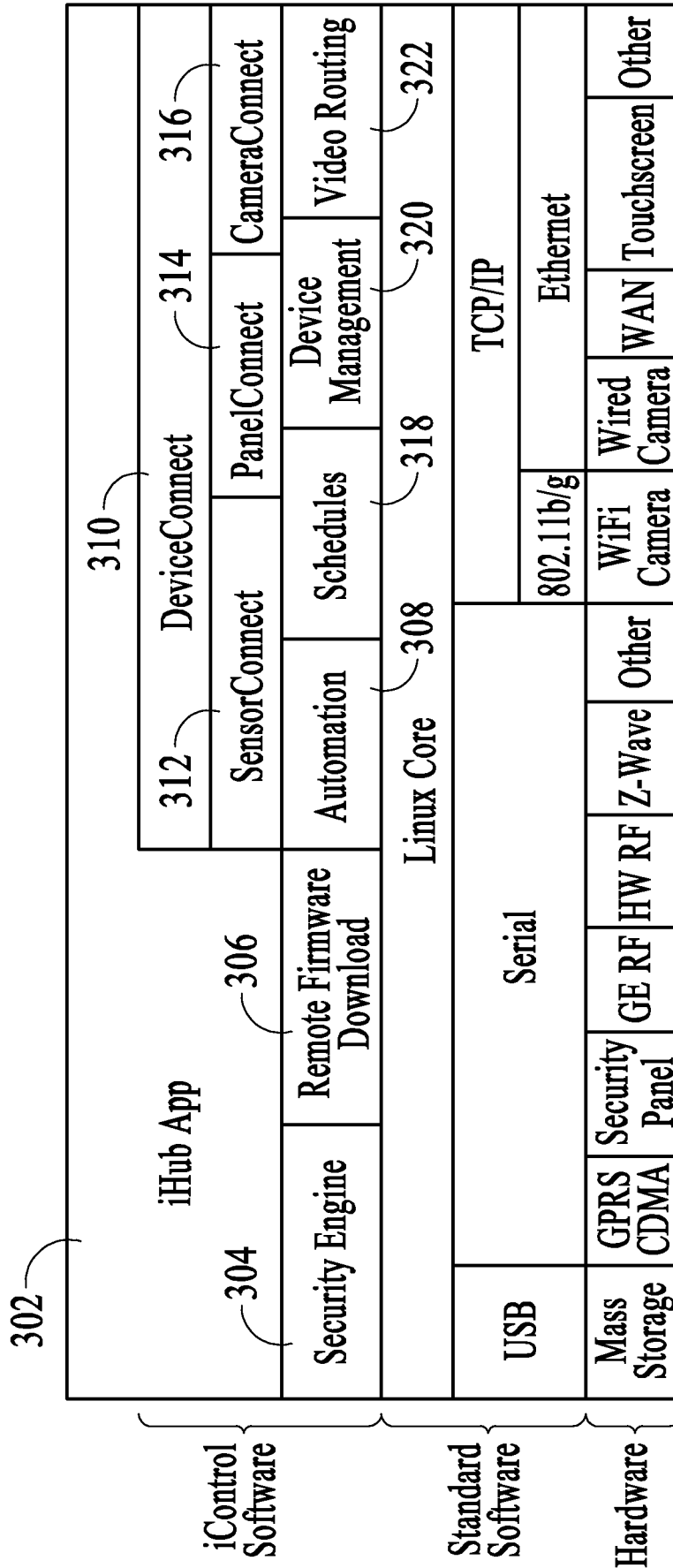


FIG.3

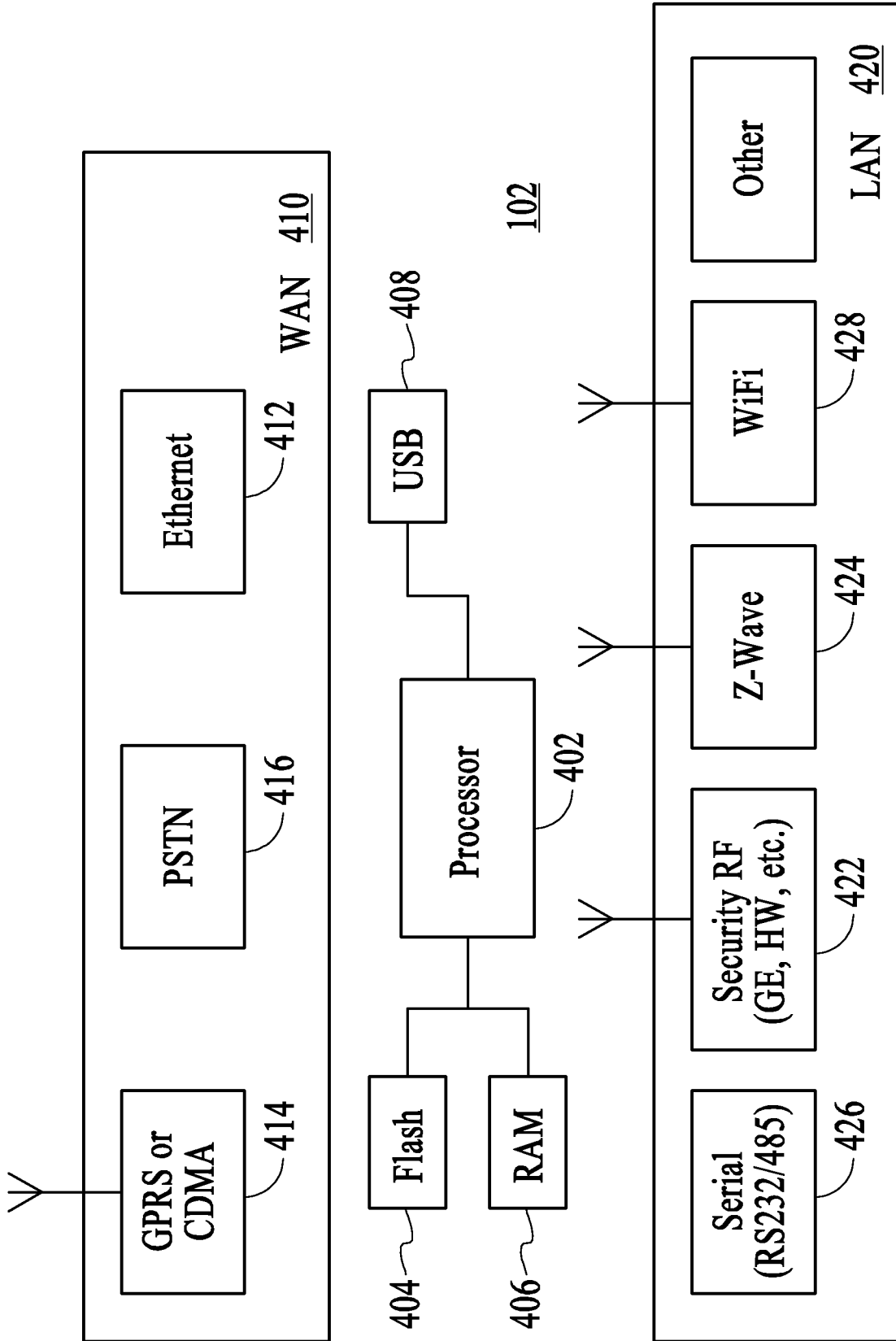


FIG.4

**FIG. 5**  
500

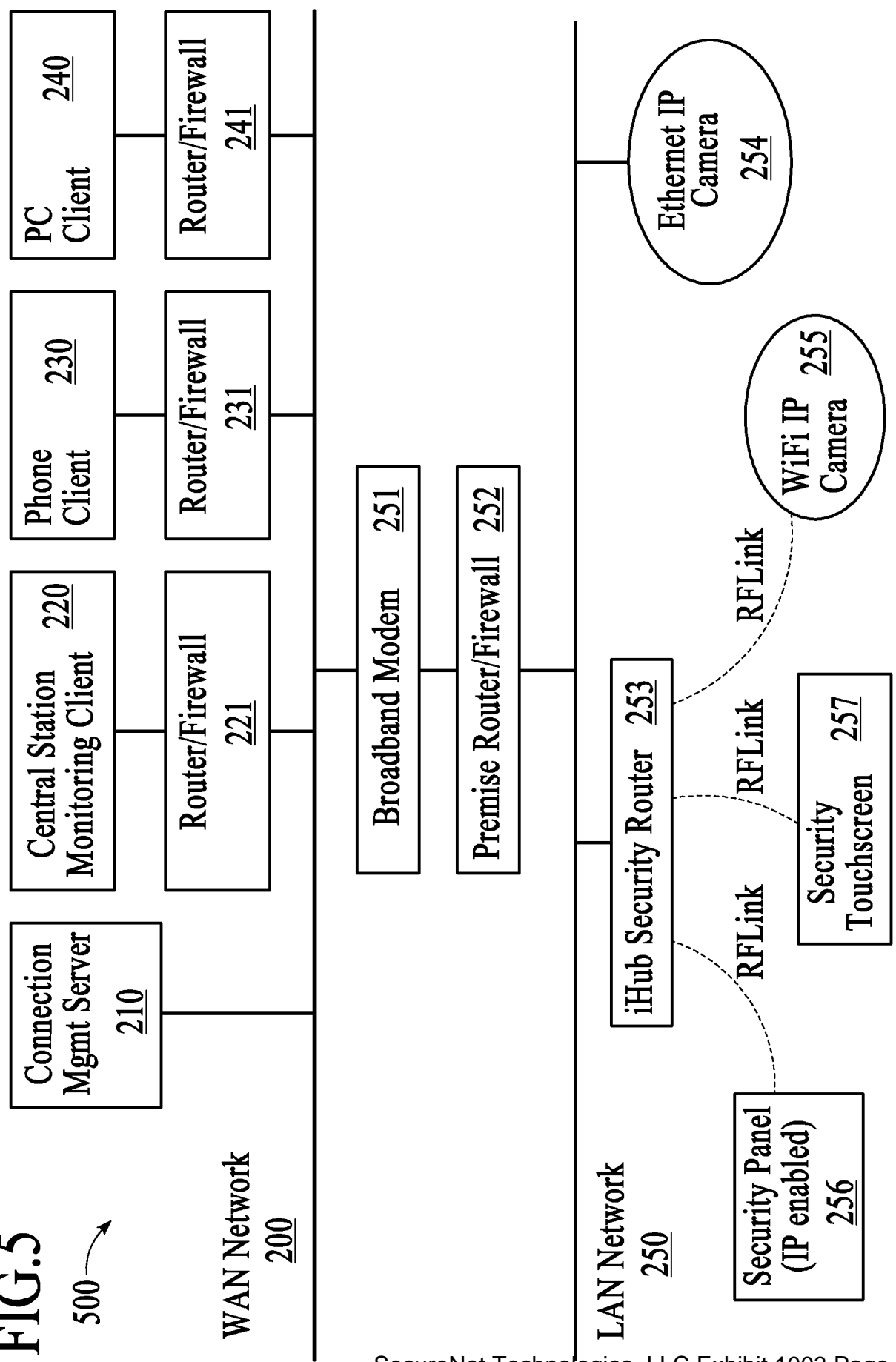
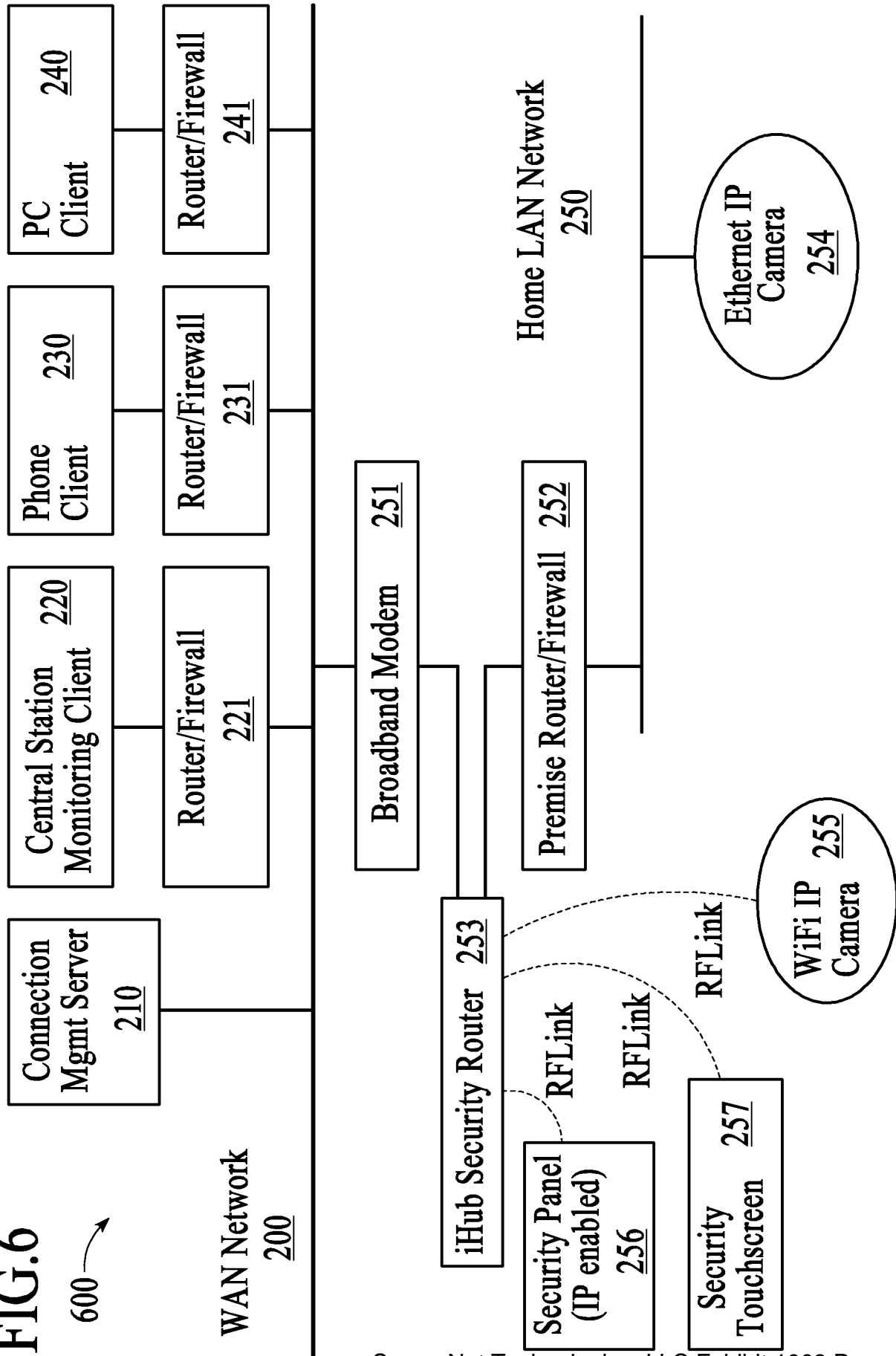


FIG. 6

600



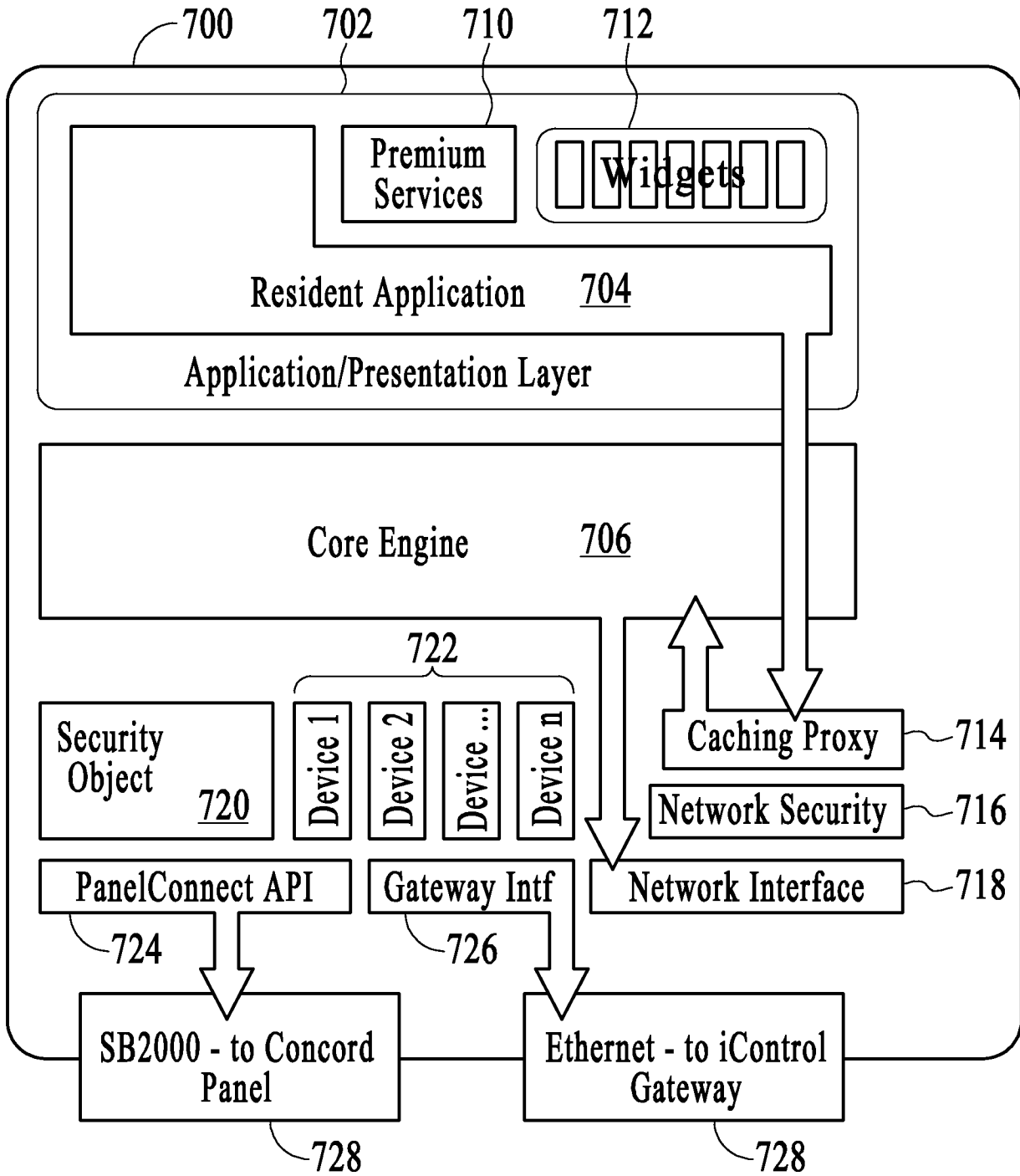
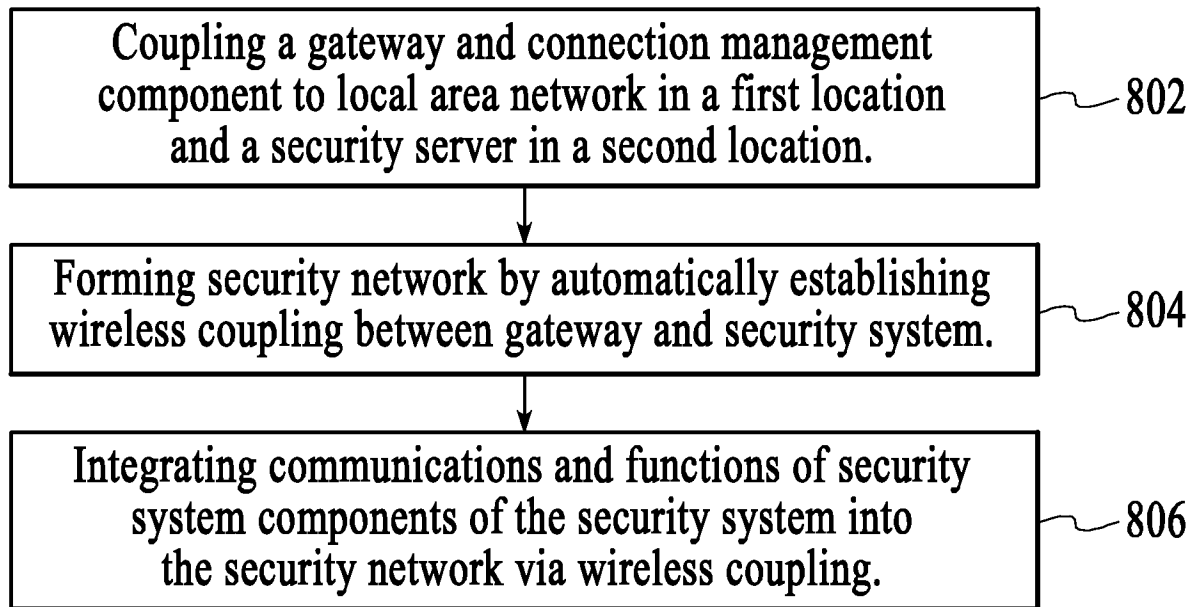
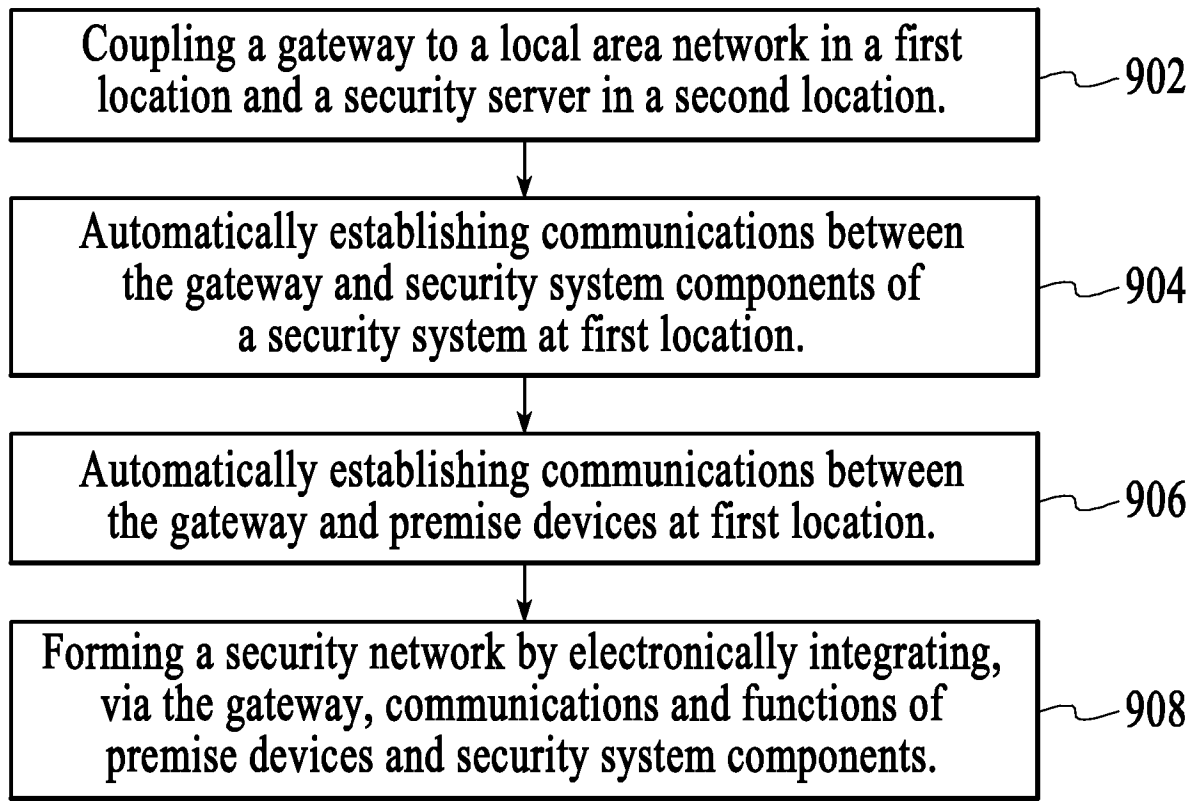


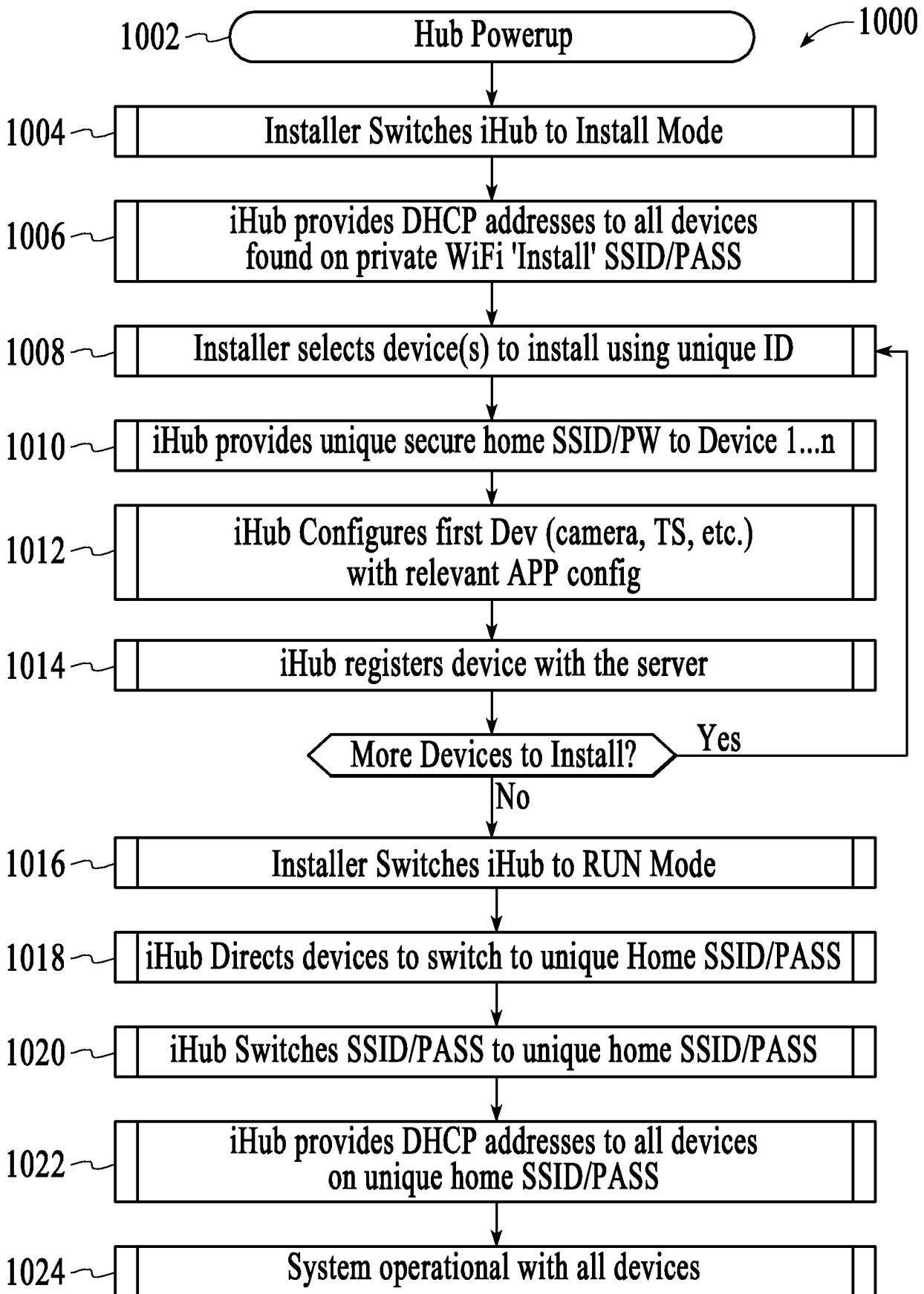
FIG. 7



**FIG.8** 800



**FIG.9** 900



**FIG. 10**

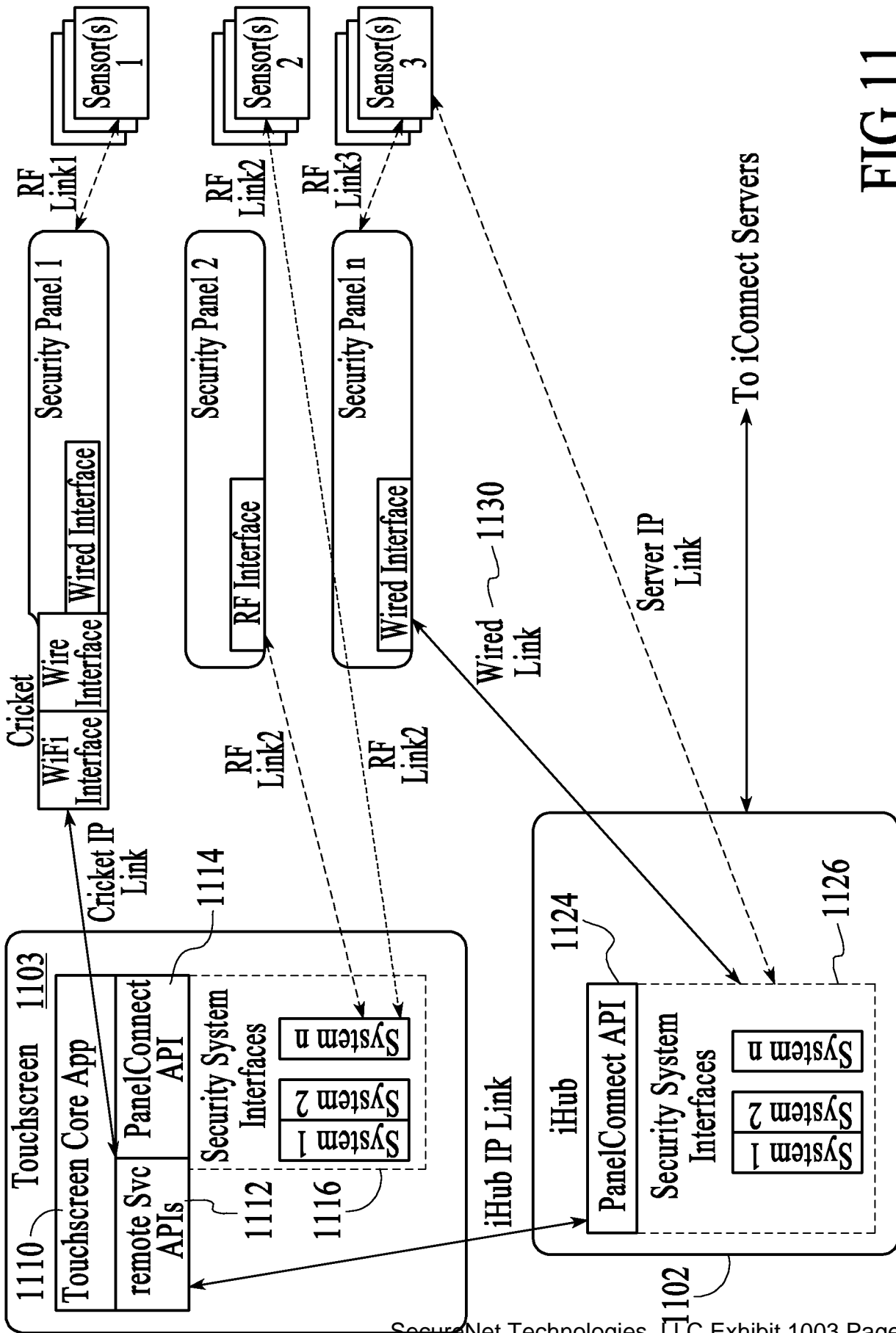


FIG.11



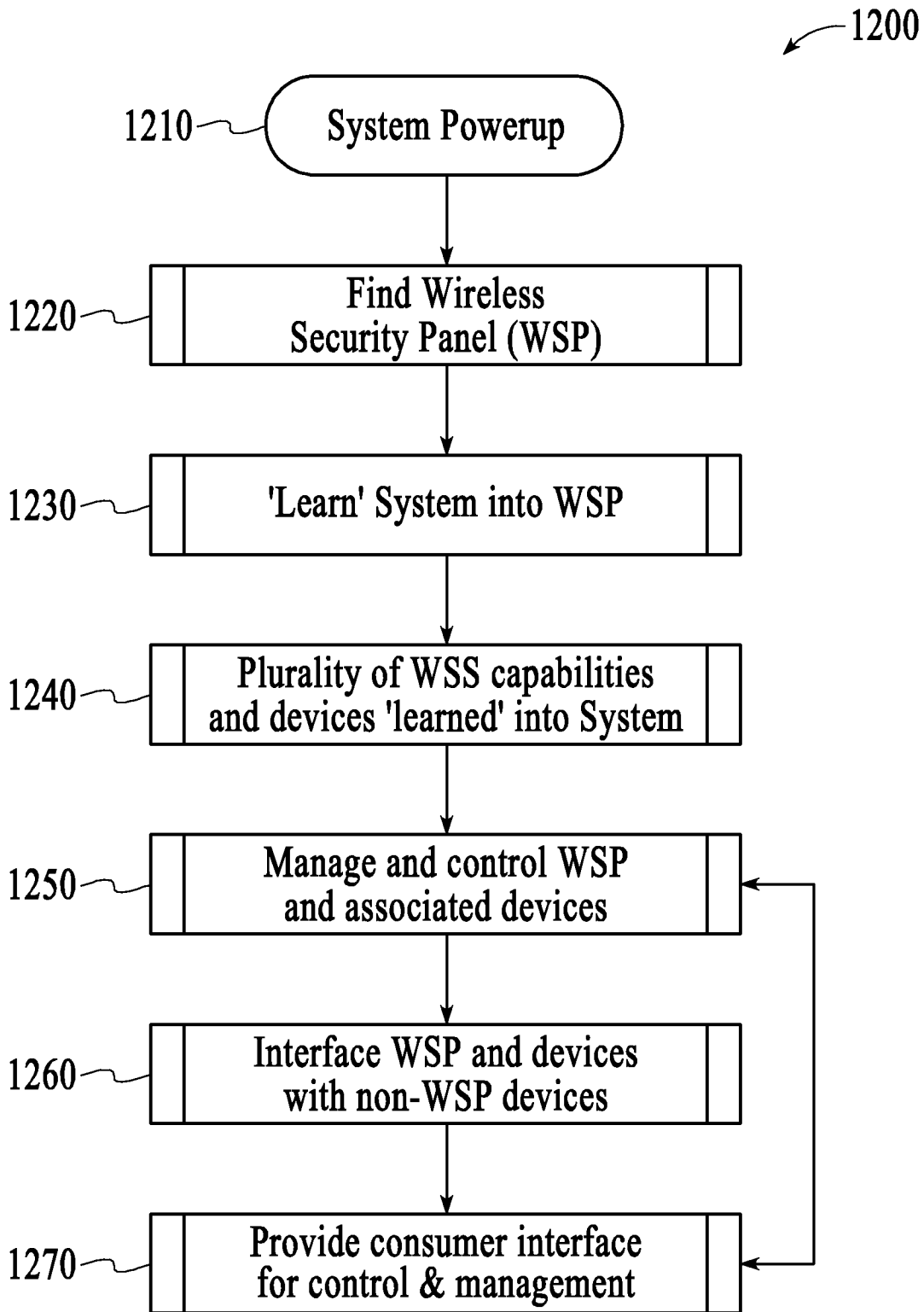


FIG.12

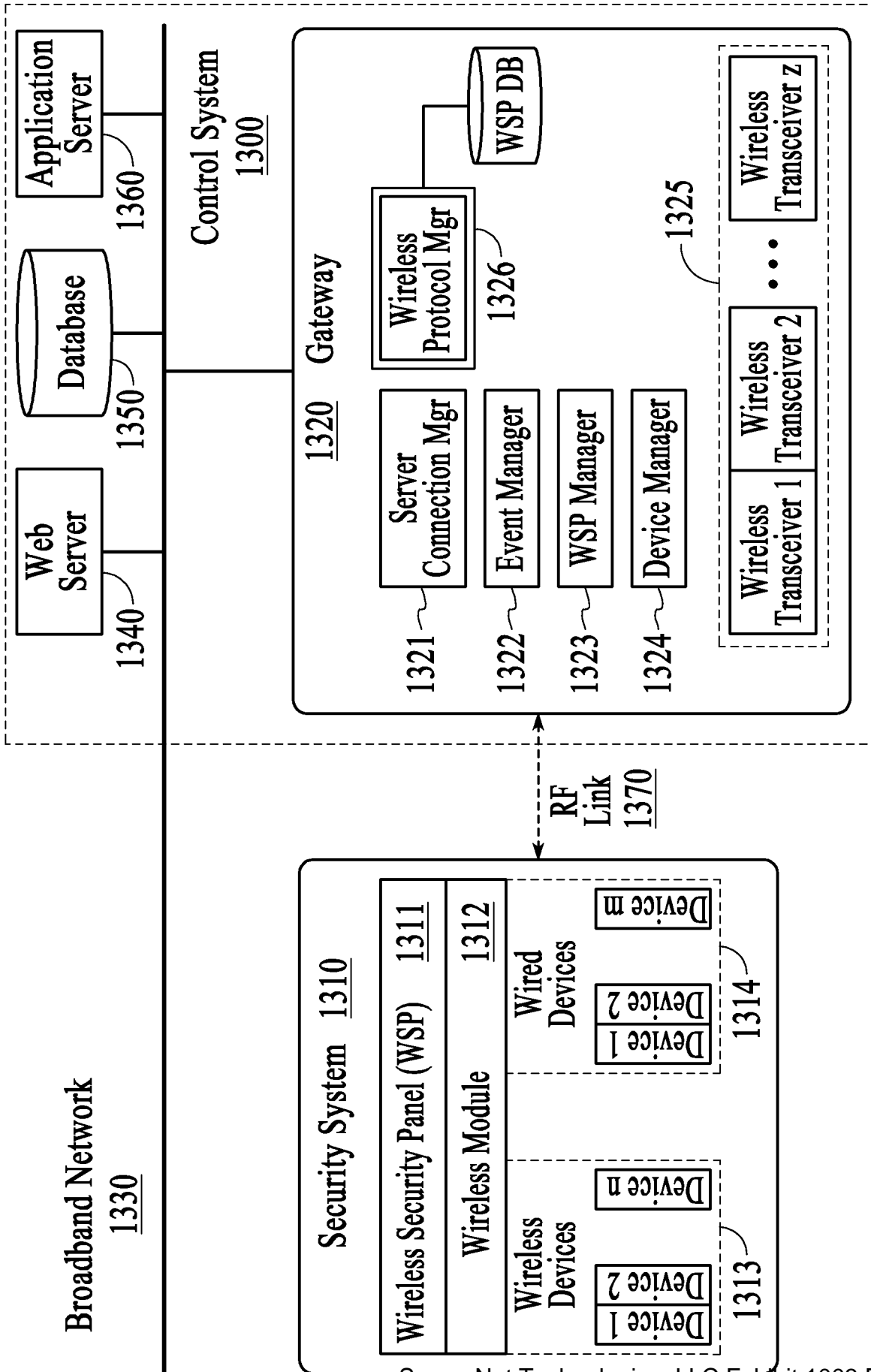


FIG.13

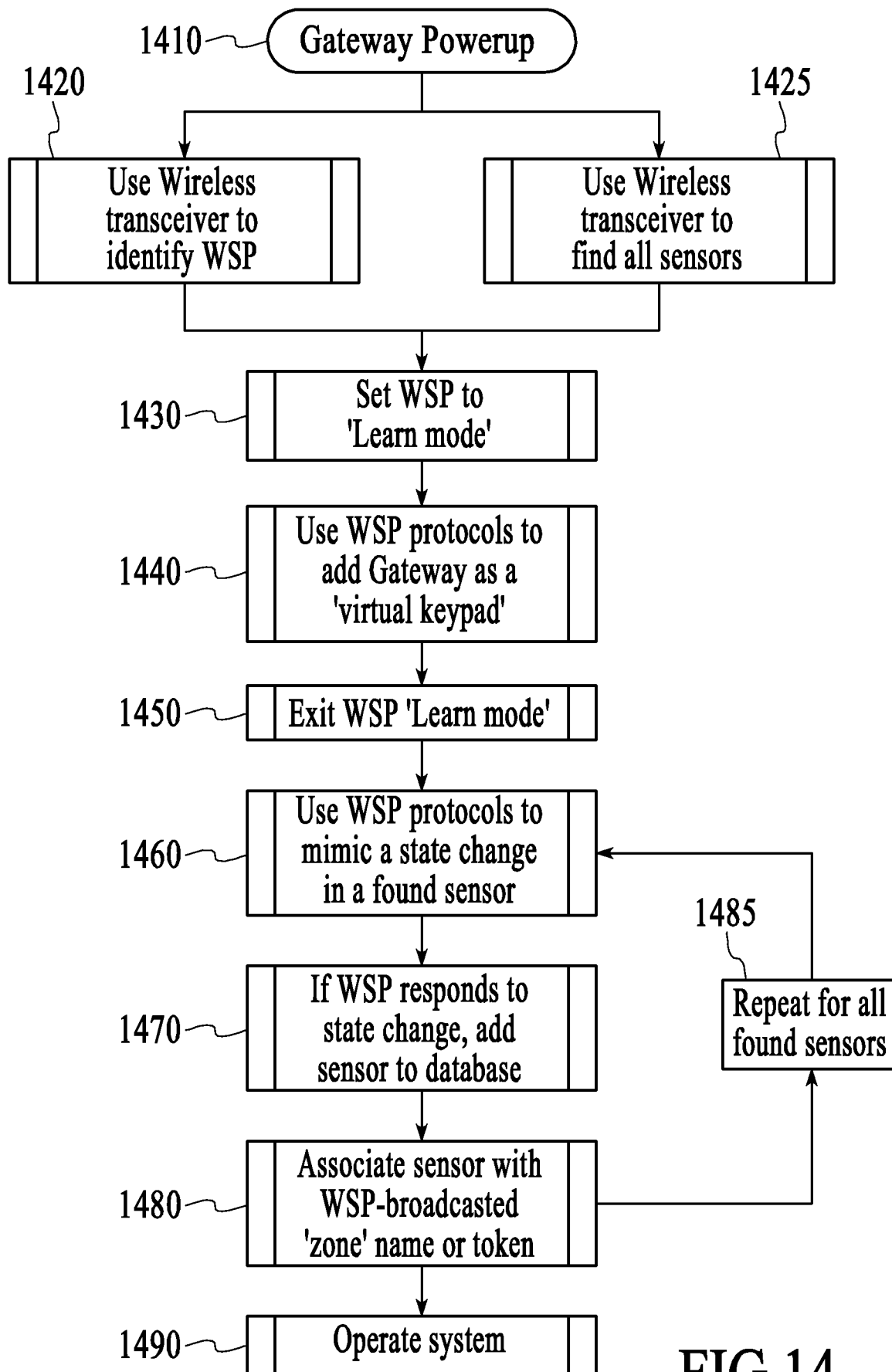


FIG. 14

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12189788
<b>Filing Date:</b>	12-Aug-2008
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Filer:</b>	Richard L. Gregory/Jerry Donnard
<b>Attorney Docket Number:</b>	ICON.P001D3

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
Late filing fee for oath or declaration	2051	1	65	65

**Petition:**

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

**Extension-of-Time:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>65</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	4347916
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	53186
<b>Filer:</b>	Richard L. Gregory/Jerry Donnard
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	24-NOV-2008
<b>Filing Date:</b>	12-AUG-2008
<b>Time Stamp:</b>	20:02:59
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$65
RAM confirmation Number	6660
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part / zip	Pages (if appl.)
SecureNet Technologies, LLC Exhibit 1003 Page 910					

1		Missing_Parts_ICONP001D3.pdf	539440 e8c1b2d30760751d86a936cf0a7de66ef97a87bd	yes	10
<b>Multipart Description/PDF files in .zip description</b>					
		<b>Document Description</b>	<b>Start</b>	<b>End</b>	
		Miscellaneous Incoming Letter	1	2	
		Oath or Declaration filed	3	6	
		Preliminary Amendment	7	10	
<b>Warnings:</b>					
<b>Information:</b>					
2	Drawings-only black and white line drawings	Replacement_Drawings_ICONP001D3.pdf	1386552 8419702801fb4987cceb954f4c0b9f27e92e00ae	no	13
<b>Warnings:</b>					
<b>Information:</b>					
3	Fee Worksheet (PTO-06)	fee-info.pdf	30376 2e66fa02068aacdf6be7b02f4d7f248f8b687a8d	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			1956368		
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

**Transmittal of Documents**

*Certification Under 37 C.F.R. §1.8(a)*

Transmitted via

**November 24, 2008**

Date of Transmission

**USPTO EFS**

I hereby certify that this document, and any other accompanying documents referred to herein are being transmitted to the United States Patent Office via EFS in accordance with 37 C.F.R. §1.6(a)(4) on the date indicated above.

***Jerry Donnard***

\_\_\_\_\_  
(Print Name of Person Transmitting Documents)

  
\_\_\_\_\_  
(Signature of Person Transmitting Documents)

Response to Notice to File Missing Parts of Nonprovisional Application;  
Declaration in Compliance with 37 CFR §1.36;  
Submission of Preliminary Amendment;  
Replacement Drawings – 13 Sheets;  
Electronic payment of filing fee.



**IN THE UNITED STATES PATENT OFFICE**

In Re Patent Application of:	)	Examiner:	Not Yet Assigned
	)		
First Named Inventor: Marc Baum	)	Art Unit:	2161
	)		
Application No. 12/189,788	)		
	)		
Filed: August 12, 2008	)		
	)		
For: FORMING A SECURITY NETWORK INCLUDING	)		
INTEGRATED SECURITY SYSTEM	)		
<u>COMPONENTS AND NETWORK DEVICES</u>	)		

Mail Stop Missing Parts  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

Sir:

In response to a Notice to File Missing Parts of Nonprovisional Application mailed September 23, 2008 in connection with the above-referenced patent application, Applicants submit herewith:

1. Declaration in compliance with 37 CFR § 1.36;
2. Electronic payment via credit card in the amount of \$65.00 for the late declaration surcharge;
3. Preliminary amendment, including replacement drawings (13 sheets).

Respectfully Submitted,  
 Courtney Staniford & Gregory & LLP

Richard L. Gregory, Jr.  
 Reg. No. 42,607

Date November 24, 2008

**DECLARATION AND POWER OF ATTORNEY**

(Docket No. ICON.P001D3)

As a below-named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the inventions described and claimed in the specification filed:

\_\_\_\_\_ HEREWITH,

  X   on August 12, 2008 , Application Number 12/189,788 ,  
and entitled:

**FORMING A SECURITY NETWORK INCLUDING INTEGRATED  
SECURITY SYSTEM COMPONENTS AND NETWORK DEVICES**

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to herein.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

The undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h).

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the application-as-filed with respect to: 1) the above-identified application, 2) any foreign application to which the above-identified application claims priority under 35 USC 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37

CFR 1.55 has been filed in the above-identified US application, and 3) any U.S. application from which benefit is sought in the above-identified application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the **registered patent practitioners associated with Customer Number 53186** with full power of substitution and revocation, to prosecute this application and transact all business in the U.S. Patent and Trademark Office connected therewith. The current mailing address and telephone and facsimile numbers are:

P.O. Box 9686  
San Jose, California 95157

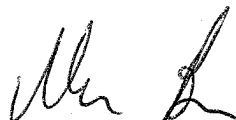
Tel: (408) 342-1900  
Fax: (408) 342-1909

Inventor:	Marc Baum		
Residence City:	San Jose	Residence State:	CA
Residence Country:	US	Citizenship:	US

Mailing Address      3045 Park Blvd., 2<sup>nd</sup> Floor  
Palo Alto, CA 94306  
US

Date: \_\_\_\_\_

11/3/08

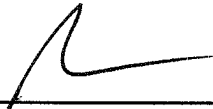


Marc Baum

Inventor: Paul J. Dawes  
Residence City: Woodside  
Residence Country: US  
Residence State: CA  
Citizenship: US

Mailing Address 3045 Park Blvd., 2<sup>nd</sup> Floor  
Palo Alto, CA 94306  
US


Date: 11/6/08

  
\_\_\_\_\_  
Paul J. Dawes

Inventor: Mike Kinney  
Residence City: Foster City  
Residence Country: US  
Residence State: CA  
Citizenship: US

Mailing Address 3045 Park Blvd., 2<sup>nd</sup> Floor  
Palo Alto, CA 94306  
US

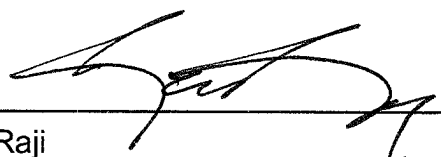
Date: 11/3/2008

  
\_\_\_\_\_  
Mike Kinney

Inventor: Reza Raji  
Residence City: Menlo Park  
Residence Country: US  
Residence State: CA  
Citizenship: US

Mailing Address 3045 Park Blvd., 2<sup>nd</sup> Floor  
Palo Alto, CA 94306  
US

Date: 11/3/08

  
\_\_\_\_\_  
Reza Raji

Inventor: David Swenson  
Residence City: Glyndon  
Residence Country: US  
Residence State: MN  
Citizenship: US

Mailing Address 3045 Park Blvd., 2<sup>nd</sup> Floor  
Palo Alto, CA 94306  
US

Date: 11/10/08



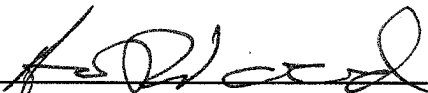
---

David Swenson

Inventor: Aaron Wood  
Residence City: Boulder Creek  
Residence Country: US  
Residence State: CA  
Citizenship: US

Mailing Address 3045 Park Blvd., 2<sup>nd</sup> Floor  
Palo Alto, CA 94306  
US

Date: 11/2/08



---

Aaron Wood

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/189,788</b>	Filing Date <b>08/12/2008</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
(Column 1)		(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>		OR	SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)		RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		OR	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =			X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	SMALL ENTITY	
AMENDMENT	11/24/2008	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 51	Minus	** 51	=	0	OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus	***4	=	0	OR	X \$ =
<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>							OR	
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	SMALL ENTITY	
AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)	
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	X \$ =	OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	X \$ =	OR	X \$ =
<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>							OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

Legal Instrument Examiner:  
 /LAJUAN HICKSON/

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 12/189,788, 08/12/2008, 2161, 1315, ICON.P001D3, 51, 4

CONFIRMATION NO. 7650

53186
COURTNEY STANIFORD & GREGORY LLP
P.O. BOX 9686
SAN JOSE, CA 95157

FILING RECEIPT



Date Mailed: 09/23/2008

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Marc Baum, Palo Alto, CA;
Paul J. Dawes, Palo Alto, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 60/957,997 08/24/2007
and claims benefit of 60/968,005 08/24/2007
and claims benefit of 60/987,359 11/12/2007
and claims benefit of 60/987,366 11/12/2007
and claims benefit of 61/019,162 01/04/2008
and claims benefit of 61/019,167 01/04/2008
and claims benefit of 61/023,489 01/25/2008
and claims benefit of 61/023,493 01/25/2008
and claims benefit of 61/023,496 01/25/2008
and claims benefit of 61/087,967 08/11/2008
and is a CIP of 11/084,232 03/16/2005
and is a CIP of 11/761,718 06/12/2007
and is a CIP of 11/761,745 06/12/2007
and is a CIP of 12/019,554 01/24/2008
and is a CIP of 12/019,568 01/24/2008

Foreign Applications

Projected Publication Date: To Be Determined - pending completion of Missing Parts

**Non-Publication Request:** No

**Early Publication Request:** No

**\*\* SMALL ENTITY \*\***

**Title**

Forming A Security Network Including Integrated Security System Components and Network Devices

**Preliminary Class**

707

## **PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).



**LICENSE FOR FOREIGN FILING UNDER**  
**Title 35, United States Code, Section 184**  
**Title 37, Code of Federal Regulations, 5.11 & 5.15**

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 4 columns: APPLICATION NUMBER (12/189,788), FILING OR 371(C) DATE (08/12/2008), FIRST NAMED APPLICANT (Marc Baum), ATTY. DOCKET NO./TITLE (ICON.P001D3)

CONFIRMATION NO. 7650

FORMALITIES LETTER



53186
COURTNEY STANIFORD & GREGORY LLP
P.O. BOX 9686
SAN JOSE, CA 95157

Date Mailed: 09/23/2008

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given TWO MONTHS from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment.

- The oath or declaration is missing. A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required. Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
- The drawings must be reasonably free from erasures and must be free from alterations, overwriting, interlineations, folds, and copy marks. See Figure(s) 4-7, 10-14.
- The drawings submitted to the Office are not electronically reproducible because portions of figures 1-3 are missing and/or blurry.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of **\$65** for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this notice.

**SUMMARY OF FEES DUE:**

Total additional fee(s) required for this application is **\$65** for a small entity

- **\$65** Surcharge.

Replies should be mailed to:

Mail Stop Missing Parts  
Commissioner for Patents  
P.O. Box 1450  
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.

<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/bto/

---

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Attorney Docket No. ICON.P001D3

Patent

**Transmittal of Patent Application**

*Certification Under 37 C.F.R. §1.8(a)*

Transmitted via

**August 11, 2008**

Date of Transmission

**USPTO EFS**

I hereby certify that this document, and any other accompanying documents referred to herein are being transmitted to the United States Patent Office via EFS in accordance with 37 C.F.R. §1.6(a)(4) on the date indicated above.

***Jerry Donnard***

(Print Name of Person Transmitting Documents)



(Signature of Person Transmitting Documents)

Application Data Sheet;  
Nonprovisional Patent Application;  
Drawings;  
Electronic payment of filing fee.

UNITED STATES PATENT APPLICATION

FOR

FORMING A SECURITY NETWORK INCLUDING INTEGRATED SECURITY  
SYSTEM COMPONENTS AND NETWORK DEVICES

Inventors:

Marc Baum

Paul J. Dawes

FORMING A SECURITY NETWORK INCLUDING INTEGRATED SECURITY  
SYSTEM COMPONENTS AND NETWORK DEVICES

RELATED APPLICATIONS

5           This application claims the benefit of United States (US) Patent Application  
Number 60/955,172, filed August 10, 2007.

          This application claims the benefit of US Patent Application Number 60/957,997,  
filed August 24, 2007.

10           This application claims the benefit of US Patent Application Number 60/968,005,  
filed August 24, 2007.

          This application claims the benefit of US Patent Application Number 60/987,359,  
filed November 12, 2007.

          This application claims the benefit of US Patent Application Number 60/987,366,  
filed November 12, 2007.

15           This application claims the benefit of US Patent Application Number 61/019,162,  
filed January 4, 2008.

          This application claims the benefit of US Patent Application Number 61/019,167,  
filed January 4, 2008.

20           This application claims the benefit of US Patent Application Number 61/023,489,  
filed January 25, 2008.

          This application claims the benefit of US Patent Application Number 61/023,493,  
filed January 25, 2008.

          This application claims the benefit of US Patent Application Number 61/023,496,  
filed January 25, 2008.

25           This application claims the benefit of US Patent Application Number 61/087,967,  
filed August 11, 2008.

          This application is a continuation in part application of US Patent Application  
Number 11/084,232, filed March 16, 2005.

30           This application is a continuation in part application of US Patent Application  
Number 11/761,718, filed June 12, 2007.

This application is a continuation in part application of US Patent Application Number 11/761,745, filed June 12, 2007.

This application is a continuation in part application of US Patent Application Number 12/019,554, filed January 24, 2008.

5 This application is a continuation in part application of US Patent Application Number 12/019,568, filed January 24, 2008.

### TECHNICAL FIELD

10 The embodiments described herein relate generally to a method and apparatus for improving the capabilities of security systems in home and business applications. More particularly, the embodiments described herein relate to a method and apparatus for wirelessly interfacing to and controlling security systems from within a home or business, and extending such control and interface to remote devices outside the premise.

### 15 BACKGROUND

The field of home and small business security is dominated by technology suppliers who build comprehensive 'closed' security systems, where the individual components (sensors, security panels, keypads) operate solely within the confines of a single vendor solution. For example, a wireless motion sensor from vendor A cannot be  
20 used with a security panel from vendor B. Each vendor typically has developed sophisticated proprietary wireless technologies to enable the installation and management of wireless sensors, with little or no ability for the wireless devices to operate separate from the vendor's homogeneous system. Furthermore, these traditional systems are extremely limited in their ability to interface either to a local or wide area standards-  
25 based network (such as an IP network); most installed systems support only a low-bandwidth, intermittent connection utilizing phone lines or cellular (RF) backup systems. Wireless security technology from providers such as GE Security, Honeywell, and DSC/Tyco are well known in the art, and are examples of this proprietary approach to security systems for home and business.

30 Furthermore, with the proliferation of the internet, ethernet and WiFi local area networks (LANs) and advanced wide area networks (WANs) that offer high bandwidth,

low latency connections (broadband), as well as more advanced wireless WAN data networks (e.g. GPRS or CDMA 1xRTT) there increasingly exists the networking capability to extend these traditional security systems to offer enhanced functionality. In addition, the proliferation of broadband access has driven a corresponding increase in home and small business networking technologies and devices. It is desirable to extend traditional security systems to encompass enhanced functionality such as the ability to control and manage security systems from the world wide web, cellular telephones, or advanced function internet-based devices. Other desired functionality includes an open systems approach to interface home security systems to home and small business networks.

Due to the proprietary approach described above, the traditional vendors are the only ones capable of taking advantage of these new network functions. To date, even though the vast majority of home and business customers have broadband network access in their premises, most security systems do not offer the advanced capabilities associated with high speed, low-latency LANs and WANs. This is primarily because the proprietary vendors have not been able to deliver such technology efficiently or effectively. Solution providers attempting to address this need are becoming known in the art, including three categories of vendors: traditional proprietary hardware providers such as Honeywell and GE Security; third party hard-wired module providers such as Alarm.com, NextAlarm, and uControl; and new proprietary systems providers such as InGrid.

A disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the continued proprietary approach of these vendors. As they develop technology in this area it once again operates only with the hardware from that specific vendor, ignoring the need for a heterogeneous, cross-vendor solution. Yet another disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the lack of experience and capability of these companies in creating open internet and web based solutions, and consumer friendly interfaces.

A disadvantage of the prior art technologies of the third party hard-wired module providers arises due to the installation and operational complexities and functional limitations associated with hardwiring a new component into existing security systems. Moreover, a disadvantage of the prior art technologies of the new proprietary systems



providers arises due to the need to discard all prior technologies, and implement an entirely new form of security system to access the new functionalities associated with broadband and wireless data networks. There remains, therefore, a need for systems, devices, and methods that easily interface to and control the existing proprietary security technologies utilizing a variety of wireless technologies.

#### INCORPORATION BY REFERENCE

Each patent, patent application, and/or publication mentioned in this specification is herein incorporated by reference in its entirety to the same extent as if each individual patent, patent application, and/or publication was specifically and individually indicated to be incorporated by reference.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**Figure 1** is a block diagram of the integrated security system, under an embodiment.

**Figure 2** is a block diagram of components of the integrated security system, under an embodiment.

**Figure 3** is a block diagram of the gateway software or applications, under an embodiment.

**Figure 4** is a block diagram of the gateway components, under an embodiment.

**Figure 5** is a block diagram of IP device integration with a premise network, under an embodiment.

**Figure 6** is a block diagram of IP device integration with a premise network, under an alternative embodiment.

**Figure 7** is a block diagram of a touchscreen, under an embodiment.

**Figure 8** is a flow diagram for a method of forming a security network including integrated security system components, under an embodiment.

**Figure 9** is a flow diagram for a method of forming a security network including integrated security system components and network devices, under an embodiment.

**Figure 10** is a flow diagram for installation of an IP device into a private network environment, under an embodiment.

**Figure 11** is a block diagram showing communications among IP devices of the private network environment, under an embodiment.

**Figure 12** is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment.

5 **Figure 13** is a block diagram of an integrated security system 1300 wirelessly interfacing to proprietary security systems, under an embodiment.

**Figure 14** is a flow diagram for wirelessly ‘learning’ the gateway into an existing security system and discovering extant sensors, under an embodiment.

10 DETAILED DESCRIPTION

An integrated security system is described that integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network (broadband, cellular/GSM, POTS access) that enables users to remotely stay connected to their premises. The integrated security system, while  
15 delivering remote premise monitoring and control functionality to conventional monitored premise protection, complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wirelessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices (cameras, lamp modules, thermostats, etc.) can be added,  
20 enabling users to remotely see live video and/or pictures and control home devices via their personal web portal or webpage, mobile phone, and/or other remote client device. Users can also receive notifications via email or text message when happenings occur, or do not occur, in their home.

Although the detailed description herein contains many specifics for the purposes  
25 of illustration, anyone of ordinary skill in the art will appreciate that many variations and alterations to the following details are within the scope of the embodiments described herein. Thus, the following illustrative embodiments are set forth without any loss of generality to, and without imposing limitations upon, the claimed invention.

In accordance with the embodiments described herein, a wireless system (e.g.,  
30 radio frequency (RF)) is provided that enables a security provider or consumer to extend the capabilities of an existing RF-capable security system or a non-RF-capable security

system that has been upgraded to support RF capabilities. The system includes an RF-capable Gateway device (physically located within RF range of the RF-capable security system) and associated software operating on the Gateway device. The system also includes a web server, application server, and remote database providing a persistent store for information related to the system.

The security systems of an embodiment, referred to herein as the iControl security system or integrated security system, extend the value of traditional home security by adding broadband access and the advantages of remote home monitoring and home control through the formation of a security network including components of the integrated security system integrated with a conventional premise security system and a premise local area network (LAN). With the integrated security system, conventional home security sensors, cameras, touchscreen keypads, lighting controls, and/or Internet Protocol (IP) devices in the home (or business) become connected devices that are accessible anywhere in the world from a web browser, mobile phone or through content-enabled touchscreens. The integrated security system experience allows security operators to both extend the value proposition of their monitored security systems and reach new consumers that include broadband users interested in staying connected to their family, home and property when they are away from home.

The integrated security system of an embodiment includes security servers (also referred to herein as iConnect servers or security network servers) and an iHub gateway (also referred to herein as the gateway, the iHub, or the iHub client) that couples or integrates into a home network (e.g., LAN) and communicates directly with the home security panel, in both wired and wireless installations. The security system of an embodiment automatically discovers the security system components (e.g., sensors, etc.) belonging to the security system and connected to a control panel of the security system and provides consumers with full two-way access via web and mobile portals. The gateway supports various wireless protocols and can interconnect with a wide range of control panels offered by security system providers. Service providers and users can then extend the system's capabilities with the additional IP cameras, lighting modules or security devices such as interactive touchscreen keypads. The integrated security system adds an enhanced value to these security systems by enabling consumers to stay

connected through email and SMS alerts, photo push, event-based video capture and rule-based monitoring and notifications. This solution extends the reach of home security to households with broadband access.

The integrated security system builds upon the foundation afforded by traditional security systems by layering broadband and mobile access, IP cameras, interactive touchscreens, and an open approach to home automation on top of traditional security system configurations. The integrated security system is easily installed and managed by the security operator, and simplifies the traditional security installation process, as described below.

The integrated security system provides an open systems solution to the home security market. As such, the foundation of the integrated security system customer premises equipment (CPE) approach has been to abstract devices, and allows applications to manipulate and manage multiple devices from any vendor. The integrated security system DeviceConnect technology that enables this capability supports protocols, devices, and panels from GE Security and Honeywell, as well as consumer devices using Z-Wave, IP cameras (e.g., Ethernet, wifi, and Homeplug), and IP touchscreens. The DeviceConnect is a device abstraction layer that enables any device or protocol layer to interoperate with integrated security system components. This architecture enables the addition of new devices supporting any of these interfaces, as well as add entirely new protocols.

The benefit of DeviceConnect is that it provides supplier flexibility. The same consistent touchscreen, web, and mobile user experience operate unchanged on whatever security equipment selected by a security system provider, with the system provider's choice of IP cameras, backend data center and central station software.

The integrated security system provides a complete system that integrates or layers on top of a conventional host security system available from a security system provider. The security system provider therefore can select different components or configurations to offer (e.g., CDMA, GPRS, no cellular, etc.) as well as have iControl modify the integrated security system configuration for the system provider's specific needs (e.g., change the functionality of the web or mobile portal, add a GE or Honeywell-compatible TouchScreen, etc.).

The integrated security system integrates with the security system provider infrastructure for central station reporting directly via Broadband and GPRS alarm transmissions. Traditional dial-up reporting is supported via the standard panel connectivity. Additionally, the integrated security system provides interfaces for advanced functionality to the CMS, including enhanced alarm events, system installation  
5 optimizations, system test verification, video verification, 2-way voice over IP and GSM.

The integrated security system is an IP centric system that includes broadband connectivity so that the gateway augments the existing security system with broadband and GPRS connectivity. If broadband is down or unavailable GPRS may be used, for  
10 example. The integrated security system supports GPRS connectivity using an optional wireless package that includes a GPRS modem in the gateway. The integrated security system treats the GPRS connection as a higher cost though flexible option for data transfers. In an embodiment the GPRS connection is only used to route alarm events (e.g., for cost), however the gateway can be configured (e.g., through the iConnect server  
15 interface) to act as a primary channel and pass any or all events over GPRS.

Consequently, the integrated security system does not interfere with the current plain old telephone service (POTS) security panel interface. Alarm events can still be routed through POTS; however the gateway also allows such events to be routed through a  
20 broadband or GPRS connection as well. The integrated security system provides a web application interface to the CSR tool suite as well as XML web services interfaces for programmatic integration between the security system provider's existing call center products. The integrated security system includes, for example, APIs that allow the security system provider to integrate components of the integrated security system into a custom call center interface. The APIs include XML web service APIs for integration of  
25 existing security system provider call center applications with the integrated security system service. All functionality available in the CSR Web application is provided with these API sets. The Java and XML-based APIs of the integrated security system support provisioning, billing, system administration, CSR, central station, portal user interfaces, and content management functions, to name a few. The integrated security system can  
30 provide a customized interface to the security system provider's billing system, or

alternatively can provide security system developers with APIs and support in the integration effort.

The integrated security system provides or includes business component interfaces for provisioning, administration, and customer care to name a few. Standard templates and examples are provided with a defined customer professional services engagement to help integrate OSS/BSS systems of a Service Provider with the integrated security system.

The integrated security system components support and allow for the integration of customer account creation and deletion with a security system. The iConnect APIs provides access to the provisioning and account management system in iConnect and provide full support for account creation, provisioning, and deletion. Depending on the requirements of the security system provider, the iConnect APIs can be used to completely customize any aspect of the integrated security system backend operational system.

The integrated security system includes a gateway that supports the following standards-based interfaces, to name a few: Ethernet IP communications via Ethernet ports on the gateway, and standard XML/TCP/IP protocols and ports are employed over secured SSL sessions; USB 2.0 via ports on the gateway; 802.11b/g/n IP communications; GSM/GPRS RF WAN communications; CDMA 1xRTT RF WAN communications (optional, can also support EVDO and 3G technologies).

The gateway supports the following proprietary interfaces, to name a few: interfaces including Dialog RF network (319.5 MHz) and RS485 Superbus 2000 wired interface; RF mesh network (908 MHz); and interfaces including RF network (345 MHz) and RS485/RS232bus wired interfaces.

Regarding security for the IP communications (e.g., authentication, authorization, encryption, anti-spoofing, etc), the integrated security system uses SSL to encrypt all IP traffic, using server and client-certificates for authentication, as well as authentication in the data sent over the SSL-encrypted channel. For encryption, integrated security system issues public/private key pairs at the time/place of manufacture, and certificates are not stored in any online storage in an embodiment.

The integrated security system does not need any special rules at the customer premise and/or at the security system provider central station because the integrated security system makes outgoing connections using TCP over the standard HTTP and HTTPS ports. Provided outbound TCP connections are allowed then no special requirements on the firewalls are necessary.

**Figure 1** is a block diagram of the integrated security system 100, under an embodiment. The integrated security system 100 of an embodiment includes the gateway 102 and the security servers 104 coupled to the conventional home security system 110. At a customer's home or business, the gateway 102 connects and manages the diverse variety of home security and self-monitoring devices. The gateway 102 communicates with the iConnect Servers 104 located in the service provider's data center 106 (or hosted in integrated security system data center), with the communication taking place via a communication network 108 or other network (e.g., cellular network, internet, etc.). These servers 104 manage the system integrations necessary to deliver the integrated system service described herein. The combination of the gateway 102 and the iConnect servers 104 enable a wide variety of remote client devices 120 (e.g., PCs, mobile phones and PDAs) allowing users to remotely stay in touch with their home, business and family. In addition, the technology allows home security and self-monitoring information, as well as relevant third party content such as traffic and weather, to be presented in intuitive ways within the home, such as on advanced touchscreen keypads.

The integrated security system service (also referred to as iControl service) can be managed by a service provider via browser-based Maintenance and Service Management applications that are provided with the iConnect Servers. Or, if desired, the service can be more tightly integrated with existing OSS/BSS and service delivery systems via the iConnect web services-based XML APIs.

The integrated security system service can also coordinate the sending of alarms to the home security Central Monitoring Station (CMS) 199. Alarms are passed to the CMS 199 using standard protocols such as Contact ID or SIA and can be generated from the home security panel location as well as by iConnect server 104 conditions (such as lack of communications with the integrated security system). In addition, the link between the security servers 104 and CMS 199 provides tighter integration between

home security and self-monitoring devices and the gateway 102. Such integration enables advanced security capabilities such as the ability for CMS personnel to view photos taken at the time a burglary alarm was triggered. For maximum security, the gateway 102 and iConnect servers 104 support the use of a mobile network (both GPRS and CDMA options are available) as a backup to the primary broadband connection.

The integrated security system service is delivered by hosted servers running software components that communicate with a variety of client types while interacting with other systems. **Figure 2** is a block diagram of components of the integrated security system 100, under an embodiment. Following is a more detailed description of the components.

The iConnect servers 104 support a diverse collection of clients 120 ranging from mobile devices, to PCs, to in-home security devices, to a service provider's internal systems. Most clients 120 are used by end-users, but there are also a number of clients 120 that are used to operate the service.

Clients 120 used by end-users of the integrated security system 100 include, but are not limited to, the following:

Clients based on gateway client applications 202 (e.g., a processor-based device running the gateway technology that manages home security and automation devices).

A web browser 204 accessing a Web Portal application, performing end-user configuration and customization of the integrated security system service as well as monitoring of in-home device status, viewing photos and video, etc. Device and user management can also be performed by this portal application.

A mobile device 206 (e.g., PDA, mobile phone, etc.) accessing the integrated security system Mobile Portal. This type of client 206 is used by end-users to view system status and perform operations on devices (e.g., turning on a lamp, arming a security panel, etc.) rather than for system configuration tasks such as adding a new device or user.

PC or browser-based "widget" containers 208 that present integrated security system service content, as well as other third-party content, in simple,



targeted ways (e.g. a widget that resides on a PC desktop and shows live video from a single in-home camera).

5 Touchscreen home security keypads 208 and advanced in-home devices that present a variety of content widgets via an intuitive touchscreen user interface.

Notification recipients 210 (e.g., cell phones that receive SMS-based notifications when certain events occur (or don't occur), email clients that receive an email message with similar information, etc.).

10 Custom-built clients (not shown) that access the iConnect web services XML API to interact with users' home security and self-monitoring information in new and unique ways. Such clients could include new types of mobile devices, or complex applications where integrated security system content is integrated into a broader set of application features.

15 In addition to the end-user clients, the iConnect servers 104 support PC browser-based Service Management clients that manage the ongoing operation of the overall service. These clients run applications that handle tasks such as provisioning, service monitoring, customer support and reporting.

20 There are numerous types of server components of the iConnect servers 104 of an embodiment including, but not limited to, the following: Business Components which manage information about all of the home security and self-monitoring devices; End-User Application Components which display that information for users and access the Business Components via published XML APIs; and Service Management Application Components which enable operators to administer the service (these components also access the Business Components via the XML APIs, and also via published SNMP  
25 MIBs).

The server components provide access to, and management of, the objects associated with an integrated security system installation. The top-level object is the "network." It is a location where a gateway 102 is located, and is also commonly referred to as a site or premises; the premises can include any type of structure (e.g.,  
30 home, office, warehouse, etc.) at which an gateway 102 is located. Users can only access the networks to which they have been granted permission. Within a network, every

object monitored by the gateway 102 is called a device. Devices include the sensors, cameras, home security panels and automation devices, as well as the controller or processor-based device running the gateway applications.

Various types of interactions are possible between the objects in a system.

5 Automations define actions that occur as a result of a change in state of a device. For example, take a picture with the front entry camera when the front door sensor changes to “open”. Notifications are messages sent to users to indicate that something has occurred, such as the front door going to “open” state, or has not occurred (referred to as an iWatch notification). Schedules define changes in device states that are to take place at  
10 predefined days and times. For example, set the security panel to “Armed” mode every weeknight at 11:00pm.

The iConnect Business Components are responsible for orchestrating all of the low-level service management activities for the integrated security system service. They define all of the users and devices associated with a network (site), analyze how the  
15 devices interact, and trigger associated actions (such as sending notifications to users). All changes in device states are monitored and logged. The Business Components also manage all interactions with external systems as required, including sending alarms and other related self-monitoring data to the home security Central Monitoring System (CMS) 199. The Business Components are implemented as portable Java J2EE Servlets,  
20 but are not so limited.

The following iConnect Business Components manage the main elements of the integrated security system service, but the embodiment is not so limited:

A Registry Manager 220 defines and manages users and networks. This component is responsible for the creation, modification and termination of users  
25 and networks. It is also where a user's access to networks is defined.

A Network Manager 222 defines and manages security and self-monitoring devices that are deployed on a network (site). This component handles the creation, modification, deletion and configuration of the devices, as well as the creation of automations, schedules and notification rules associated  
30 with those devices.

5 A Data Manager 224 manages access to current and logged state data for an existing network and its devices. This component specifically does not provide any access to network management capabilities, such as adding new devices to a network, which are handled exclusively by the Network Manager 222.

To achieve optimal performance for all types of queries, data for current device states is stored separately from historical state data (a.k.a. “logs”) in the database. A Log Data Manager 226 performs ongoing transfers of current device state data to the historical data log tables.

10 Additional iConnect Business Components handle direct communications with certain clients and other systems, for example:

15 An iHub Manager 228 directly manages all communications with iHub clients, including receiving information about device state changes, changing the configuration of devices, and pushing new versions of the iHub client to the hardware it is running on.

A Notification Manager 230 is responsible for sending all notifications to clients via SMS (mobile phone messages), email (via a relay server like an SMTP email server), etc.

20 An Alarm and CMS Manager 232 sends critical server-generated alarm events to the home security Central Monitoring Station (CMS) and manages all other communications of integrated security system service data to and from the CMS.

25 The Element Management System (EMS) 234 is an iControl Business Component that manages all activities associated with service installation, scaling and monitoring, and filters and packages service operations data for use by service management applications. The SNMP MIBs published by the EMS can also be incorporated into any third party monitoring system if desired.

30 The iConnect Business Components store information about the objects that they manage in the iControl Service Database 240 and in the iControl Content Store 242. The iControl Content Store is used to store media objects like video, photos and widget content, while the Service Database stores information about users, networks, and

devices. Database interaction is performed via a JDBC interface. For security purposes, the Business Components manage all data storage and retrieval.

The iControl Business Components provide web services-based APIs that application components use to access the Business Components' capabilities. Functions of application components include presenting integrated security system service data to end-users, performing administrative duties, and integrating with external systems and back-office applications.

The primary published APIs for the iConnect Business Components include, but are not limited to, the following:

10           A Registry Manager API 252 provides access to the Registry Manager Business Component's functionality, allowing management of networks and users.

15           A Network Manager API 254 provides access to the Network Manager Business Component's functionality, allowing management of devices on a network.

          A Data Manager API 256 provides access to the Data Manager Business Component's functionality, such as setting and retrieving (current and historical) data about device states.

20           A Provisioning API 258 provides a simple way to create new networks and configure initial default properties.

Each API of an embodiment includes two modes of access: Java API or XML API. The XML APIs are published as web services so that they can be easily accessed by applications or servers over a network. The Java APIs are a programmer-friendly wrapper for the XML APIs. Application components and integrations written in Java should generally use the Java APIs rather than the XML APIs directly.

25           The iConnect Business Components also have an XML-based interface 260 for quickly adding support for new devices to the integrated security system. This interface 260, referred to as DeviceConnect 260, is a flexible, standards-based mechanism for defining the properties of new devices and how they can be managed. Although the format is flexible enough to allow the addition of any type of future device, pre-defined

30

XML profiles are currently available for adding common types of devices such as sensors (SensorConnect), home security panels (PanelConnect) and IP cameras (CameraConnect).

5 The iConnect End-User Application Components deliver the user interfaces that run on the different types of clients supported by the integrated security system service. The components are written in portable Java J2EE technology (e.g., as Java Servlets, as JavaServer Pages (JSPs), etc.) and they all interact with the iControl Business Components via the published APIs.

10 The following End-User Application Components generate CSS-based HTML/JavaScript that is displayed on the target client. These applications can be dynamically branded with partner-specific logos and URL links (such as Customer Support, etc.). The End-User Application Components of an embodiment include, but are not limited to, the following:

15 An iControl Activation Application 270 that delivers the first application that a user sees when they set up the integrated security system service. This wizard-based web browser application securely associates a new user with a purchased gateway and the other devices included with it as a kit (if any). It primarily uses functionality published by the Provisioning API.

20 An iControl Web Portal Application 272 runs on PC browsers and delivers the web-based interface to the integrated security system service. This application allows users to manage their networks (e.g. add devices and create automations) as well as to view/change device states, and manage pictures and videos. Because of the wide scope of capabilities of this application, it uses three different Business Component APIs that include the Registry Manager API, Network  
25 Manager API, and Data Manager API, but the embodiment is not so limited.

30 An iControl Mobile Portal 274 is a small-footprint web-based interface that runs on mobile phones and PDAs. This interface is optimized for remote viewing of device states and pictures/videos rather than network management. As such, its interaction with the Business Components is primarily via the Data Manager API.

Custom portals and targeted client applications can be provided that leverage the same Business Component APIs used by the above applications.

5 A Content Manager Application Component 276 delivers content to a variety of clients. It sends multimedia-rich user interface components to widget container clients (both PC and browser-based), as well as to advanced touchscreen keypad clients. In addition to providing content directly to end-user devices, the Content Manager 276 provides widget-based user interface components to satisfy requests from other Application Components such as the iControl Web 272 and Mobile 274 portals.

10 A number of Application Components are responsible for overall management of the service. These pre-defined applications, referred to as Service Management Application Components, are configured to offer off-the-shelf solutions for production management of the integrated security system service including provisioning, overall service monitoring, customer support, and reporting, for example. The Service  
15 Management Application Components of an embodiment include, but are not limited to, the following:

A Service Management Application 280 allows service administrators to perform activities associated with service installation, scaling and monitoring/alerting. This application interacts heavily with the Element  
20 Management System (EMS) Business Component to execute its functionality, and also retrieves its monitoring data from that component via protocols such as SNMP MIBs.

A Kitting Application 282 is used by employees performing service provisioning tasks. This application allows home security and self-monitoring  
25 devices to be associated with gateways during the warehouse kitting process.

A CSR Application and Report Generator 284 is used by personnel supporting the integrated security system service, such as CSRs resolving end-user issues and employees enquiring about overall service usage. Pushes of new gateway firmware to deployed gateways is also managed by this application.

The iConnect servers 104 also support custom-built integrations with a service provider's existing OSS/BSS, CSR and service delivery systems 290. Such systems can access the iConnect web services XML API to transfer data to and from the iConnect servers 104. These types of integrations can compliment or replace the PC browser-based Service Management applications, depending on service provider needs.

As described above, the integrated security system of an embodiment includes an gateway, or iHub. The gateway of an embodiment includes a device that is deployed in the home or business and couples or connects the various third-party cameras, home security panels, sensors and devices to the iConnect server over a WAN connection as described in detail herein. The gateway couples to the home network and communicates directly with the home security panel in both wired and wireless sensor installations. The gateway is configured to be low-cost, reliable and thin so that it complements the integrated security system network-based architecture.

The gateway supports various wireless protocols and can interconnect with a wide range of home security control panels. Service providers and users can then extend the system's capabilities by adding IP cameras, lighting modules and additional security devices. The gateway is configurable to be integrated into many consumer appliances, including set-top boxes, routers and security panels. The small and efficient footprint of the gateway enables this portability and versatility, thereby simplifying and reducing the overall cost of the deployment.

**Figure 3** is a block diagram of the gateway 102 including gateway software or applications, under an embodiment. The gateway software architecture is relatively thin and efficient, thereby simplifying its integration into other consumer appliances such as set-top boxes, routers, touch screens and security panels. The software architecture also provides a high degree of security against unauthorized access. This section describes the various key components of the gateway software architecture.

The gateway application layer 302 is the main program that orchestrates the operations performed by the gateway. The Security Engine 304 provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the

WAN). The Security Engine 304 of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

5 Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.

10 Bi-directional authentication between the gateway and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.

15 Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The gateway provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.

802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.

20 An gateway-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying gateway-enabled devices have the knowledge that only an gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

25 As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.



A Remote Firmware Download module 306 allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server 104, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download  
5 mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Gateway firmware can be remotely download either for one gateway at a time, a group of gateways, or in batches.

The Automations engine 308 manages the user-defined rules of interaction  
10 between the different devices (e.g. when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

DeviceConnect 310 includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The  
15 DeviceConnect module 310 offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect 312 is provided for adding new sensors, CameraConnect 316 for adding IP cameras, and  
20 PanelConnect 314 for adding home security panels.

The Schedules engine 318 is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application. The Schedules  
25 Engine 318 then interfaces with SensorConnect 312 to ensure that scheduled events occur at precisely the desired time.

The Device Management module 320 is in charge of all discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated  
30 security system, require user configuration of many IP and security parameters – to simplify the user experience and reduce the customer support burden, the device

management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

5 The video routing engine 322 is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing.

**Figure 4** is a block diagram of components of the gateway 102, under an embodiment. Depending on the specific set of functionality desired by the service provider deploying the integrated security system service, the gateway 102 can use any of  
10 a number of processors 402, due to the small footprint of the gateway application firmware. In an embodiment, the gateway could include the Broadcom BCM5354 as the processor for example. In addition, the gateway 102 includes memory (e.g., FLASH 404, RAM 406, etc.) and any number of input/output (I/O) ports 408.

Referring to the WAN portion 410 of the gateway 102, the gateway 102 of an  
15 embodiment can communicate with the iConnect server using a number of communication types and/or protocols, for example Broadband 412, GPRS 414 and/or Public Switched Telephone Network (PSTN) 416 to name a few. In general, broadband communication 412 is the primary means of connection between the gateway 102 and the iConnect server 104 and the GPRS/CDMA 414 and/or PSTN 416 interfaces acts as back-  
20 up for fault tolerance in case the user's broadband connection fails for whatever reason, but the embodiment is not so limited.

Referring to the LAN portion 420 of the gateway 102, various protocols and physical transceivers can be used to communicate to off-the-shelf sensors and cameras. The gateway 102 is protocol-agnostic and technology-agnostic and as such can easily  
25 support almost any device networking protocol. The gateway 102 can, for example, support GE and Honeywell security RF protocols 422, Z-Wave 424, serial (RS232 and RS485) 426 for direct connection to security panels as well as WiFi 428 (802.11b/g) for communication to WiFi cameras.

The integrated security system includes couplings or connections among a variety  
30 of IP devices or components, and the device management module is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the

system, as described above. The integrated security system of an embodiment uses a “sandbox” network to discover and manage all IP devices coupled or connected as components of the system. The IP devices of an embodiment include wired devices, wireless devices, cameras, interactive touchscreens, and security panels to name a few.

5 These devices can be wired via ethernet cable or Wifi devices, all of which are secured within the sandbox network, as described below. The “sandbox” network is described in detail below.

**Figure 5** is a block diagram 500 of network or premise device integration with a premise network 250, under an embodiment. In an embodiment, network devices 255-  
10 257 are coupled to the gateway 102 using a secure network connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption), and the gateway 102 is coupled to the premise router/firewall 252 via a coupling with a premise LAN 250. The premise router/firewall 252 is coupled to a  
15 broadband modem 251, and the broadband modem 251 is coupled to a WAN 200 or other network outside the premise. The gateway 102 thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or  
connected to the LAN 250 of the host premises. The gateway sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway 102 manages  
20 or controls the sub-network separately from the LAN 250 and transfers data and information between components of the sub-network and the LAN 250/WAN 200, but is not so limited. Additionally, other network devices 254 can be coupled to the LAN 250 without being coupled to the gateway 102.

**Figure 6** is a block diagram 600 of network or premise device integration with a  
25 premise network 250, under an alternative embodiment. The network or premise devices 255-257 are coupled to the gateway 102, and the gateway 102 is coupled or connected between the premise router/firewall 252 and the broadband modem 251. The broadband modem 251 is coupled to a WAN 200 or other network outside the premise, while the  
premise router/firewall 252 is coupled to a premise LAN 250. As a result of its location  
30 between the broadband modem 251 and the premise router/firewall 252, the gateway 102 can be configured or function as the premise router routing specified data between the

outside network (e.g., WAN 200) and the premise router/firewall 252 of the LAN 250.

As described above, the gateway 102 in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices 255-257 and is coupled or connected between the LAN 250 of the host premises and the WAN

5 200. The gateway sub-network can include, but is not limited to, any number of network or premise devices 255-257 like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway 102 manages or controls the sub-network separately from the LAN 250 and transfers data and information between components of the sub-network and the LAN 250/WAN 200, but is not so limited.

10 Additionally, other network devices 254 can be coupled to the LAN 250 without being coupled to the gateway 102.

The examples described above with reference to Figures 5 and 6 are presented only as examples of IP device integration. The integrated security system is not limited to the type, number and/or combination of IP devices shown and described in these

15 examples, and any type, number and/or combination of IP devices is contemplated within the scope of this disclosure as capable of being integrated with the premise network.

The integrated security system of an embodiment includes an iControl touchscreen (also referred to as the touchscreen or integrated security system touchscreen), as described above, which provides core security keypad functionality,

20 content management and presentation, and embedded systems design. The networked security touchscreen system of an embodiment enables a consumer or security provider to easily and automatically install, configure and manage the security system and touchscreen located at a customer premise. Using this system the customer may access and control the local security system, local IP devices such as cameras, local sensors and control devices (such as lighting controls or pipe freeze sensors), as well as the local

25 security system panel and associated security sensors (such as door/window, motion, and smoke detectors). The customer premise may be a home, business, and/or other location equipped with a wired or wireless broadband IP connection. The system of an embodiment includes a touchscreen with a configurable software user interface, a

30 gateway device (e.g., iHub) that couples or connects to the security panel through a wired or wireless connection, a security panel, and a remote server that provides access to

content and information from the premises devices to a user when they are remote from the home. Note that the gateway device may be a separate device or may be physically incorporated into the touchscreen.

5 The touchscreen of an embodiment is integrated into a premise network using the gateway, as described above. The gateway as described herein functions to enable a separate wireless network, or sub-network, that is coupled, connected, or integrated with a network (e.g., WAN, LAN, etc.) of or coupled to the host premises. The sub-network enabled by the gateway optimizes the installation process for IP devices, like the touchscreen, that couple or connect to the sub-network by segregating these IP devices  
10 from other such devices on the network. This segregation of the IP devices of the sub-network further enables separate security and privacy policies to be implemented for these IP devices so that, where the IP devices are dedicated to specific functions (e.g., security), the security and privacy policies can be tailored specifically for the specific functions. Furthermore, the gateway and the sub-network it forms enables the  
15 segregation of data traffic, resulting in faster and more efficient data flow between components of the host network, components of the sub-network, and between components of the sub-network and components of the network.

The touchscreen of an embodiment includes a core functional embedded system that includes an embedded operating system, required hardware drivers, and an open  
20 system interface to name a few. The core functional embedded system can be provided by or as a component of a conventional security system (e.g., security system available from GE Security). These core functional units are used with components of the integrated security system as described herein. Note that portions of the touchscreen description below may include reference to a host premise security system (e.g., GE  
25 security system), but these references are included only as an example and do not limit the touchscreen to integration with any particular security system.

As an example, regarding the core functional embedded system, a reduced memory footprint version of embedded Linux forms the core operating system in an embodiment, and provides basic TCP/IP stack and memory management functions, along  
30 with a basic set of low-level graphics primitives. A set of device drivers is also provided or included that offer low-level hardware and network interfaces. In addition to the

standard drivers, an interface to the RS 485 bus is included that couples or connects to the security system panel (e.g., GE Concord panel). The interface may, for example, implement the Superbus 2000 protocol, which can then be utilized by the more comprehensive transaction-level security functions implemented in PanelConnect technology (e.g SetAlarmLevel (int level, int partition, char \*accessCode)). Power control drivers are also provided.

**Figure 7** is a block diagram of a touchscreen 700 of the integrated security system, under an embodiment. The touchscreen 700 generally includes an application/presentation layer 702 with a resident application 704, and a core engine 706. The touchscreen 700 also includes one or more of the following, but is not so limited: applications of premium services 710, widgets 712, a caching proxy 714, network security 716, network interface 718, security object 720, applications supporting devices 722, PanelConnect API 724, a gateway interface 726, and one or more ports 728.

More specifically, the touchscreen, when configured as a home security device, includes but is not limited to the following application or software modules: RS 485 and/or RS-232 bus security protocols to conventional home security system panel (e.g., GE Concord panel); functional home security classes and interfaces (e.g. Panel ARM state, Sensor status, etc.); Application/Presentation layer or engine; Resident Application; Consumer Home Security Application; installer home security application; core engine; and System bootloader/Software Updater. The core Application engine and system bootloader can also be used to support other advanced content and applications. This provides a seamless interaction between the premise security application and other optional services such as weather widgets or IP cameras.

An alternative configuration of the touchscreen includes a first Application engine for premise security and a second Application engine for all other applications. The integrated security system application engine supports content standards such as HTML, XML, Flash, etc. and enables a rich consumer experience for all 'widgets', whether security-based or not. The touchscreen thus provides service providers the ability to use web content creation and management tools to build and download any 'widgets' regardless of their functionality.

As discussed above, although the Security Applications have specific low-level functional requirements in order to interface with the premise security system, these applications make use of the same fundamental application facilities as any other 'widget', application facilities that include graphical layout, interactivity, application handoff, screen management, and network interfaces, to name a few.

Content management in the touchscreen provides the ability to leverage conventional web development tools, performance optimized for an embedded system, service provider control of accessible content, content reliability in a consumer device, and consistency between 'widgets' and seamless widget operational environment. In an embodiment of the integrated security system, widgets are created by web developers and hosted on the integrated security system Content Manager (and stored in the Content Store database). In this embodiment the server component caches the widgets and offers them to consumers through the web-based integrated security system provisioning system. The servers interact with the advanced touchscreen using HTTPS interfaces controlled by the core engine and dynamically download widgets and updates as needed to be cached on the touchscreen. In other embodiments widgets can be accessed directly over a network such as the Internet without needing to go through the iControl Content Manager

Referring to **Figure 7**, the touchscreen system is built on a tiered architecture, with defined interfaces between the Application/Presentation Layer (the Application Engine) on the top, the Core Engine in the middle, and the security panel and gateway APIs at the lower level. The architecture is configured to provide maximum flexibility and ease of maintenance.

The application engine of the touchscreen provides the presentation and interactivity capabilities for all applications (widgets) that run on the touchscreen, including both core security function widgets and third party content widgets. A fundamental component of the application engine is the Presentation Engine, which includes a set of libraries that implement the standards-based widget content (e.g., XML, HTML, JavaScript, Flash) layout and interactivity. This engine provides the widget with interfaces to dynamically load both graphics and application logic from third parties, support high level data description language as well as standard graphic formats. The set

of web content-based functionality available to a widget developer is extended by specific touchscreen functions implemented as local web services by the Core Engine.

The resident application of the touchscreen is the master service that controls the interaction of all widgets (all applications in the system), and enforces the business and security rules required by the service provider. For example, the resident application  
5 determines the priority of widgets, thereby enabling a home security widget to override resource requests from a less critical widget (e.g. a weather widget). The resident application also monitors widget behavior, and responds to client or server requests for cache updates.

10 The core engine of the touchscreen manages interaction with other components of the integrated security system, and provides an interface through which the resident application and authorized widgets can get information about the home security system, set alarms, install sensors, etc. At the lower level, the Core Engine's main interactions are through the PanelConnect API, which handles all communication with the security  
15 panel, and the gateway Interface, which handles communication with the gateway. In an embodiment, both the iHub Interface and PanelConnect API are resident and operating on the touchscreen. In another embodiment, the PanelConnect API runs on the gateway or other device that provides security system interaction and is accessed by the touchscreen through a web services interface.

20 The Core Engine also handles application and service level persistent and cached memory functions, as well as the dynamic provisioning of content and widgets, including but not limited to: flash memory management, local widget and content caching, widget version management (download, cache flush new/old content versions), as well as the caching and synchronization of user preferences. As a portion of these services the Core  
25 engine incorporates the bootloader functionality that is responsible for maintaining a consistent software image on the touchscreen, and acts as the client agent for all software updates. The bootloader is configured to ensure full update redundancy so that unsuccessful downloads cannot corrupt the integrated security system.

Video management is provided as a set of web services by the Core Engine.

30 Video management includes the retrieval and playback of local video feeds as well as



remote control and management of cameras (all through iControl CameraConnect technology).

Both the high level application layer and the mid-level core engine of the touchscreen can make calls to the network. Any call to the network made by the application layer is automatically handed off to a local caching proxy, which determines whether the request should be handled locally. Many of the requests from the application layer are web services API requests; although such requests could be satisfied by the iControl servers, they are handled directly by the touchscreen and the gateway. Requests that get through the caching proxy are checked against a white list of acceptable sites, and, if they match, are sent off through the network interface to the gateway. Included in the Network Subsystem is a set of network services including HTTP, HTTPS, and server-level authentication functions to manage the secure client-server interface. Storage and management of certificates is incorporated as a part of the network services layer.

Server components of the integrated security system servers support interactive content services on the touchscreen. These server components include, but are not limited to the content manager, registry manager, network manager, and global registry, each of which is described herein.

The Content Manager oversees aspects of handling widget data and raw content on the touchscreen. Once created and validated by the service provider, widgets are 'ingested' to the Content Manager, and then become available as downloadable services through the integrated security system Content Management APIs. The Content manager maintains versions and timestamp information, and connects to the raw data contained in the backend Content Store database. When a widget is updated (or new content becomes available) all clients registering interest in a widget are systematically updated as needed (a process that can be configured at an account, locale, or system-wide level).

The Registry Manager handles user data, and provisioning accounts, including information about widgets the user has decided to install, and the user preferences for these widgets.

The Network Manager handles getting and setting state for all devices on the integrated security system network (e.g., sensors, panels, cameras, etc.). The Network

manager synchronizes with the gateway, the advanced touchscreen, and the subscriber database.

The Global Registry is a primary starting point server for all client services, and is a logical referral service that abstracts specific server locations/addresses from clients  
5 (touchscreen, gateway 102, desktop widgets, etc.). This approach enables easy scaling/migration of server farms.

The gateway 102 of an embodiment, as described herein, enables couplings or connections and thus the flow of information between various components of the host premises and various types and/or combinations of IP devices, where the components of  
10 the host premises include a network, a security system or subsystem to name a few. Consequently, the gateway 102 controls the association between and the flow of information or data between the components of the host premises. For example, the gateway 102 of an embodiment forms a sub-network coupled to another network (e.g., WAN, LAN, etc.), with the sub-network including IP devices. The gateway further  
15 enables the association of the IP devices of the sub-network with appropriate systems on the premises (e.g., security system, etc.). Therefore, for example, the gateway can form a sub-network of IP devices configured for security functions, and associate the sub-network only with the premises security system, thereby segregating the IP devices dedicated to security from other IP devices that may be coupled to another network on  
20 the premises.

**Figure 8** is a flow diagram for a method 800 of forming a security network including integrated security system components, under an embodiment. Generally, the method comprises coupling 802 a gateway comprising a connection management component to a local area network in a first location and a security server in a second  
25 location. The method comprises forming 804 a security network by automatically establishing a wireless coupling between the gateway and a security system using the connection management component. The security system of an embodiment comprises security system components located at the first location. The method comprises integrating 806 communications and functions of the security system components into the  
30 security network via the wireless coupling.

**Figure 9** is a flow diagram for a method 900 of forming a security network including integrated security system components and network devices, under an embodiment. Generally, the method comprises coupling 902 a gateway to a local area network located in a first location and a security server in a second location. The method  
5 comprises automatically establishing 904 communications between the gateway and security system components at the first location, the security system including the security system components. The method comprises automatically establishing 906 communications between the gateway and premise devices at the first location. The method comprises forming 908 a security network by electronically integrating, via the  
10 gateway, communications and functions of the premise devices and the security system components.

In an example embodiment, **Figure 10** is a flow diagram 1000 for integration or installation of an IP device into a private network environment, under an embodiment. The variables of an embodiment set at time of installation include, but are not limited to,  
15 one or more of a private SSID/Password, an gateway identifier, a security panel identifier, a user account TS, and a Central Monitoring Station account identification.

An embodiment of the IP device discovery and management begins with a user or installer activating 1002 the gateway and initiating 1004 the install mode of the system. This places the gateway in an install mode. Once in install mode, the gateway shifts to a  
20 default (Install) Wifi configuration. This setting will match the default setting for other integrated security system-enabled devices that have been pre-configured to work with the integrated security system. The gateway will then begin to provide 1006 DHCP addresses for these IP devices. Once the devices have acquired a new DHCP address from the gateway, those devices are available for configuration into a new secured Wifi  
25 network setting.

The user or installer of the system selects 1008 all devices that have been identified as available for inclusion into the integrated security system. The user may select these devices by their unique IDs via a web page, Touchscreen, or other client interface. The gateway provides 1010 data as appropriate to the devices. Once selected,  
30 the devices are configured 1012 with appropriate secured Wifi settings, including SSID and WPA/WPA-2 keys that are used once the gateway switches back to the secured

sandbox configuration from the “Install” settings. Other settings are also configured as appropriate for that type of device. Once all devices have been configured, the user is notified and the user can exit install mode. At this point all devices will have been registered 1014 with the integrated security system servers.

5           The installer switches 1016 the gateway to an operational mode, and the gateway instructs or directs 1018 all newly configured devices to switch to the “secured” Wifi sandbox settings. The gateway then switches 1020 to the “secured” Wifi settings. Once the devices identify that the gateway is active on the “secured” network, they request new DHCP addresses from the gateway which, in response, provides 1022 the new addresses.  
10   The devices with the new addresses are then operational 1024 on the secured network.

          In order to ensure the highest level of security on the secured network, the gateway can create or generate a dynamic network security configuration based on the unique ID and private key in the gateway, coupled with a randomizing factor that can be based on online time or other inputs. This guarantees the uniqueness of the gateway  
15   secured network configuration.

          To enable the highest level of performance, the gateway analyzes the RF spectrum of the 802.11x network and determines which frequency band/channel it should select to run.

          An alternative embodiment of the camera/IP device management process  
20   leverages the local ethernet connection of the sandbox network on the gateway. This alternative process is similar to the Wifi discovery embodiment described above, except the user connects the targeted device to the ethernet port of the sandbox network to begin the process. This alternative embodiment accommodates devices that have not been pre-configured with the default “Install” configuration for the integrated security system.

25           This alternative embodiment of the IP device discovery and management begins with the user/installer placing the system into install mode. The user is instructed to attach an IP device to be installed to the sandbox ethernet port of the gateway. The IP device requests a DHCP address from the gateway which, in response to the request, provides the address. The user is presented the device and is asked if he/she wants to  
30   install the device. If yes, the system configures the device with the secured Wifi settings and other device-specific settings (e.g., camera settings for video length, image quality

etc.). The user is next instructed to disconnect the device from the ethernet port. The device is now available for use on the secured sandbox network.

**Figure 11** is a block diagram showing communications among integrated IP devices of the private network environment, under an embodiment. The IP devices of this example include a security touchscreen 1103, gateway 1102 (e.g., “iHub”), and security panel (e.g., “Security Panel 1”, “Security Panel 2”, “Security Panel n”), but the embodiment is not so limited. In alternative embodiments any number and/or combination of these three primary component types may be combined with other components including IP devices and/or security system components. For example, a single device which comprises an integrated gateway, touchscreen, and security panel is merely another embodiment of the integrated security system described herein. The description that follows includes an example configuration that includes a touchscreen hosting particular applications. However, the embodiment is not limited to the touchscreen hosting these applications, and the touchscreen should be thought of as representing any IP device.

Referring to Figure 11, the touchscreen 1103 incorporates an application 1110 that is implemented as computer code resident on the touchscreen operating system, or as a web-based application running in a browser, or as another type of scripted application (e.g., Flash, Java, Visual Basic, etc.). The touchscreen core application 1110 represents this application, providing user interface and logic for the end user to manage their security system or to gain access to networked information or content (Widgets). The touchscreen core application 1110 in turn accesses a library or libraries of functions to control the local hardware (e.g. screen display, sound, LEDs, memory, etc.) as well as specialized librariе(s) to couple or connect to the security system.

In an embodiment of this security system connection, the touchscreen 1103 communicates to the gateway 1102, and has no direct communication with the security panel. In this embodiment, the touchscreen core application 1110 accesses the remote service APIs 1112 which provide security system functionality (e.g. ARM/DISARM panel, sensor state, get/set panel configuration parameters, initiate or get alarm events, etc.). In an embodiment, the remote service APIs 1112 implement one or more of the following functions, but the embodiment is not so limited:

- Armstate = setARMState(type="ARM STAY| ARM AWAY| DISARM",  
Parameters="ExitDelay=30 |Lights=OFF")
- sensorState=getSensors(type="ALL| SensorName | SensorNameList")
- 5     ▪ result = setSensorState(SensorName, parameters="Option1,  
Options2,...Option n")
- interruptHandler =SensorEvent()
- interruptHandler=alarmEvent()

Functions of the remote service APIs 1112 of an embodiment use a remote PanelConnect API 1124 which which resides in memory on the gateway 1102. The  
10 touchscreen 1103 communicates with the gateway 1102 through a suitable network interface such as an Ethernet or 802.11 RF connection, for example. The remote PanelConnect API 1124 provides the underlying Security System Interfaces 1126 used to communicate with and control one or more types of security panel via wired link 1130 and/or RF link 3. The PanelConnect API 1124 provides responses and input to the  
15 remote services APIs 1126, and in turn translates function calls and data to and from the specific protocols and functions supported by a specific implementation of a Security Panel (e.g. a GE Security Simon XT or Honeywell Vista 20P). In an embodiment, the PanelConnect API 1124 uses a 345MHz RF transceiver or receiver hardware/firmware module to communicate wirelessly to the security panel and directly to a set of 345 MHz  
20 RF-enabled sensors and devices, but the embodiment is not so limited.

The gateway of an alternative embodiment communicates over a wired physical coupling or connection to the security panel using the panel's specific wired hardware (bus) interface and the panel's bus-level protocol.

In an alternative embodiment, the Touchscreen 1103 implements the same  
25 PanelConnect API 1114 locally on the Touchscreen 1103, communicating directly with the Security Panel 2 and/or Sensors 2 over the proprietary RF link or over a wired link for that system. In this embodiment the Touchscreen 1103, instead of the gateway 1102, incorporates the 345 MHz RF transceiver to communicate directly with Security Panel 2 or Sensors 2 over the RF link 2. In the case of a wired link the Touchscreen 1103  
30 incorporates the real-time hardware (e.g. a PIC chip and RS232-variant serial link) to

physically connect to and satisfy the specific bus-level timing requirements of the SecurityPanel2.

In yet another alternative embodiment, either the gateway 1102 or the Touchscreen 1103 implements the remote service APIs. This embodiment includes a Cricket device (“Cricket”) which comprises but is not limited to the following components: a processor (suitable for handling 802.11 protocols and processing, as well as the bus timing requirements of SecurityPanel1); an 802.11 (WiFi) client IP interface chip; and, a serial bus interface chip that implements variants of RS232 or RS485, depending on the specific Security Panel.

The Cricket also implements the full PanelConnect APIs such that it can perform the same functions as the case where the gateway implements the PanelConnect APIs. In this embodiment, the touchscreen core application 1110 calls functions in the remote service APIs 1112 (such as setArmState()). These functions in turn couple or connect to the remote Cricket through a standard IP connection (“Cricket IP Link”) (e.g., Ethernet, Homeplug, the gateway’s proprietary Wifi network, etc.). The Cricket in turn implements the PanelConnect API, which responds to the request from the touchscreen core application, and performs the appropriate function using the proprietary panel interface. This interface uses either the wireless or wired proprietary protocol for the specific security panel and/or sensors.

**Figure 12** is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment. Operations begin when the system is powered on 1210, involving at a minimum the power-on of the gateway device, and optionally the power-on of the connection between the gateway device and the remote servers. The gateway device initiates 1220 a software and RF sequence to locate the extant security system. The gateway and installer initiate and complete 1230 a sequence to ‘learn’ the gateway into the security system as a valid and authorized control device. The gateway initiates 1240 another software and RF sequence of instructions to discover and learn the existence and capabilities of existing RF devices within the extant security system, and store this information in the system. These operations under the system of an embodiment are described in further detail below.

Unlike conventional systems that extend an existing security system, the system of an embodiment operates utilizing the proprietary wireless protocols of the security system manufacturer. In one illustrative embodiment, the gateway is an embedded computer with an IP LAN and WAN connection and a plurality of RF transceivers and software protocol modules capable of communicating with a plurality of security systems each with a potentially different RF and software protocol interface. After the gateway has completed the discovery and learning of sensors and has been integrated as a virtual control device in the extant security system, the system becomes operational. Thus, the security system and associated sensors are presented as accessible devices to a potential plurality of user interface subsystems.

The system of an embodiment integrates the functionality of the extant security system with other non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms, which may be controlled via RF, wired, or powerline-based networking mechanisms supported by the gateway or servers.

The system of an embodiment provides a user interface subsystem enabling a user to monitor, manage, and control the system and associated sensors and security systems. In an embodiment of the system, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX/Flash presentation of a monitoring and control application, enabling users to view the state of all sensors and controllers in the extant security system from a web browser or equivalent operating on a computer, PDA, mobile phone, or other consumer device.

In another illustrative embodiment of the system described herein, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX presentation of a monitoring and control application, enabling users to combine the monitoring and control of the extant security system and sensors with the monitoring and control of non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms.

In another illustrative embodiment of the system described herein, a user interface subsystem is a mobile phone application enabling users to monitor and control the extant security system as well as other non-security devices.



In another illustrative embodiment of the system described herein, a user interface subsystem is an application running on a keypad or touchscreen device enabling users to monitor and control the extant security system as well as other non-security devices.

In another illustrative embodiment of the system described herein, a user interface  
5 subsystem is an application operating on a TV or set-top box connected to a TV enabling users to monitor and control the extant security system as well as other non-security devices.

**Figure 13** is a block diagram of an integrated security system 1300 wirelessly interfacing to proprietary security systems, under an embodiment. A security system  
10 1310 is coupled or connected to a Gateway 1320, and from Gateway 1320 coupled or connected to a plurality of information and content sources across a network 1330 including one or more web servers 1340, system databases 1350, and applications servers 1360. While in one embodiment network 1330 is the Internet, including the World Wide Web, those of skill in the art will appreciate that network 1330 may be any type of  
15 network, such as an intranet, an extranet, a virtual private network (VPN), a mobile network, or a non- TCP/IP based network.

Moreover, other elements of the system of an embodiment may be conventional, well-known elements that need not be explained in detail herein. For example, security system 1310 could be any type home or business security system, such devices including  
20 but not limited to a standalone RF home security system or a non-RF-capable wired home security system with an add-on RF interface module. In the example of Figure 13, security system 1310 includes an RF-capable wireless security panel (WSP) 1311 that acts as the master controller for security system 1310. Well-known examples of such a WSP include the GE Security Concord, Networx, and Simon panels, the Honeywell Vista  
25 and Lynx panels, and similar panesl from DSC and Napco, to name a few. A wireless module 1314 includes the RF hardware and protocol software necessary to enable communication with and control of a plurality of wireless devices 1313. WSP 1311 may also manage wired devices 1314 physically connected to WSP 1311 with an RS232 or RS485 or Ethernet connection or similar such wired interface.

30 In an implementation consistent with the systems and methods described herein, Gateway 1320 provides the interface between security system 1310 and LAN and/or

WAN for purposes of remote control, monitoring, and management. Gateway 1320 communicates with an external web server 1340, database 1350, and application server 1360 over network 1330 (which may comprise WAN, LAN, or a combination thereof). In this example system, application logic, remote user interface functionality, as well as user state and account are managed by the combination of these remote servers. Gateway 5 1320 includes server connection manager 1321, a software interface module responsible for all server communication over network 1330. Event manager 1322 implements the main event loop for Gateway 1320, processing events received from device manager 1324 (communicating with non-security system devices including but not limited to IP 10 cameras, wireless thermostats, or remote door locks). Event manager 1322 further processes events and control messages from and to security system 1310 by utilizing WSP manager 1323.

WSP manager 1323 and device manager 1324 both rely upon wireless protocol manager 1326 which receives and stores the proprietary or standards-based protocols 15 required to support security system 1310 as well as any other devices interfacing with gateway 1320. WSP manager 1323 further utilizes the comprehensive protocols and interface algorithms for a plurality of security systems 1310 stored in the WSP DB client database associated with wireless protocol manager 1326. These various components implement the software logic and protocols necessary to communicate with and manager 20 devices and security systems 1310. Wireless Transceiver hardware modules 1325 are then used to implement the physical RF communications link to such devices and security systems 1310. An illustrative wireless transceiver 1325 is the GE Security Dialog circuit board, implementing a 319.5MHz two-way RF transceiver module. In this example, RF Link 1370 represents the 319.5MHz RF communication link, enabling 25 gateway 1320 to monitor and control WSP 1311 and associated wireless and wired devices 1313 and 1314, respectively.

In one embodiment, server connection manager 1321 requests and receives a set of wireless protocols for a specific security system 1310 (an illustrative example being that of the GE Security Concord panel and sensors) and stores them in the WSP DB 30 portion of the wireless protocol manager 1326. WSP manager 1323 then utilizes such protocols from wireless protocol manager 1326 to initiate the sequence of processes

detailed in Figure 12 and Figure 13 for learning gateway 1320 into security system 1310 as an authorized control device. Once learned in, as described with reference to Figure 13 (and above), event manager 1322 processes all events and messages detected by the combination of WSP manager 1323 and the GE Security wireless transceiver module  
5 1325.

In another embodiment, gateway 1320 incorporates a plurality of wireless transceivers 1325 and associated protocols managed by wireless protocol manager 1326. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP 1311, wireless devices 1313, and wired devices 1314. For  
10 example a wireless sensor from one manufacturer may be utilized to control a device using a different protocol from a different manufacturer.

In another embodiment, gateway 1320 incorporates a wired interface to security system 1310, and incorporates a plurality of wireless transceivers 1325 and associated protocols managed by wireless protocol manager 1326. In this embodiment events and  
15 control of multiple heterogeneous devices may be coordinated with WSP 1311, wireless devices 1313, and wired devices 1314.

Of course, while an illustrative embodiment of an architecture of the system of an embodiment is described in detail herein with respect to Figure 13, one of skill in the art will understand that modifications to this architecture may be made without departing  
20 from the scope of the description presented herein. For example, the functionality described herein may be allocated differently between client and server, or amongst different server or processor-based components. Likewise, the entire functionality of the gateway 1320 described herein could be integrated completely within an existing security system 1310. In such an embodiment, the architecture could be directly integrated with a  
25 security system 1310 in a manner consistent with the currently described embodiments.

**Figure 14** is a flow diagram for wirelessly ‘learning’ the Gateway into an existing security system and discovering extant sensors, under an embodiment. The learning interfaces gateway 1320 with security system 1310. Gateway 1320 powers up 1410 and initiates software sequences 1420 and 1425 to identify accessible WSPs 1311 and  
30 wireless devices 1313, respectively (e.g., one or more WSPs and/or devices within range of gateway 1320). Once identified, WSP 1311 is manually or automatically set into

'learn mode' 1430, and gateway 1320 utilizes available protocols to add 1440 itself as an authorized control device in security system 1310. Upon successful completion of this task, WSP 1311 is manually or automatically removed from 'learn mode' 1450.

5 Gateway 1320 utilizes the appropriate protocols to mimic 1460 the first identified device 1314. In this operation gateway 1320 identifies itself using the unique or pseudo-unique identifier of the first found device 1314, and sends an appropriate change of state message over RF Link 1370. In the event that WSP 1311 responds to this change of state message, the device 1314 is then added 1470 to the system in database 1350. Gateway 1320 associates 1480 any other information (such as zone name or token-based identifier) 10 with this device 1314 in database 1350, enabling gateway 1320, user interface modules, or any application to retrieve this associated information.

In the event that WSP 1311 does not respond to the change of state message, the device 1314 is not added 1470 to the system in database 1350, and this device 1314 is identified as not being a part of security system 1310 with a flag, and is either ignored or 15 added as an independent device, at the discretion of the system provisioning rules. Operations hereunder repeat 1485 operations 1460, 1470, 1480 for all devices 1314 if applicable. Once all devices 1314 have been tested in this way, the system begins operation 1490.

In another embodiment, gateway 1320 utilizes a wired connection to WSP 1311, 20 but also incorporates a wireless transceiver 1325 to communicate directly with devices 1314. In this embodiment, operations under 1420 above are removed, and operations under 1440 above are modified so the system of this embodiment utilizes wireline protocols to add itself as an authorized control device in security system 1310.

A description of an example embodiment follows in which the Gateway (Figure 25 13, element 1320) is the iHub available from iControl Networks, Palo Alto, CA, and described in detail herein. In this example the gateway is "automatically" installed with a security system.

The automatic security system installation begins with the assignment of an authorization key to components of the security system (e.g., gateway, kit including the 30 gateway, etc.). The assignment of an authorization key is done in lieu of creating a user account. An installer later places the gateway in a user's premises along with the

premises security system. The installer uses a computer to navigate to a web portal (e.g., integrated security system web interface), logs in to the portal, and enters the authorization key of the installed gateway into the web portal for authentication. Once authenticated, the gateway automatically discovers devices at the premises (e.g., sensors, cameras, light controls, etc.) and adds the discovered devices to the system or “network”. The installer assigns names to the devices, and tests operation of the devices back to the server (e.g., did the door open, did the camera take a picture, etc.). The security device information is optionally pushed or otherwise propagated to a security panel and/or to the server network database. The installer finishes the installation, and instructs the end user on how to create an account, username, and password. At this time the user enters the authorization key which validates the account creation (uses a valid authorization key to associate the network with the user’s account). New devices may subsequently be added to the security network in a variety of ways (e.g., user first enters a unique ID for each device/sensor and names it in the server, after which the gateway can automatically discover and configure the device).

A description of another example embodiment follows in which the security system (Figure 13, element 1310) is a Dialog system and the WSP (Figure 13, element 1311) is a SimonXT available from General Electric Security, and the Gateway (Figure 13, element 1320) is the iHub available from iControl Networks, Palo Alto, CA, and described in detail herein. Descriptions of the install process for the SimonXT and iHub are also provided below.

GE Security’s Dialog network is one of the most widely deployed and tested wireless security systems in the world. The physical RF network is based on a 319.5 MHz unlicensed spectrum, with a bandwidth supporting up to 19Kbps communications. Typical use of this bandwidth –even in conjunction with the integrated security system— is far less than that. Devices on this network can support either one-way communication (either a transmitter or a receiver) or two-way communication (a transceiver). Certain GE Simon, Simon XT, and Concord security control panels incorporate a two-way transceiver as a standard component. The gateway also incorporates the same two-way transceiver card. The physical link layer of the network is managed by the transceiver

module hardware and firmware, while the coded payload bitstreams are made available to the application layer for processing.

Sensors in the Dialog network typically use a 60-bit protocol for communicating with the security panel transceiver, while security system keypads and the gateway use the encrypted 80-bit protocol. The Dialog network is configured for reliability, as well as  
5 low-power usage. Many devices are supervised, i.e. they are regularly monitored by the system 'master' (typically a GE security panel), while still maintaining excellent power usage characteristics. A typical door window sensor has a battery life in excess of 5-7 years.

10 The gateway has two modes of operation in the Dialog network: a first mode of operation is when the gateway is configured or operates as a 'slave' to the GE security panel; a second mode of operation is when the gateway is configured or operates as a 'master' to the system in the event a security panel is not present. In both configurations, the gateway has the ability to 'listen' to network traffic, enabling the gateway to  
15 continually keep track of the status of all devices in the system. Similarly, in both situations the gateway can address and control devices that support setting adjustments (such as the GE wireless thermostat).

In the configuration in which the gateway acts as a 'slave' to the security panel, the gateway is 'learned into' the system as a GE wireless keypad. In this mode of  
20 operation, the gateway emulates a security system keypad when managing the security panel, and can query the security panel for status and 'listen' to security panel events (such as alarm events).

The gateway incorporates an RF Transceiver manufactured by GE Security, but is not so limited. This transceiver implements the Dialog protocols and handles all network  
25 message transmissions, receptions, and timing. As such, the physical, link, and protocol layers of the communications between the gateway and any GE device in the Dialog network are totally compliant with GE Security specifications.

At the application level, the gateway emulates the behavior of a GE wireless keypad utilizing the GE Security 80-bit encrypted protocol, and only supported protocols  
30 and network traffic are generated by the gateway. Extensions to the Dialog RF protocol of an embodiment enable full control and configuration of the panel, and iControl can

both automate installation and sensor enrollment as well as direct configuration downloads for the panel under these protocol extensions.

As described above, the gateway participates in the GE Security network at the customer premises. Because the gateway has intelligence and a two-way transceiver, it can ‘hear’ all of the traffic on that network. The gateway makes use of the periodic sensor updates, state changes, and supervisory signals of the network to maintain a current state of the premises. This data is relayed to the integrated security system server (e.g., Figure 2, element 260) and stored in the event repository for use by other server components. This usage of the GE Security RF network is completely non-invasive; there is no new data traffic created to support this activity.

The gateway can directly (or indirectly through the Simon XT panel) control two-way devices on the network. For example, the gateway can direct a GE Security Thermostat to change its setting to ‘Cool’ from ‘Off’, as well as request an update on the current temperature of the room. The gateway performs these functions using the existing GE Dialog protocols, with little to no impact on the network; a gateway device control or data request takes only a few dozen bytes of data in a network that can support 19 Kbps.

By enrolling with the Simon XT as a wireless keypad, as described herein, the gateway includes data or information of all alarm events, as well as state changes relevant to the security panel. This information is transferred to the gateway as encrypted packets in the same way that the information is transferred to all other wireless keypads on the network.

Because of its status as an authorized keypad, the gateway can also initiate the same panel commands that a keypad can initiate. For example, the gateway can arm or disarm the panel using the standard Dialog protocol for this activity. Other than the monitoring of standard alarm events like other network keypads, the only incremental data traffic on the network as a result of the gateway is the infrequent remote arm/disarm events that the gateway initiates, or infrequent queries on the state of the panel.

The gateway is enrolled into the Simon XT panel as a ‘slave’ device which, in an embodiment, is a wireless keypad. This enables the gateway for all necessary functionality for operating the Simon XT system remotely, as well as combining the

actions and information of non-security devices such as lighting or door locks with GE Security devices. The only resource taken up by the gateway in this scenario is one wireless zone (sensor ID).

5 The gateway of an embodiment supports three forms of sensor and panel enrollment/installation into the integrated security system, but is not limited to this number of enrollment/installation options. The enrollment/installation options of an embodiment include installer installation, kitting, and panel, each of which is described below.

10 Under the installer option, the installer enters the sensor IDs at time of installation into the integrated security system web portal or iScreen. This technique is supported in all configurations and installations.

Kits can be pre-provisioned using integrated security system provisioning applications when using the kitting option. At kitting time, multiple sensors are automatically associated with an account, and at install time there is no additional work  
15 required.

In the case where a panel is installed with sensors already enrolled (i.e. using the GE Simon XT enrollment process), the gateway has the capability to automatically extract the sensor information from the system and incorporate it into the user account on the integrated security system server.

20 The gateway and integrated security system of an embodiment uses an auto-learn process for sensor and panel enrollment in an embodiment. The deployment approach of an embodiment can use additional interfaces that GE Security is adding to the Simon XT panel. With these interfaces, the gateway has the capability to remotely enroll sensors in the panel automatically. The interfaces include, but are not limited to, the following:  
25 EnrollDevice(ID, type, name, zone, group); SetDeviceParameters(ID, type, Name, zone, group), GetDeviceParameters(zone); and RemoveDevice(zone).

The integrated security system incorporates these new interfaces into the system, providing the following install process. The install process can include integrated security system logistics to handle kitting and pre-provisioning. Pre-kitting and logistics  
30 can include a pre-provisioning kitting tool provided by integrated security system that enables a security system vendor or provider (“provider”) to offer pre-packaged initial



'kits'. This is not required but is recommended for simplifying the install process. This example assumes a 'Basic' kit is preassembled and includes one (1) Simon XT, three (3) Door/ window sensors, one (1) motion sensor, one (1) gateway, one (1) keyfob, two (2) cameras, and ethernet cables. The kit also includes a sticker page with all Zones (1-24) and Names (full name list).

The provider uses the integrated security system kitting tool to assemble 'Basic' kit packages. The contents of different types of starter kits may be defined by the provider. At the distribution warehouse, a worker uses a bar code scanner to scan each sensor and the gateway as it is packed into the box. An ID label is created that is attached to the box. The scanning process automatically associates all the devices with one kit, and the new ID label is the unique identifier of the kit. These boxes are then sent to the provider for distribution to installer warehouses. Individual sensors, cameras, etc. are also sent to the provider installer warehouse. Each is labeled with its own barcode/ ID.

An installation and enrollment procedure of a security system including an gateway is described below as one example of the installation process.

#### 1. Order and Physical Install Process

- a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the provider for assignment to an installer.
- b. The assigned installer picks up his/her ticket(s) and fills his/her truck with Basic and/or Advanced starter kits. He/she also keeps a stock of individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.
- c. The installer arrives at the address on the ticket, and pulls out the Basic kit. The installer determines sensor locations from a tour of the premises and discussion with the homeowner. At this point assume the homeowner requests additional equipment including an extra camera, two (2) additional door/window sensors, one (1) glass break detector, and one (1) smoke detector.
- d. Installer mounts SimonXT in the kitchen or other location in the home as directed by the homeowner, and routes the phone line to Simon XT if available. GPRS and Phone numbers pre-programmed in SimonXT to point to the provider Central Monitoring Station (CMS).
- e. Installer places iHub in the home in the vicinity of a router and cable modem. Installer installs an ethernet line from iHub to router and plugs iHub into an electrical outlet.

2. Associate and Enroll iHub into SimonXT

- a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with installer ID/pass.
- 5 b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer for kit ID (on box's barcode label).
- c. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add iHub as a wireless keypad. It is noted that this step is for security only and can be automated in an embodiment.
- 10 d. Installer enters the installer code into the Simon XT. Installer Learns 'iHub' into the panel as a wireless keypad as a group 1 device.
- e. Installer goes back to Web portal, and clicks the 'Finished Adding SimonXT' button.

3. Enroll Sensors into SimonXT via iControl

- 15 a. All devices in the Basic kit are already associated with the user's account.
- b. For additional devices, Installer clicks 'Add Device' and adds the additional camera to the user's account (by typing in the camera ID/Serial #).
- c. Installer clicks 'Add Device' and adds other sensors (two (2) door/window sensors, one (1) glass break sensor, and one (1) smoke sensor) to the account (e.g., by typing in IDs).
- 20 d. As part of Add Device, Installer assigns zone, name, and group to the sensor. Installer puts appropriate Zone and Name sticker on the sensor temporarily.
- 25 e. All sensor information for the account is pushed or otherwise propagated to the iConnect server, and is available to propagate to CMS automation software through the CMS application programming interface (API).
- f. Web interface displays 'Installing Sensors in System....' and automatically adds all of the sensors to the Simon XT panel through the GE RF link.
- 30 g. Web interface displays 'Done Installing' --> all sensors show green.

4. Place and Tests Sensors in Home

- a. Installer physically mounts each sensor in its desired location, and removes the stickers.
- 35 b. Installer physically mounts WiFi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
- c. Installer goes to Web interface and is prompted for automatic camera install. Each camera is provisioned as a private, encrypted Wifi device on the iHub secured sandbox network, and firewall NAT traversal is initiated. Upon completion the customer is prompted to test the security system.
- 40 d. Installer selects the 'Test System' button on the web portal -- the SimonXT is put into Test mode by the iHub over GE RF.

- e. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.
  - f. iHub sends test data directly to CMS over broadband link, as well as storing the test data in the user's account for subsequent report generation.
  - 5 g. Installer exits test mode from the Web portal.
5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the iControl web and mobile portals. Customer creates a username/password at this time.
  - 10 6. Installer instructs customer how to change Simon XT user code from the Web interface. Customer changes user code which is pushed to SimonXT automatically over GE RF.

An installation and enrollment procedure of a security system including an gateway is described below as an alternative example of the installation process. This  
15 installation process is for use for enrolling sensors into the SimonXT and integrated security system and is compatible with all existing GE Simon panels.

The integrated security system supports all pre-kitting functionality described in the installation process above. However, for the purpose of the following example, no  
20 kitting is used.

#### 1. Order and Physical Install Process

- a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the security system provider for assignment to an installer.
- 25 b. The assigned installer picks up his/her ticket(s) and fills his/her truck with individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.
- c. The installer arrives at the address on the ticket, and analyzes the house and talks with the homeowner to determine sensor locations. At this point  
30 assume the homeowner requests three (3) cameras, five (5) door/window sensors, one (1) glass break detector, one (1) smoke detector, and one (1) keyfob.
- d. Installer mounts SimonXT in the kitchen or other location in the home. The installer routes a phone line to Simon XT if available. GPRS and  
35 Phone numbers are pre-programmed in SimonXT to point to the provider CMS.
- e. Installer places iHub in home in the vicinity of a router and cable modem, and installs an ethernet line from iHub to the router, and plugs iHub into an electrical outlet.

2. Associate and Enroll iHub into SimonXT

- 5
- a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with an installer ID/pass.
  - b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer to add devices.
  - c. Installer types in ID of iHub, and it is associated with the user's account.
  - d. Installer clicks 'Add Device' and adds the cameras to the user's account (by
  - 10 typing in the camera ID/Serial #).
  - e. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add iHub as a wireless keypad.
  - f. Installer goes to Simon XT and enters the installer code into the Simon XT. Learns 'iHub' into the panel as a wireless keypad as group 1 type
  - 15 sensor.
  - g. Installer returns to Web portal, and clicks the 'Finished Adding SimonXT' button.
  - h. iHub now is alerted to all subsequent installs over the security system RF.

3. Enroll Sensors into SimonXT via iControl

- 20
- a. Installer clicks 'Add Simon XT Sensors' -- Displays instructions for adding sensors to Simon XT.
  - b. Installer goes to Simon XT and uses Simon XT install process to add each sensor, assigning zone, name, group. These assignments are recorded for later use.
  - 25 c. The iHub automatically detects each sensor addition and adds the new sensor to the integrated security system.
  - d. Installer exits install mode on the Simon XT, and returns to the Web portal.
  - e. Installer clicks 'Done Adding Devices'.
  - 30 f. Installer enters zone/sensor naming from recorded notes into integrated security system to associate sensors to friendly names.
  - g. All sensor information for the account is pushed to the iConnect server, and is available to propagate to CMS automation software through the
  - 35 CMS API.

4. Place and Tests Sensors in Home

- 40
- a. Installer physically mounts each sensor in its desired location.
  - b. Installer physically mounts Wifi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
  - c. Installer puts SimonXT into Test mode from the keypad.
  - 45 d. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.

- e. Installer exits test mode from the Simon XT keypad.
  - f. Installer returns to web interface and is prompted to automatically set up cameras. After waiting for completion cameras are now provisioned and operational.
- 5 5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the integrated security system web and mobile portals. Customer creates a username/password at this time.
  6. Customer and Installer observe that all sensors/cameras are green.
  7. Installer instructs customer how to change Simon XT user code from the keypad.
  - 10 8. Customer changes user code and stores in SimonXT.
  8. The first time the customer uses the web portal to Arm/Disarm system the web interface prompts the customer for the user code, which is then stored securely on the server. In the event the user code is changed on the panel the web interface once again prompts the customer.

15

The panel of an embodiment can be programmed remotely. The CMS pushes new programming to SimonXT over a telephone or GPRS link. Optionally, iControl and GE provide a broadband link or coupling to the gateway and then a link from the gateway to the Simon XT over GE RF.

20

As described above, computer networks suitable for use with the embodiments described herein include local area networks (LAN), wide area networks (WAN), Internet, or other connection services and network variations such as the world wide web, the public internet, a private internet, a private computer network, a public network, a mobile network, a cellular network, a value-added network, and the like. Computing devices coupled or connected to the network may be any microprocessor controlled device that permits access to the network, including terminal devices, such as personal computers, workstations, servers, mini computers, main-frame computers, laptop computers, mobile computers, palm top computers, hand held computers, mobile phones, TV set-top boxes, or combinations thereof. The computer network may include one of

25

30 more LANs, WANs, Internets, and computers. The computers may serve as servers, clients, or a combination thereof.

35

The integrated security system can be a component of a single system, multiple systems, and/or geographically separate systems. The integrated security system can also be a subcomponent or subsystem of a single system, multiple systems, and/or geographically separate systems. The integrated security system can be coupled to one or

more other components (not shown) of a host system or a system coupled to the host system.

One or more components of the integrated security system and/or a corresponding system or application to which the integrated security system is coupled or connected includes and/or runs under and/or in association with a processing system. The processing system includes any collection of processor-based devices or computing devices operating together, or components of processing systems or devices, as is known in the art. For example, the processing system can include one or more of a portable computer, portable communication device operating in a communication network, and/or a network server. The portable computer can be any of a number and/or combination of devices selected from among personal computers, personal digital assistants, portable computing devices, and portable communication devices, but is not so limited. The processing system can include components within a larger computer system.

The processing system of an embodiment includes at least one processor and at least one memory device or subsystem. The processing system can also include or be coupled to at least one database. The term “processor” as generally used herein refers to any logic processing unit, such as one or more central processing units (CPUs), digital signal processors (DSPs), application-specific integrated circuits (ASIC), etc. The processor and memory can be monolithically integrated onto a single chip, distributed among a number of chips or components, and/or provided by some combination of algorithms. The methods described herein can be implemented in one or more of software algorithm(s), programs, firmware, hardware, components, circuitry, in any combination.

The components of any system that includes the integrated security system can be located together or in separate locations. Communication paths couple the components and include any medium for communicating or transferring files among the components. The communication paths include wireless connections, wired connections, and hybrid wireless/wired connections. The communication paths also include couplings or connections to networks including local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), proprietary networks, interoffice or backend networks, and the Internet. Furthermore, the communication paths include

removable fixed mediums like floppy disks, hard disk drives, and CD-ROM disks, as well as flash RAM, Universal Serial Bus (USB) connections, RS-232 connections, telephone lines, buses, and electronic mail messages.

5 Embodiments of the integrated security system include a system comprising: a gateway located at a first location; a connection management component coupled to the gateway, the connection management component automatically establishing a wireless coupling with a security system installed at the first location, the security system including security system components, wherein the connection management component forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling; and a security server at a second location different from the first location, wherein security server is coupled to the gateway.

15 The gateway of an embodiment is connected to a local area network at the first location, and the local area network is coupled to a wide area network via a router at the first location.

The gateway of an embodiment is coupled to a wide area network and is coupled to a local area network at the first location via the connection management component and a router at the first location.

The gateway of an embodiment is coupled to the security server via the internet.

20 The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user.

25 The system of an embodiment comprises a portal coupled to the gateway, wherein the portal provides access to the communications and the functions of the security network via remote client devices.

The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network from the remote client devices.

30 The remote client devices of an embodiment include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

The gateway of an embodiment including the connection management component automatically discovers the security system components.

The gateway of an embodiment includes protocols of the security system from the security server and uses the protocols to discover the security system components.

5 The gateway of an embodiment requests and receives protocols of the security system from the security server, wherein the gateway uses the protocols received to discover the security system components.

10 The gateway of an embodiment including the connection management component automatically establishes and controls the communications with the security system components.

The gateway of an embodiment including the connection management component automatically establishes a coupling with the security system including the security system components.

15 The gateway of an embodiment includes a rules component that manages rules of interaction between the gateway and the security system components.

The gateway of an embodiment includes a device connect component that includes definitions of the security system components.

20 The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

25 The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The secondary communication link of an embodiment includes a broadband coupling.

30 The secondary communication link of an embodiment includes a General Packet Radio Service (GPRS) coupling.



The gateway of an embodiment transmits messages comprising event data of the security system components to remote client devices over the secondary communication link.

5 The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The gateway of an embodiment receives control data for control of the security system components from remote client devices via the secondary communication link.

10 The security network of an embodiment comprises network devices coupled to the gateway via a wireless coupling.

The gateway of an embodiment including the connection management component automatically discovers the network devices.

The gateway of an embodiment including the connection management component automatically installs the network devices in the security network.

15 The gateway of an embodiment including the connection management component automatically configures the network devices for operation in the security network.

The gateway of an embodiment controls communications between the network devices, the security system components, and the security server.

20 The gateway of an embodiment including the connection management component transmits event data of the network devices to remote client devices over at least one of a plurality of communication links.

The gateway of an embodiment receives control data for control of the network devices from remote client devices via at least one of the plurality of communication links.

25 The event data of an embodiment comprises changes in device states of the network devices, data of the network devices, and data received by the network devices.

The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary  
30 communication link.

The gateway of an embodiment transmits event data of the network devices to the central monitoring station over the secondary communication link.

The secondary communication link of an embodiment includes a broadband coupling.

5 The secondary communication link of an embodiment includes a General Packet Radio Service (GPRS) coupling.

The gateway of an embodiment transmits messages comprising event data of the network devices to remote client devices over the secondary communication link.

10 The security server of an embodiment creates, modifies and terminates couplings between the gateway and the network devices.

The security server of an embodiment performs creation, modification, deletion and configuration of the network devices.

The security server of an embodiment creates automations, schedules and notification rules associated with the network devices.

15 The security server of an embodiment manages access to current and logged state data for the network devices.

The security server of an embodiment manages access to current and logged state data for couplings between the gateway and the network devices.

20 The security server of an embodiment manages communications with the network devices.

The network device of an embodiment is an Internet Protocol device.

The network device of an embodiment is a camera.

The network device of an embodiment is a touchscreen.

25 The network device of an embodiment is a device controller that controls an attached device.

The network device of an embodiment is a sensor.

The security server of an embodiment creates, modifies and terminates users corresponding to the security system.

30 The security server of an embodiment creates, modifies and terminates couplings between the gateway and the security system components.

The security server of an embodiment performs creation, modification, deletion and configuration of the security system components.

The security server of an embodiment creates automations, schedules and notification rules associated with the security system components.

5 The security server of an embodiment manages access to current and logged state data for the security system components.

The security server of an embodiment manages access to current and logged state data for couplings between the gateway and the security system components.

10 The security server of an embodiment manages communications with the security system components.

The security server of an embodiment generates and transfers notifications to remote client devices, the notifications comprising event data.

The notifications of an embodiment include one or more of short message service messages and electronic mail messages.

15 The event data of an embodiment is event data of the security system components.

The security server of an embodiment transmits event data of the security system components to a central monitoring station of the security system over the secondary communication link.

20 The security system components of an embodiment include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.

Embodiments of the integrated security system include a security network comprising: a gateway including a connection management component located at a first location, the connection management component automatically establishing a wireless coupling with a security system installed at the first location, the security system including security system components, wherein the connection management component forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling; and a security server at a second location different from the first location, wherein security server is coupled to the gateway and includes a plurality of security network applications.

30 Embodiments of the integrated security system include a security network comprising: a gateway including a connection management component located at a first

location; a wireless coupling between the gateway and a security system installed at the first location, wherein the security system includes a plurality of security system components that are proprietary to the security system, the connection management component automatically establishing the wireless coupling with the security system components and forming a security network that integrates communications and functions of the security system components into the security network; and an interface coupled to the gateway, the interface providing communications with the security network and control of the functions of the security network from a remote client device.

Embodiments of the integrated security system include a system comprising: a security network comprising a gateway coupled to a security system and located at a first location, the security system including a plurality of security system components, the security network comprising a plurality of premise devices coupled to the gateway, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components; and a security server located at a second location different from the first location, the security server coupled to the security network via the gateway.

The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user.

The system of an embodiment comprises a portal coupled to the gateway, wherein the portal provides access to the communications and the functions of the security network via remote client devices.

The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network from the remote client devices.

The remote client devices of an embodiment include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

The gateway of an embodiment automatically discovers the security system components.

The gateway of an embodiment includes protocols of the security system from the security server and uses the protocols to discover the security system components.

The gateway of an embodiment requests and receives protocols of the security system from the security server, wherein the gateway uses the protocols received to discover the security system components.

5 The gateway of an embodiment automatically establishes the communications with the security system components.

The gateway of an embodiment includes a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components.

10 The connection management component of an embodiment automatically discovers the premise devices.

The connection management component of an embodiment automatically installs the premise devices in the security network.

The connection management component of an embodiment automatically configures the premise devices for operation in the security network.

15 The gateway of an embodiment includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices.

The gateway of an embodiment includes a device connect component that includes definitions of the security system components and the premise devices.

20 The gateway of an embodiment is connected to a premise local area network, and the premise local area network is coupled to a wide area network via a premise router/firewall.

The gateway of an embodiment is coupled to premise local area network via a premise router/firewall, and the gateway is coupled to a wide area network.

25 The gateway of an embodiment is coupled to the premise devices using a wireless coupling.

The gateway of an embodiment is coupled to the security server via the internet.

The gateway of an embodiment is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at  
30 a third location different from the first location and the second location.

The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link.

5           The gateway of an embodiment transmits event data of the security system components and the premise devices to the central monitoring station over the secondary communication link.

10           The event data of an embodiment comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

The gateway of an embodiment transmits event data of the security system to the central monitoring station over the secondary communication link when the primary communication link is unavailable.

15           The secondary communication link of an embodiment includes a broadband coupling.

The secondary communication link of an embodiment includes a General Packet Radio Service (GPRS) coupling.

20           The gateway of an embodiment transmits messages comprising event data of the security system components and the premise devices to remote client devices over the secondary communication link.

25           The event data of an embodiment comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

The security server of an embodiment creates, modifies and terminates users corresponding to the security system.

The security server of an embodiment creates, modifies and terminates couplings between the gateway and the security system components.

30           The security server of an embodiment creates, modifies and terminates couplings between the gateway and the premise devices.

The security server of an embodiment performs creation, modification, deletion and configuration of the security system components.

The security server of an embodiment performs creation, modification, deletion and configuration of the premise devices.

5 The security server of an embodiment creates automations, schedules and notification rules associated with the security system components.

The security server of an embodiment creates automations, schedules and notification rules associated with the premise devices.

10 The security server of an embodiment manages access to current and logged state data for the security system components.

The security server of an embodiment manages access to current and logged state data for the premise devices.

15 The security server of an embodiment manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices.

The security server of an embodiment manages communications with the security system components.

The security server of an embodiment manages communications with the premise devices.

20 The security server of an embodiment generates and transfers notifications to remote client devices, the notifications comprising event data.

The notifications of an embodiment include one or more of short message service messages and electronic mail messages.

The event data of an embodiment is event data of the security system components.

25 The event data of an embodiment is event data of the premise devices.

The security server of an embodiment transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link.

30 The security system components of an embodiment include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.

The premise device of an embodiment is an Internet Protocol device.

The premise device of an embodiment is a camera.

The premise device of an embodiment is a touchscreen.

The premise device of an embodiment is a device controller that controls an attached device.

5 The premise device of an embodiment is a sensor.

Embodiments of the integrated security system include a system comprising: a security network comprising a gateway coupled to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location; and a plurality of  
10 premise devices located at the first location and coupled to the gateway, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the security network.

Embodiments of the integrated security system include a security network  
15 comprising: a gateway, wherein the gateway is coupled to a security system that includes a plurality of security system components that are proprietary to the security system; a plurality of network devices coupled to the gateway, wherein the gateway forms a premise security network at a first location and couples the premise security network to a local area network of the first location, wherein the gateway forms the premise security  
20 network by electronically integrating communications and functions of the plurality of network devices and the security system components; and an application server located at a second location different from the first location, the application server coupled to the premise security network via the gateway and a communication network.

Embodiments of the integrated security system include a system comprising: a  
25 security network comprising a gateway coupled to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location; a plurality of premise devices located at the first location and coupled to the gateway, wherein the  
30 gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the security network; and an



interface coupled to the gateway, the interface providing communications with the security network and control of the functions of the security system components and the premise devices from a remote client device.

Embodiments of the integrated security system include a method comprising:  
5 coupling a gateway comprising a connection management component to a local area network located in a first location and a security server in a second location; and forming a security network by automatically establishing a wireless coupling between the gateway and a security system using the connection management component, the security system comprising a plurality of security system components located at the first location,  
10 wherein forming the security network includes integrating communications and functions of the security system components into the security network via the wireless coupling.

The method of an embodiment comprises coupling the gateway to a local area network at the first location, wherein the local area network is coupled to a wide area network via a router at the first location.

15 The gateway of an embodiment is coupled to a wide area network and is coupled to a local area network at the first location via the connection management component and a router at the first location.

The gateway of an embodiment is coupled to the security server via the internet.

20 The method of an embodiment comprises providing an interface of the security network, wherein the interface allows control of the functions of the security network by a user.

The method of an embodiment comprises providing access to the communications and the functions of the security network via remote client devices and a portal coupled to the gateway.

25 The method of an embodiment comprises providing an interface coupled to the security network, wherein the interface allows control of the functions of the security network from the remote client devices.

The remote client devices of an embodiment include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

30 The gateway of an embodiment automatically discovers the security system components.

The method of an embodiment comprises using protocols of the security system to discover the security system components, wherein the gateway includes the protocols.

5 The method of an embodiment comprises requesting and receiving protocols of the security system from the security server, wherein the gateway receives and uses the protocols to discover the security system components.

The method of an embodiment comprises automatically establishing and controlling the communications with the security system components using the gateway.

10 The gateway of an embodiment including the connection management component automatically establishes a coupling with the security system including the security system components.

The gateway of an embodiment includes a rules component that manages rules of interaction between the gateway and the security system components.

The gateway of an embodiment includes a device connect component that includes definitions of the security system components.

15 The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

20 The method of an embodiment comprises transmitting event data of the security system components from the gateway to the central monitoring station over the secondary communication link.

25 The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The secondary communication link of an embodiment includes a broadband coupling.

The secondary communication link of an embodiment includes a General Packet Radio Service (GPRS) coupling.

The gateway of an embodiment transmits messages comprising event data of the security system components to remote client devices over the secondary communication link.

5 The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

The gateway of an embodiment receives control data for control of the security system components from remote client devices via the secondary communication link.

10 The security network of an embodiment comprises network devices coupled to the gateway via a wireless coupling.

The gateway of an embodiment including the connection management component automatically discovers the network devices.

The gateway of an embodiment including the connection management component automatically installs the network devices in the security network.

15 The gateway of an embodiment including the connection management component automatically configures the network devices for operation in the security network.

The gateway of an embodiment controls communications between the network devices, the security system components, and the security server.

20 The gateway of an embodiment including the connection management component transmits event data of the network devices to remote client devices over at least one of a plurality of communication links.

The gateway of an embodiment receives control data for control of the network devices from remote client devices via at least one of the plurality of communication links.

25 The event data of an embodiment comprises changes in device states of the network devices, data of the network devices, and data received by the network devices.

The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary  
30 communication link.

The gateway of an embodiment transmits event data of the network devices to the central monitoring station over the secondary communication link.

The secondary communication link of an embodiment includes a broadband coupling.

5 The secondary communication link of an embodiment includes a General Packet Radio Service (GPRS) coupling.

The gateway of an embodiment transmits messages comprising event data of the network devices to remote client devices over the secondary communication link.

10 The security server of an embodiment creates, modifies and terminates couplings between the gateway and the network devices.

The security server of an embodiment performs creation, modification, deletion and configuration of the network devices.

The security server of an embodiment creates automations, schedules and notification rules associated with the network devices.

15 The security server of an embodiment manages access to current and logged state data for the network devices.

The security server of an embodiment manages access to current and logged state data for couplings between the gateway and the network devices.

20 The security server of an embodiment manages communications with the network devices.

The network device of an embodiment is an Internet Protocol device.

The network device of an embodiment is a camera.

The network device of an embodiment is a touchscreen.

25 The network device of an embodiment is a device controller that controls an attached device.

The network device of an embodiment is a sensor.

The security server of an embodiment creates, modifies and terminates users corresponding to the security system.

30 The security server of an embodiment creates, modifies and terminates couplings between the gateway and the security system components.

The security server of an embodiment performs creation, modification, deletion and configuration of the security system components.

The security server of an embodiment creates automations, schedules and notification rules associated with the security system components.

5 The security server of an embodiment manages access to current and logged state data for the security system components.

The security server of an embodiment manages access to current and logged state data for couplings between the gateway and the security system components.

10 The security server of an embodiment manages communications with the security system components.

The security server of an embodiment generates and transfers notifications to remote client devices, the notifications comprising event data.

The notifications of an embodiment include one or more of short message service messages and electronic mail messages.

15 The event data of an embodiment is event data of the security system components.

The security server of an embodiment transmits event data of the security system components to a central monitoring station of the security system over the secondary communication link.

20 The security system components of an embodiment include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.

Embodiments of the integrated security system include a method comprising: coupling a gateway comprising a connection management component to a local area network located at a facility; and forming a security network by automatically establishing a wireless coupling between the gateway and a security system using the connection management component, the security system comprising a plurality of security system components located at the facility, wherein forming the security network includes integrating communications and functions of the security system components into the security network via the wireless coupling.

30 Embodiments of the integrated security system include a method comprising: forming a security network, the forming including automatically establishing a wireless coupling between a gateway and a security system installed at a facility, wherein the

security system includes a plurality of security system components that are proprietary to the security system, the forming including the gateway automatically integrating communications and functions of the security system components into a local area network of the facility; and providing an interface by which a remote client device  
5 accesses the security network, the interface enabling communications with and control of the functions of the security system.

Embodiments of the integrated security system include a method comprising:  
coupling a gateway to a local area network located in a first location and a security server in a second location, wherein the first location includes a security system comprising a  
10 plurality of security system components; automatically establishing communications between the gateway and the security system components; automatically establishing communications between the gateway and premise devices; and forming a security network by electronically integrating, via the gateway, communications and functions of the plurality of premise devices and the security system components.

15 The method of an embodiment comprises controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device.

The remote client devices of an embodiment include one or more of personal computers, personal digital assistants, cellular telephones, and mobile computing devices.

20 The method of an embodiment comprises the gateway automatically discovering the security system components.

The method of an embodiment comprises using protocols of the security system to discover the security system components, wherein the gateway includes the protocols of the security system.

25 The method of an embodiment comprises the gateway receiving protocols of the security system from the security server in response to a request, wherein the gateway uses the protocols received to discover the security system components.

The gateway of an embodiment comprises a connection management component, the connection management component automatically establishing a coupling with the  
30 security system including the security system components.

The connection management component of an embodiment automatically discovers the premise devices.

The connection management component of an embodiment automatically installs the premise devices in the security network.

5 The connection management component of an embodiment automatically configures the premise devices for operation in the security network.

The gateway of an embodiment includes a rules component that manages rules of interaction between the gateway, the security system components, and the premise devices.

10 The gateway of an embodiment includes a device connect component that includes definitions of the security system components and the premise devices.

The premise local area network of an embodiment is coupled to a wide area network via a premise router.

15 The gateway of an embodiment is coupled to the local area network using a premise router, and the gateway is coupled to a wide area network.

The gateway of an embodiment is coupled to the premise devices using a wireless coupling.

The gateway of an embodiment is coupled to the security server via the internet.

20 The gateway of an embodiment is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location.

25 The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link.

The method of an embodiment comprises transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link.

30 The event data of an embodiment comprises changes in device states of at least one of security system components and premise devices, data of at least one of security

system components and premise devices, and data received by at least one of security system components and premise devices.

5 The method of an embodiment comprises transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable.

The secondary communication link of an embodiment includes a broadband coupling.

The secondary communication link of an embodiment includes a General Packet Radio Service (GPRS) coupling.

10 The method of an embodiment comprises transmitting messages comprising event data of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link.

15 The event data of an embodiment comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

The security server of an embodiment creates, modifies and terminates users corresponding to the security system.

20 The security server of an embodiment creates, modifies and terminates couplings between the gateway and the security system components.

The security server of an embodiment creates, modifies and terminates couplings between the gateway and the premise devices.

The security server of an embodiment performs creation, modification, deletion and configuration of the security system components.

25 The security server of an embodiment performs creation, modification, deletion and configuration of the premise devices.

The security server of an embodiment creates automations, schedules and notification rules associated with the security system components.

30 The security server of an embodiment creates automations, schedules and notification rules associated with the premise devices.



The security server of an embodiment manages access to current and logged state data for the security system components.

The security server of an embodiment manages access to current and logged state data for the premise devices.

5 The security server of an embodiment manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices.

The security server of an embodiment manages communications with the security system components.

10 The security server of an embodiment manages communications with the premise devices.

The security server of an embodiment generates and transfers notifications to remote client devices, the notifications comprising event data.

15 The notifications of an embodiment include one or more of short message service messages and electronic mail messages.

The event data of an embodiment is event data of the security system components.

The event data of an embodiment is event data of the premise devices.

20 The security server of an embodiment transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link.

The security system components of an embodiment include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.

The premise device of an embodiment is an Internet Protocol device.

The premise device of an embodiment is a camera.

25 The premise device of an embodiment is a touchscreen.

The premise device of an embodiment is a device controller that controls an attached device.

The premise device of an embodiment is a sensor.

30 Embodiments of the integrated security system include a method comprising: forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system

including security system components located at the first location, wherein the security server is located at a second location different from the first location; and establishing a coupling between the gateway and a plurality of premise devices located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the security network.

Embodiments of the integrated security system include a method comprising: automatically establishing communications between a gateway and a security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system; and automatically establishing communications between the gateway and a plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating communications and functions of the plurality of network devices and the security system components.

Embodiments of the integrated security system include a method comprising: forming a security network by automatically establishing communications between a gateway and a security system, the security system including security system components installed at a facility; automatically establishing communications between the security network and a plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the security network; and providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the network devices.

Aspects of the integrated security system and corresponding systems and methods described herein may be implemented as functionality programmed into any of a variety of circuitry, including programmable logic devices (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for

implementing aspects of the integrated security system and corresponding systems and methods include: microcontrollers with memory (such as electronically erasable programmable read only memory (EEPROM)), embedded microprocessors, firmware, software, etc. Furthermore, aspects of the integrated security system and corresponding systems and methods may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

It should be noted that any system, method, and/or other components disclosed herein may be described using computer aided design tools and expressed (or represented), as data and/or instructions embodied in various computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such formatted data and/or instructions by carrier waves include, but are not limited to, transfers (uploads, downloads, e-mail, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g., HTTP, FTP, SMTP, etc.). When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of the above described components may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs.

Unless the context clearly requires otherwise, throughout the description and the claims, the words “comprise,” “comprising,” and the like are to be construed in an

inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of “including, but not limited to.” Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words “herein,”

5 “hereunder,” “above,” “below,” and words of similar import, when used in this application, refer to this application as a whole and not to any particular portions of this application. When the word “or” is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

10 The above description of embodiments of the integrated security system and corresponding systems and methods is not intended to be exhaustive or to limit the systems and methods to the precise forms disclosed. While specific embodiments of, and examples for, the integrated security system and corresponding systems and methods are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the systems and methods, as those skilled in the relevant art will  
15 recognize. The teachings of the integrated security system and corresponding systems and methods provided herein can be applied to other systems and methods, not only for the systems and methods described above.

The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the  
20 integrated security system and corresponding systems and methods in light of the above detailed description.

In general, in the following claims, the terms used should not be construed to limit the integrated security system and corresponding systems and methods to the specific  
25 embodiments disclosed in the specification and the claims, but should be construed to include all systems that operate under the claims. Accordingly, the integrated security system and corresponding systems and methods is not limited by the disclosure, but instead the scope is to be determined entirely by the claims.

While certain aspects of the integrated security system and corresponding systems and methods are presented below in certain claim forms, the inventors contemplate the  
30 various aspects of the integrated security system and corresponding systems and methods in any number of claim forms. Accordingly, the inventors reserve the right to add

additional claims after filing the application to pursue such additional claim forms for other aspects of the integrated security system and corresponding systems and methods.

CLAIMS

What is claimed is:

1. A method comprising:
  - coupling a gateway to a local area network located in a first location and a
  - 5 security server in a second location, wherein the first location includes a security system comprising a plurality of security system components;
  - automatically establishing communications between the gateway and the security system components;
  - automatically establishing communications between the gateway and premise
  - 10 devices; and
  - forming a security network by electronically integrating, via the gateway, communications and functions of the plurality of premise devices and the security system components.
- 15 2. The method of claim 1, comprising controlling the functions of the security network via an interface coupled to the security network, wherein the interface is accessed using a remote client device.
3. The method of claim 2, wherein the remote client devices include one or more of
- 20 personal computers, personal digital assistants, cellular telephones, and mobile computing devices.
4. The method of claim 1, comprising the gateway automatically discovering the security system components.
- 25 5. The method of claim 4, comprising using protocols of the security system to discover the security system components, wherein the gateway includes the protocols of the security system.

6. The method of claim 4, comprising the gateway receiving protocols of the security system from the security server in response to a request, wherein the gateway uses the protocols received to discover the security system components.

5 7. The method of claim 1, wherein the gateway comprises a connection management component, the connection management component automatically establishing a coupling with the security system including the security system components.

8. The method of claim 7, wherein the connection management component  
10 automatically discovers the premise devices.

9. The method of claim 7, wherein the connection management component automatically installs the premise devices in the security network.

15 10. The method of claim 7, wherein the connection management component automatically configures the premise devices for operation in the security network.

11. The method of claim 1, wherein the gateway includes a rules component that manages rules of interaction between the gateway, the security system components, and  
20 the premise devices.

12. The method of claim 1, wherein the gateway includes a device connect component that includes definitions of the security system components and the premise  
25 devices.

13. The method of claim 1, wherein the premise local area network is coupled to a wide area network via a premise router.

14. The method of claim 1, wherein the gateway is coupled to the local area network  
30 using a premise router, and the gateway is coupled to a wide area network.

15. The method of claim 1, wherein the gateway is coupled to the premise devices using a wireless coupling.

16. The method of claim 1, wherein the gateway is coupled to the security server via  
5 the internet.

17. The method of claim 1, wherein the gateway is coupled to a central monitoring station corresponding to the security system, wherein the central monitoring station is located at a third location different from the first location and the second location.

10

18. The method of claim 1, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link.

15

19. The method of claim 18, comprising transmitting event data of the security system components and the premise devices to the central monitoring station via the gateway and the secondary communication link.

20. The method of claim 19, wherein the event data comprises changes in device states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

21. The method of claim 18, comprising transmitting event data of the security system to the central monitoring station via the gateway and the secondary communication link when the primary communication link is unavailable.

22. The method of claim 18, wherein the secondary communication link includes a  
30 broadband coupling.



23. The method of claim 18, wherein the secondary communication link includes a General Packet Radio Service (GPRS) coupling.

24. The method of claim 18, comprising transmitting messages comprising event data  
5 of the security system components and the premise devices to remote client devices via the gateway and the secondary communication link.

25. The method of claim 24, wherein the event data comprises changes in device  
10 states of at least one of security system components and premise devices, data of at least one of security system components and premise devices, and data received by at least one of security system components and premise devices.

26. The method of claim 1, wherein the security server creates, modifies and  
15 terminates users corresponding to the security system.

27. The method of claim 1, wherein the security server creates, modifies and  
terminates couplings between the gateway and the security system components.

28. The method of claim 1, wherein the security server creates, modifies and  
20 terminates couplings between the gateway and the premise devices.

29. The method of claim 1, wherein the security server performs creation,  
modification, deletion and configuration of the security system components.

25 30. The method of claim 1, wherein the security server performs creation,  
modification, deletion and configuration of the premise devices.

31. The method of claim 1, wherein the security server creates automations, schedules  
and notification rules associated with the security system components.

30

32. The method of claim 1, wherein the security server creates automations, schedules and notification rules associated with the premise devices.

33. The method of claim 1, wherein the security server manages access to current and  
5 logged state data for the security system components.

34. The method of claim 1, wherein the security server manages access to current and logged state data for the premise devices.

10 35. The method of claim 1, wherein the security server manages access to current and logged state data for couplings among the gateway, the security system components and the IP devices.

36. The method of claim 1, wherein the security server manages communications  
15 with the security system components.

37. The method of claim 1, wherein the security server manages communications with the premise devices.

20 38. The method of claim 1, wherein the security server generates and transfers notifications to remote client devices, the notifications comprising event data.

39. The method of claim 38, wherein the notifications include one or more of short message service messages and electronic mail messages.

25

40. The method of claim 38, wherein the event data is event data of the security system components.

41. The method of claim 38, wherein the event data is event data of the premise  
30 devices.

42. The method of claim 1, wherein the security server transmits event data of the security system components and the premise devices to a central monitoring station of the security system over the secondary communication link.
- 5 43. The method of claim 1, wherein the security system components include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.
44. The method of claim 1, wherein the premise device is an Internet Protocol device.
- 10 45. The method of claim 1, wherein the premise device is a camera.
46. The method of claim 1, wherein the premise device is a touchscreen.
47. The method of claim 1, wherein the premise device is a device controller that  
15 controls an attached device.
48. The method of claim 1, wherein the premise device is a sensor.
49. A method comprising:  
20 forming a security network by coupling a gateway to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location; and  
establishing a coupling between the gateway and a plurality of premise devices  
25 located at the first location, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the security network.
50. A method comprising:

automatically establishing communications between a gateway and a security system in a facility, wherein the security system includes a plurality of security system components that are proprietary to the security system; and

5 automatically establishing communications between the gateway and a plurality of network devices, wherein the gateway forms a premise security network at the facility and couples the premise security network to a local area network of the facility, wherein the gateway forms the premise security network by electronically integrating communications and functions of the plurality of network devices and the security system components.

10

51. A method comprising:

forming a security network by automatically establishing communications between a gateway and a security system, the security system including security system components installed at a facility;

15

automatically establishing communications between the security network and a plurality of network devices located at the facility, the gateway electronically integrating communications and functions of the plurality of network devices and the security system components into the security network; and

20

providing an interface by which a remote client device accesses the security network, the interface enabling communications with and control of the functions of the security system components and the network devices.

ABSTRACT

An integrated security system is described that integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network (broadband, cellular/GSM, POTS access) that enables users to remotely stay connected to their premises. The integrated security system, while delivering remote premise monitoring and control functionality to conventional monitored premise protection, complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wirelessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices (cameras, lamp modules, thermostats, etc.) can be added, enabling users to remotely see live video and/or pictures and control home devices via their personal web portal or webpage, mobile phone, and/or other remote client device. Users can also receive notifications via email or text message when happenings occur, or do not occur, in their home.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>				
<b>Filing Date:</b>				
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices			
First Named Inventor/Applicant Name:	Marc Baum			
<b>Filer:</b>	Richard L. Gregory/Jerry Donnard			
<b>Attorney Docket Number:</b>	ICON.P001D3			
Filed as Small Entity				
<b>Utility Filing Fees</b>				
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>
<b>Basic Filing:</b>				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	255	255
Utility Examination Fee	2311	1	105	105
<b>Pages:</b>				
<b>Claims:</b>				
Claims in excess of 20	2202	31	25	775
Independent claims in excess of 3	2201	1	105	105
<b>Miscellaneous-Filing:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
Post-Allowance-and-Post-Issuance:				
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>1315</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	3762275
<b>Application Number:</b>	12189788
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7650
<b>Title of Invention:</b>	Forming A Security Network Including Integrated Security System Components and Network Devices
<b>First Named Inventor/Applicant Name:</b>	Marc Baum
<b>Customer Number:</b>	53186
<b>Filer:</b>	Richard L. Gregory/Jerry Donnard
<b>Filer Authorized By:</b>	Richard L. Gregory
<b>Attorney Docket Number:</b>	ICON.P001D3
<b>Receipt Date:</b>	12-AUG-2008
<b>Filing Date:</b>	
<b>Time Stamp:</b>	00:06:45
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1315
RAM confirmation Number	3684
Deposit Account	
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part (.zip (if appl.))	Pages
		SecureNet Technologies, LLC Exhibit 1003 Page 1008	Message Digest		



1	Application Data Sheet	ADS_ICONP001D3.pdf	2079263	no	6
			3b973dfc2b78425343b8c1f8a5b8631a a70d087c		

**Warnings:**

**Information:**

2		Patent_Application_ICONP001D3.pdf	10857355	yes	96
			7462130f773157ea82d34bd09f10562a 4cd3bef0		

**Multipart Description/PDF files in .zip description**

Document Description	Start	End
Transmittal of New Application	1	1
Specification	2	74
Claims	75	81
Abstract	82	82
Drawings-only black and white line drawings	83	96

**Warnings:**

**Information:**

3	Fee Worksheet (PTO-06)	fee-info.pdf	8591	no	2
			349ec3eeb9a8ba0ecf9ebae2ab81bc1d ac0cf2bf		

**Warnings:**

**Information:**

**Total Files Size (in bytes):** 12945209

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	ICON.P001D3
		Application Number	
Title of Invention	Forming A Security Network Including Integrated Security System Components and Network Devices		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

**Secrecy Order 37 CFR 5.2**

- Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

**Applicant Information:**

<b>Applicant 1</b>						<input type="button" value="Remove"/>	
<b>Applicant Authority</b>		<input checked="" type="radio"/> Inventor		<input type="radio"/> Legal Representative under 35 U.S.C. 117		<input type="radio"/> Party of Interest under 35 U.S.C. 118	
<b>Prefix</b>	<b>Given Name</b>	<b>Middle Name</b>	<b>Family Name</b>		<b>Suffix</b>		
	Marc		Baum				
<b>Residence Information (Select One)</b>							
		<input checked="" type="radio"/> US Residency		<input type="radio"/> Non US Residency		<input type="radio"/> Active US Military Service	
<b>City</b>	Palo Alto	<b>State/Province</b>	CA	<b>Country of Residence<sup>i</sup></b>	US		
<b>Citizenship under 37 CFR 1.41(b)<sup>i</sup></b>		US					
<b>Mailing Address of Applicant:</b>							
<b>Address 1</b>		3045 Park Blvd., 2nd Floor					
<b>Address 2</b>							
<b>City</b>	Palo Alto	<b>State/Province</b>	CA				
<b>Postal Code</b>	94306	<b>Country<sup>i</sup></b>	US				
<b>Applicant 2</b>						<input type="button" value="Remove"/>	
<b>Applicant Authority</b>		<input checked="" type="radio"/> Inventor		<input type="radio"/> Legal Representative under 35 U.S.C. 117		<input type="radio"/> Party of Interest under 35 U.S.C. 118	
<b>Prefix</b>	<b>Given Name</b>	<b>Middle Name</b>	<b>Family Name</b>		<b>Suffix</b>		
	Paul	J.	Dawes				
<b>Residence Information (Select One)</b>							
		<input checked="" type="radio"/> US Residency		<input type="radio"/> Non US Residency		<input type="radio"/> Active US Military Service	
<b>City</b>	Palo Alto	<b>State/Province</b>	CA	<b>Country of Residence<sup>i</sup></b>	US		
<b>Citizenship under 37 CFR 1.41(b)<sup>i</sup></b>		US					
<b>Mailing Address of Applicant:</b>							
<b>Address 1</b>		3045 Park Blvd., 2nd Floor					
<b>Address 2</b>							
<b>City</b>	Palo Alto	<b>State/Province</b>	CA				
<b>Postal Code</b>	94306	<b>Country<sup>i</sup></b>	US				
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the <b>Add</b> button.						<input type="button" value="Add"/>	

**Correspondence Information:**

Enter either Customer Number or complete the Correspondence Information section below.  
For further information see 37 CFR 1.33(a).

- An Address is being provided for the correspondence information of this application.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	ICON.P001D3	
		Application Number		
Title of Invention	Forming A Security Network Including Integrated Security System Components and Network Devices			
Customer Number	53186			
Email Address	rgregory@csgip.com	<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>	

**Application Information:**

Title of the Invention	Forming A Security Network Including Integrated Security System Components and Network Devices			
Attorney Docket Number	ICON.P001D3	Small Entity Status Claimed <input checked="" type="checkbox"/>		
Application Type	Nonprovisional			
Subject Matter	Utility			
Suggested Class (if any)		Sub Class (if any)		
Suggested Technology Center (if any)				
Total Number of Drawing Sheets (if any)	14	Suggested Figure for Publication (if any)		

**Publication Information:**

<input type="checkbox"/>	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
<input type="checkbox"/>	<b>Request Not to Publish.</b> I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application <b>has not and will not</b> be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

**Representative Information:**

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.			
Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> Limited Recognition (37 CFR 11.9)
Customer Number	53186		

**Domestic Benefit/National Stage Information:**

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.			
Prior Application Status		<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	60955172	2007-08-10
Prior Application Status		<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	60957997	2007-08-24

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	ICON.P001D3
		Application Number	
Title of Invention	Forming A Security Network Including Integrated Security System Components and Network Devices		
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	60968005	2007-08-24
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	60987359	2007-11-12
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	60987366	2007-11-12
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61019162	2008-01-04
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61019167	2008-01-04
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61023489	2008-01-25
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61023493	2008-01-25
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61023496	2008-01-25
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61087967	2008-08-11
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	11084232	2005-03-16
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	11761718	2007-06-12
Prior Application Status			<input type="button" value="Remove"/>
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation in part of	11761745	2007-06-12

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	ICON.P001D3	
		Application Number		
Title of Invention	Forming A Security Network Including Integrated Security System Components and Network Devices			
Prior Application Status			<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	
	Continuation in part of	12019554	2008-01-24	
Prior Application Status			<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	
	Continuation in part of	12019568	2008-01-24	
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the <b>Add</b> button.			<input type="button" value="Add"/>	

### Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
			<input type="button" value="Remove"/>
Application Number	Country <sup>i</sup>	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			<input checked="" type="radio"/> Yes <input type="radio"/> No
Additional Foreign Priority Data may be generated within this form by selecting the <b>Add</b> button.			<input type="button" value="Add"/>

### Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.				
<b>Assignee 1</b>				<input type="button" value="Remove"/>
If the Assignee is an Organization check here. <input type="checkbox"/>				
Prefix	Given Name	Middle Name	Family Name	Suffix
<b>Mailing Address Information:</b>				
Address 1				
Address 2				
City		State/Province		
Country <sup>i</sup>			Postal Code	
Phone Number		Fax Number		
Email Address				
Additional Assignee Data may be generated within this form by selecting the <b>Add</b> button.				<input type="button" value="Add"/>

### Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.			
Signature	/Richard L. Gregory, Jr./	Date (YYYY-MM-DD)	2008-08-11

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>Application Data Sheet 37 CFR 1.76</b>		Attorney Docket Number	ICON.P001D3		
		Application Number			
Title of Invention	Forming A Security Network Including Integrated Security System Components and Network Devices				
First Name	Richard	Last Name	Gregory	Registration Number	42607

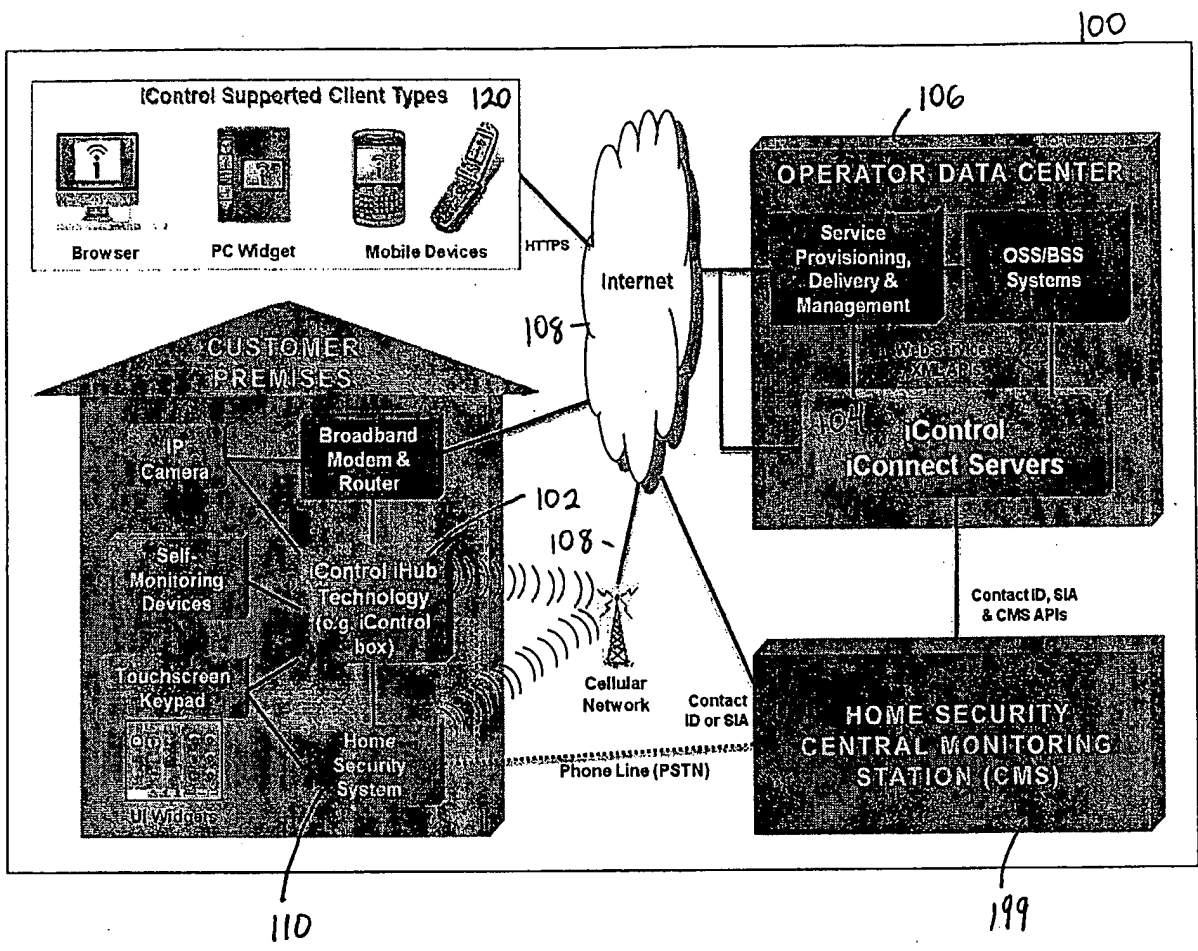
This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



**FIG. 1**



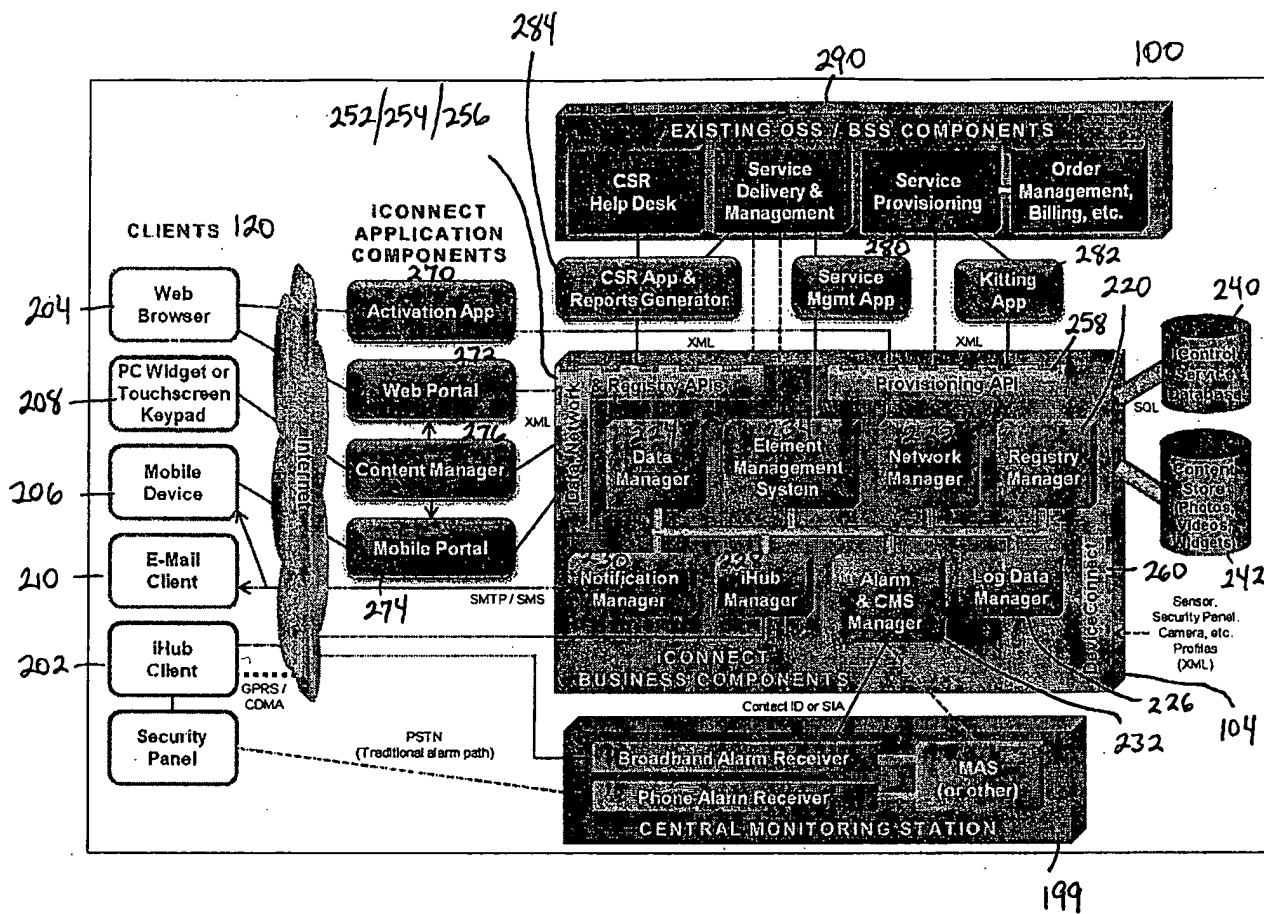
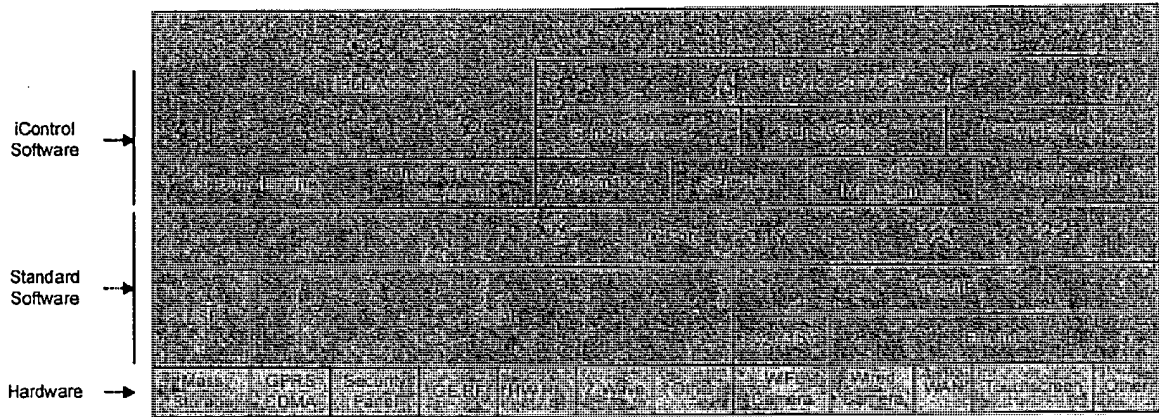
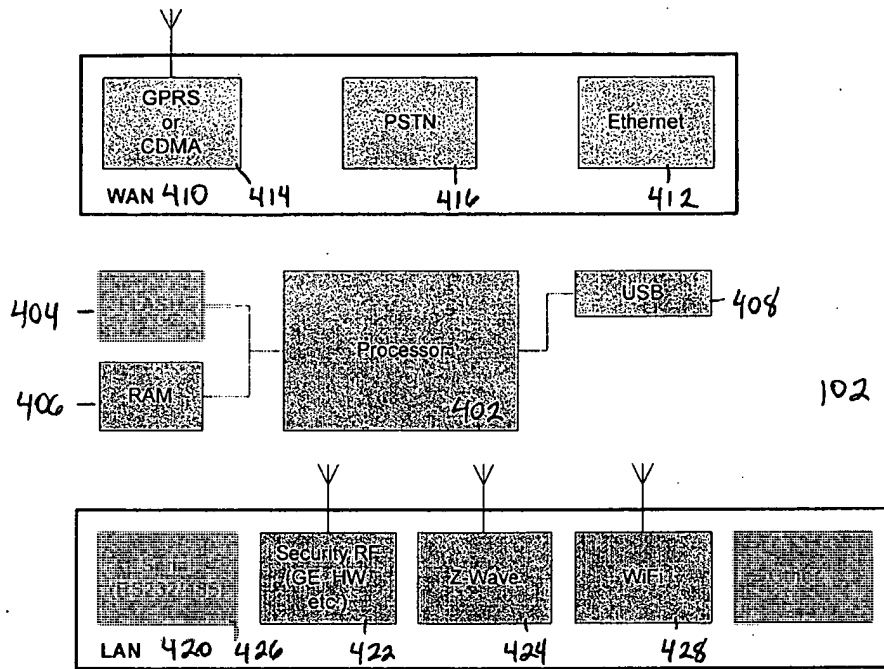


FIG. 2

102  
↓



**FIG. 3**



**FIG. 4**

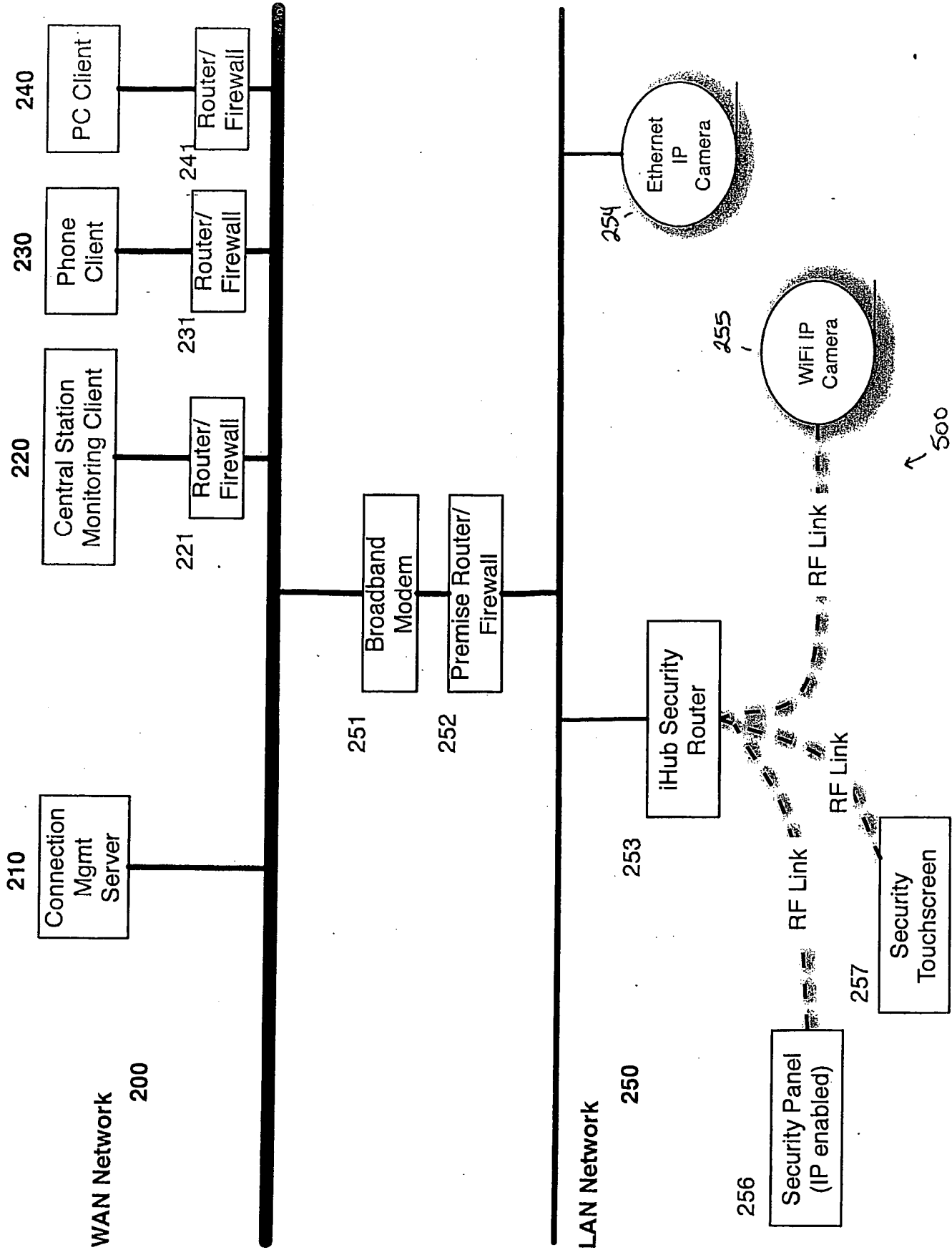
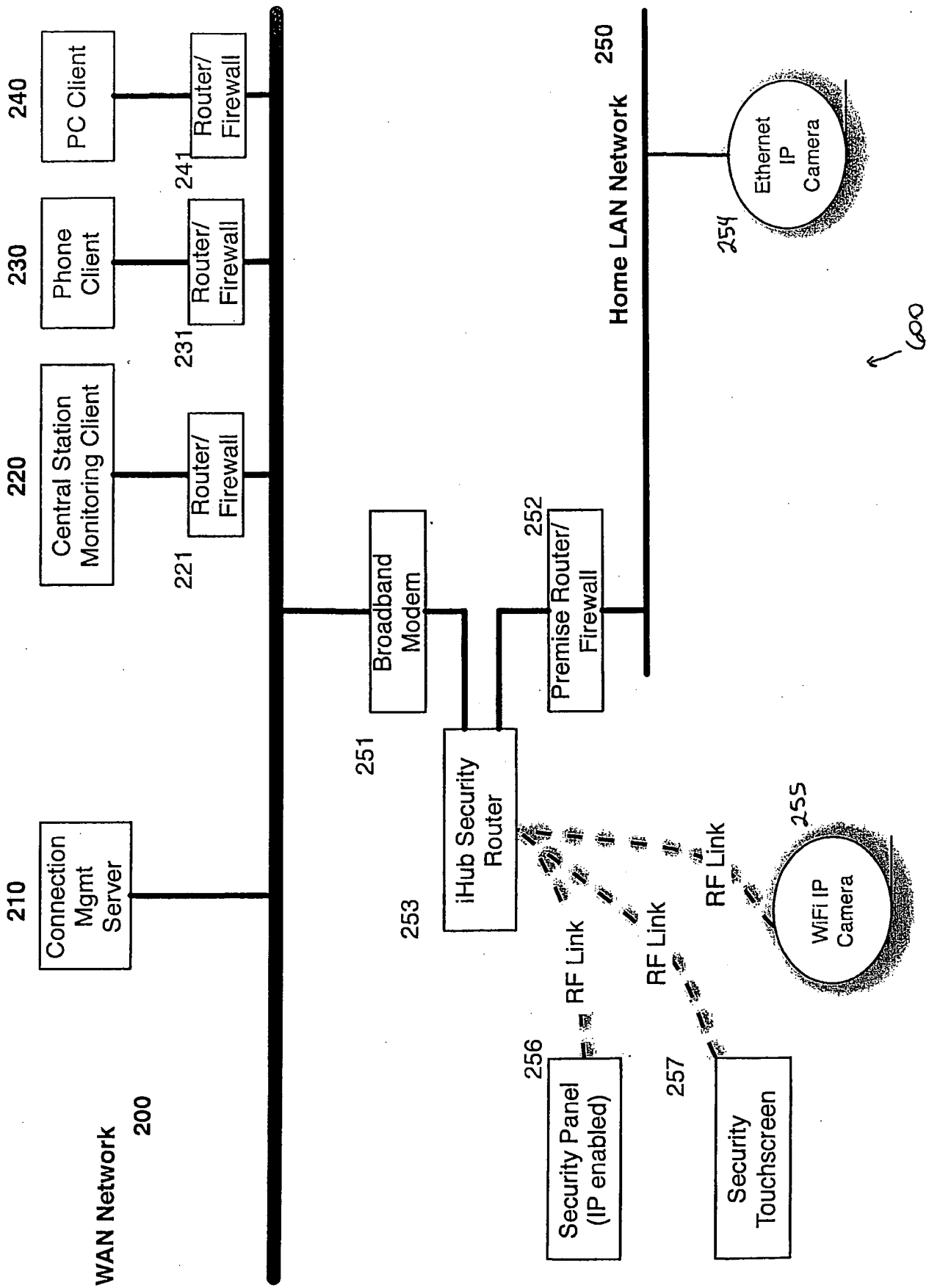


FIG. 5



600 ↖

FIG. 6

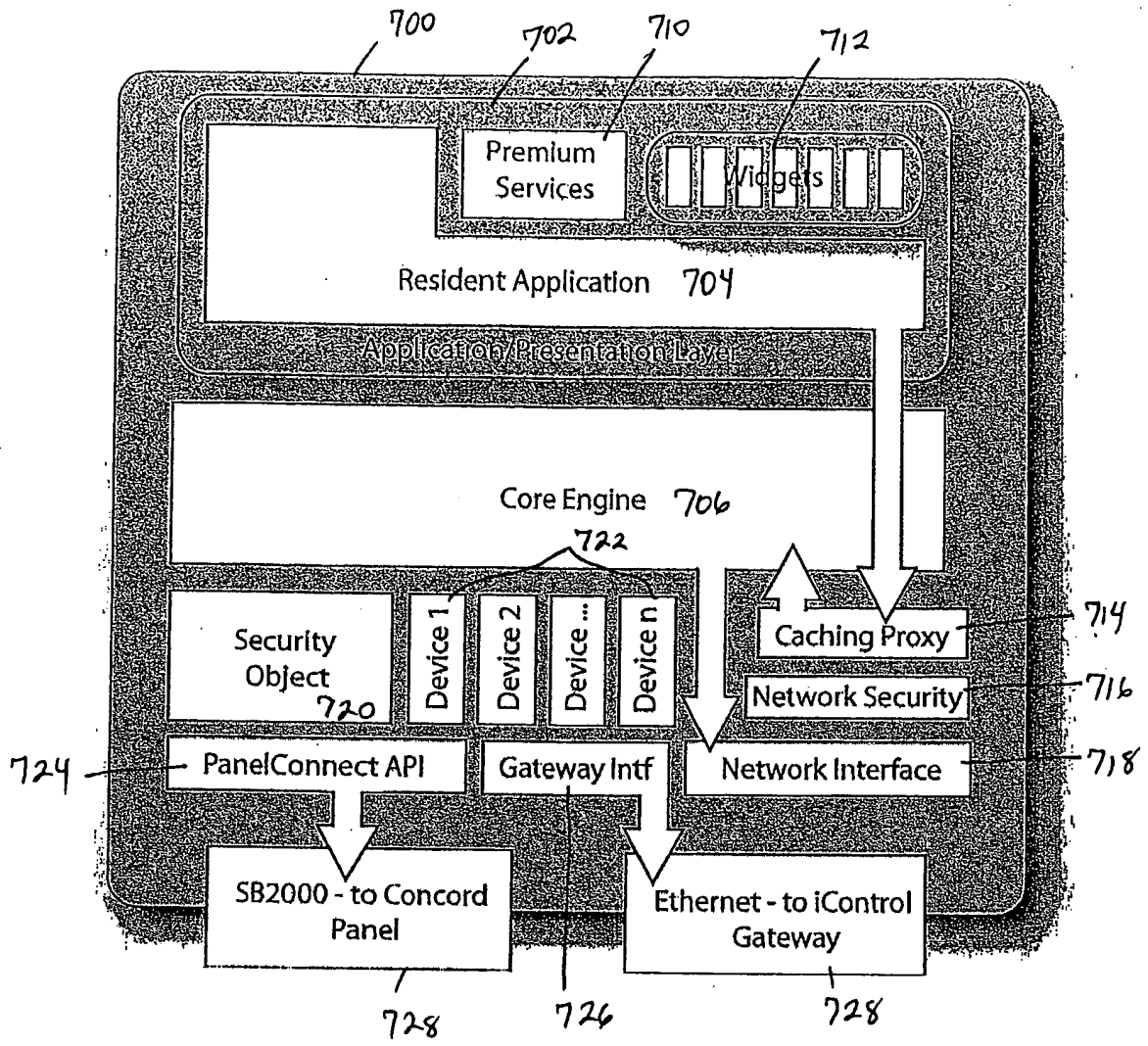
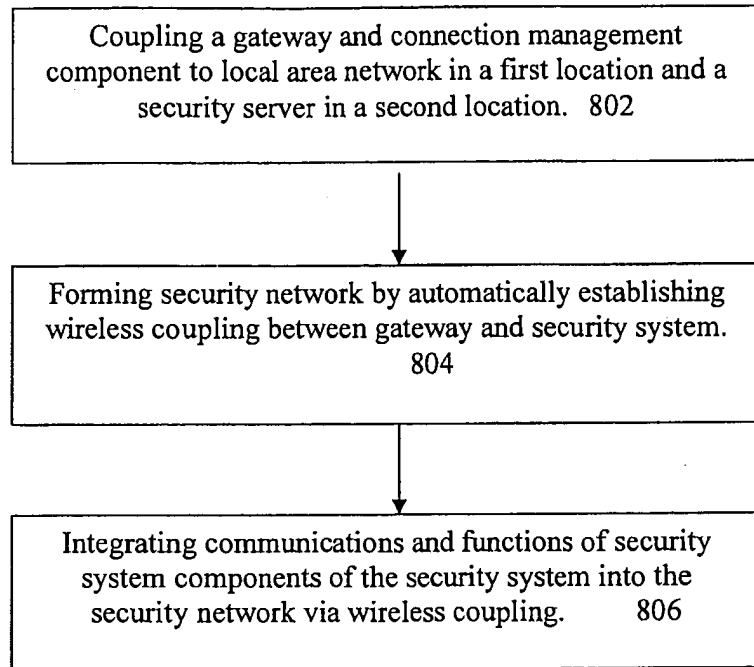


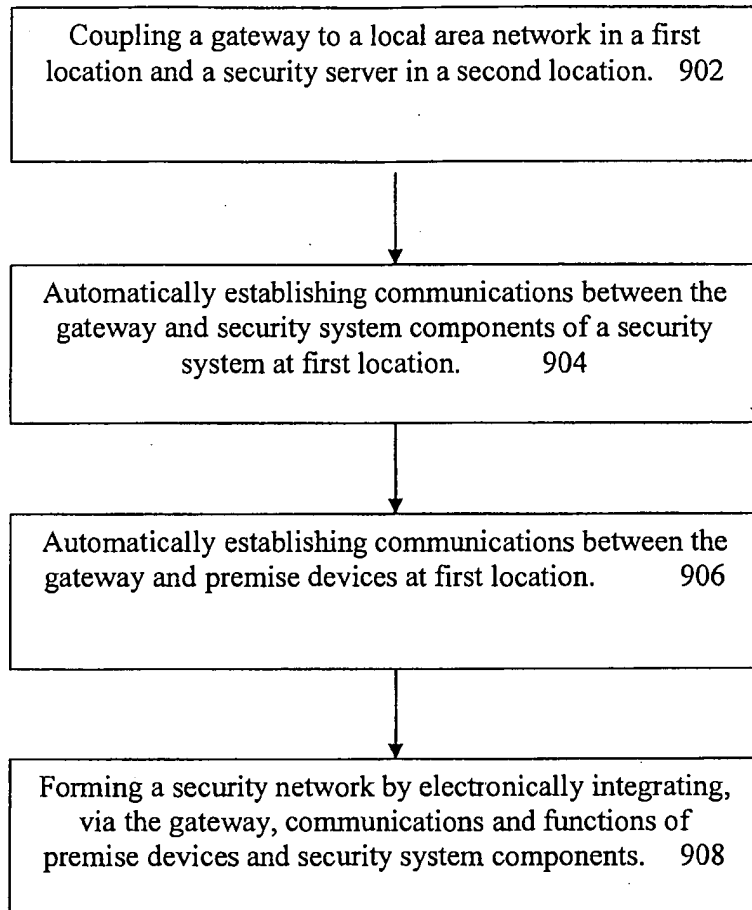
FIG. 7

800



**Figure 8**

900



**Figure 9**



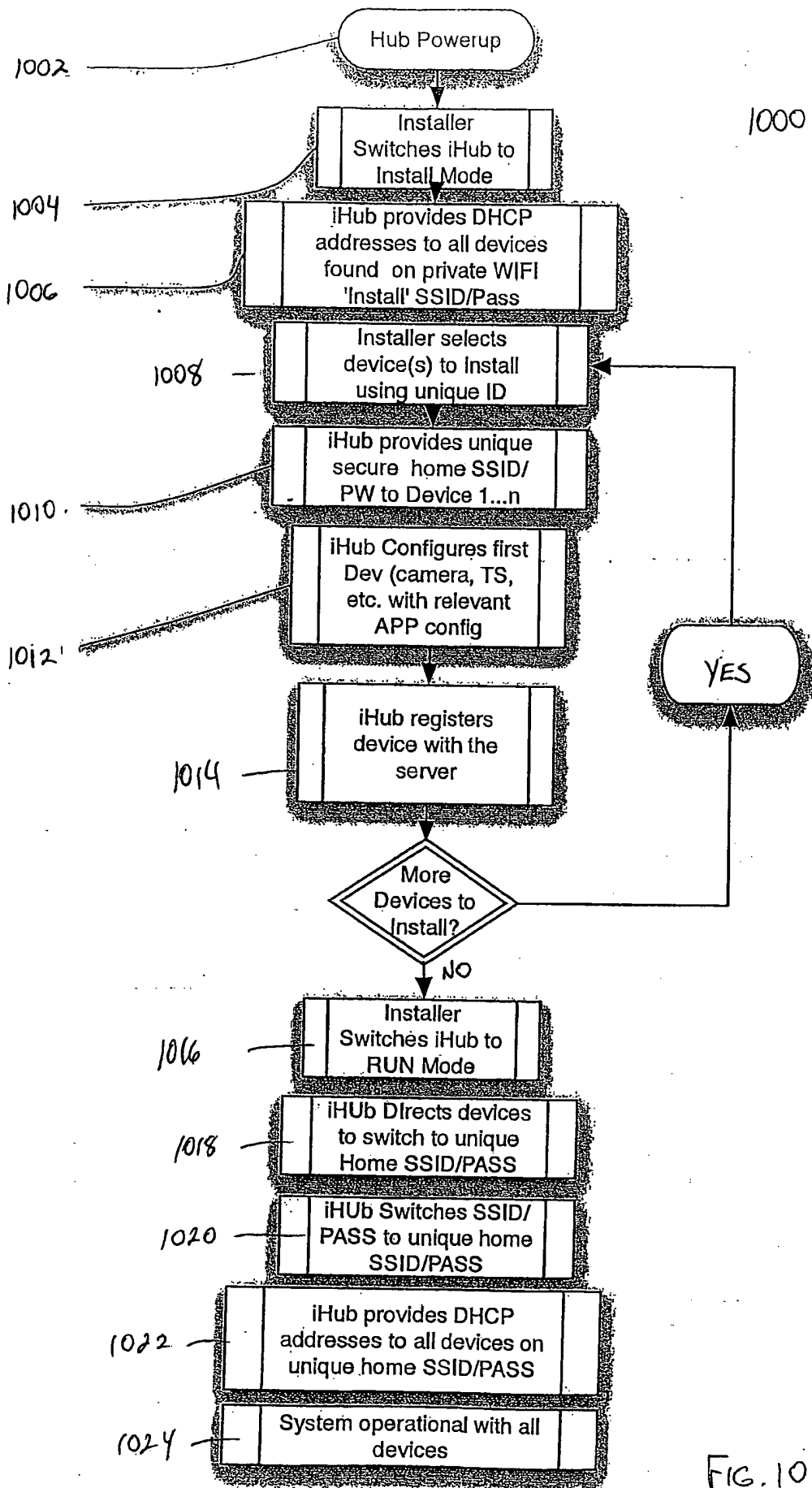


FIG. 10

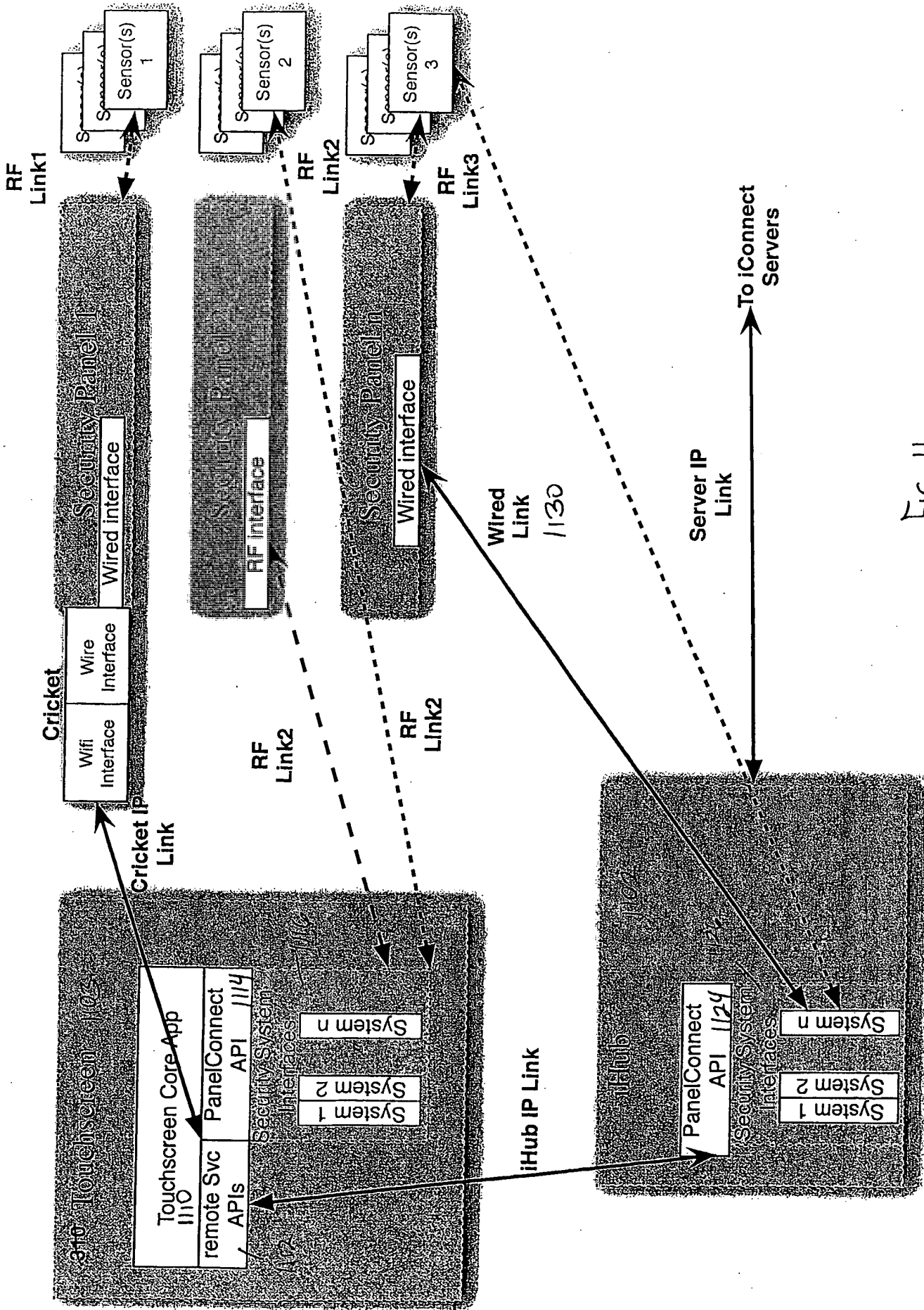


FIG. 11

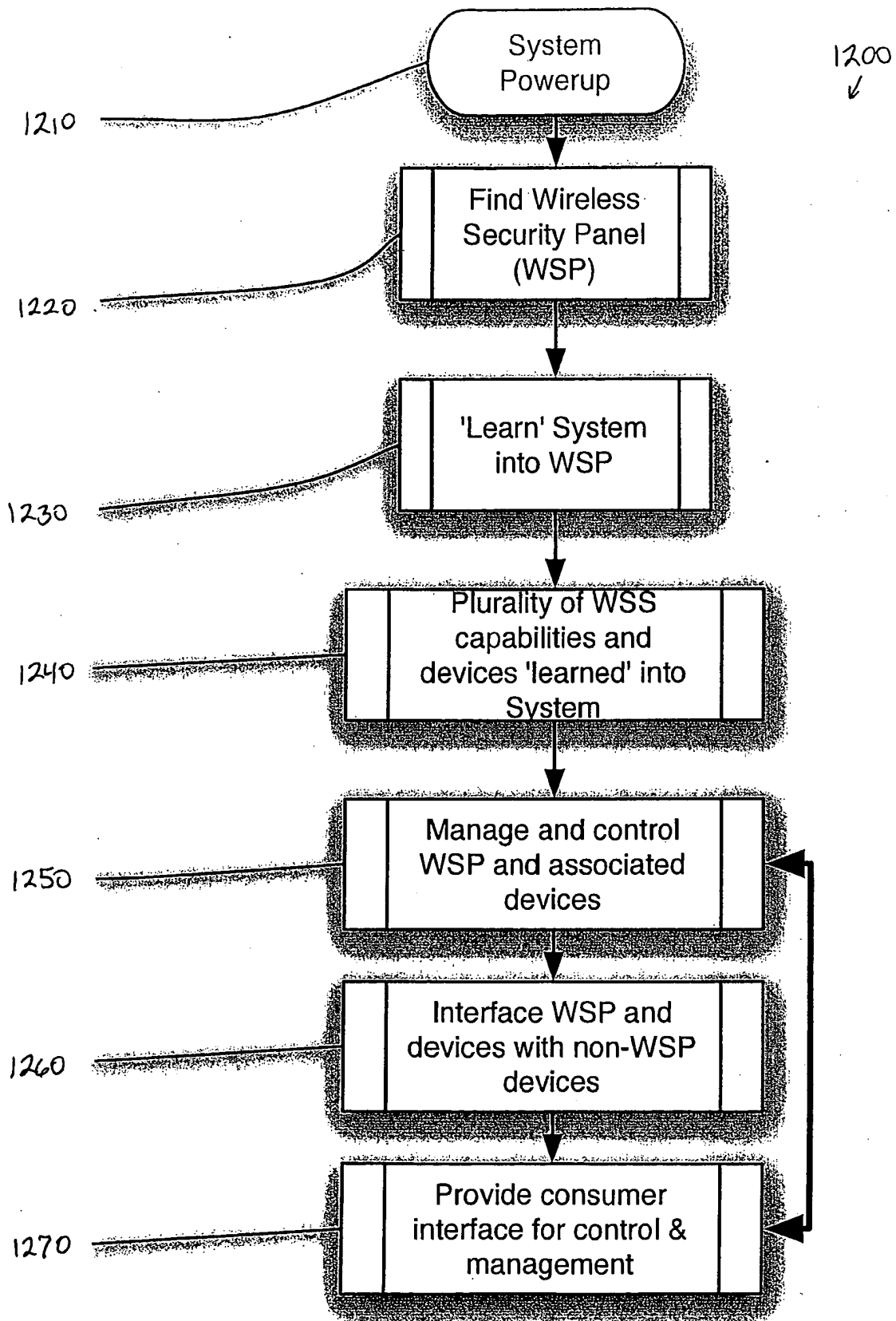


FIG. 12

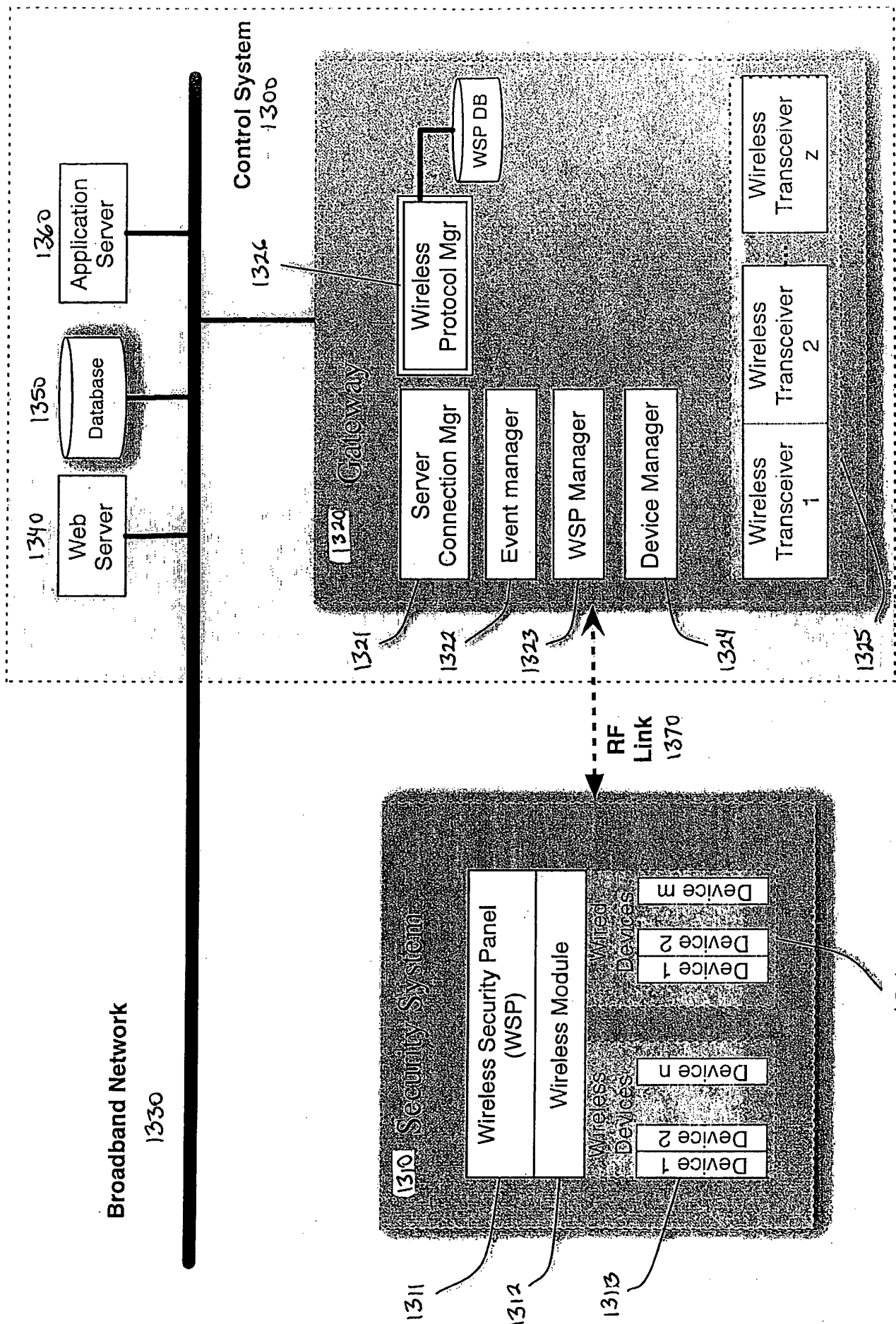


Fig. 13

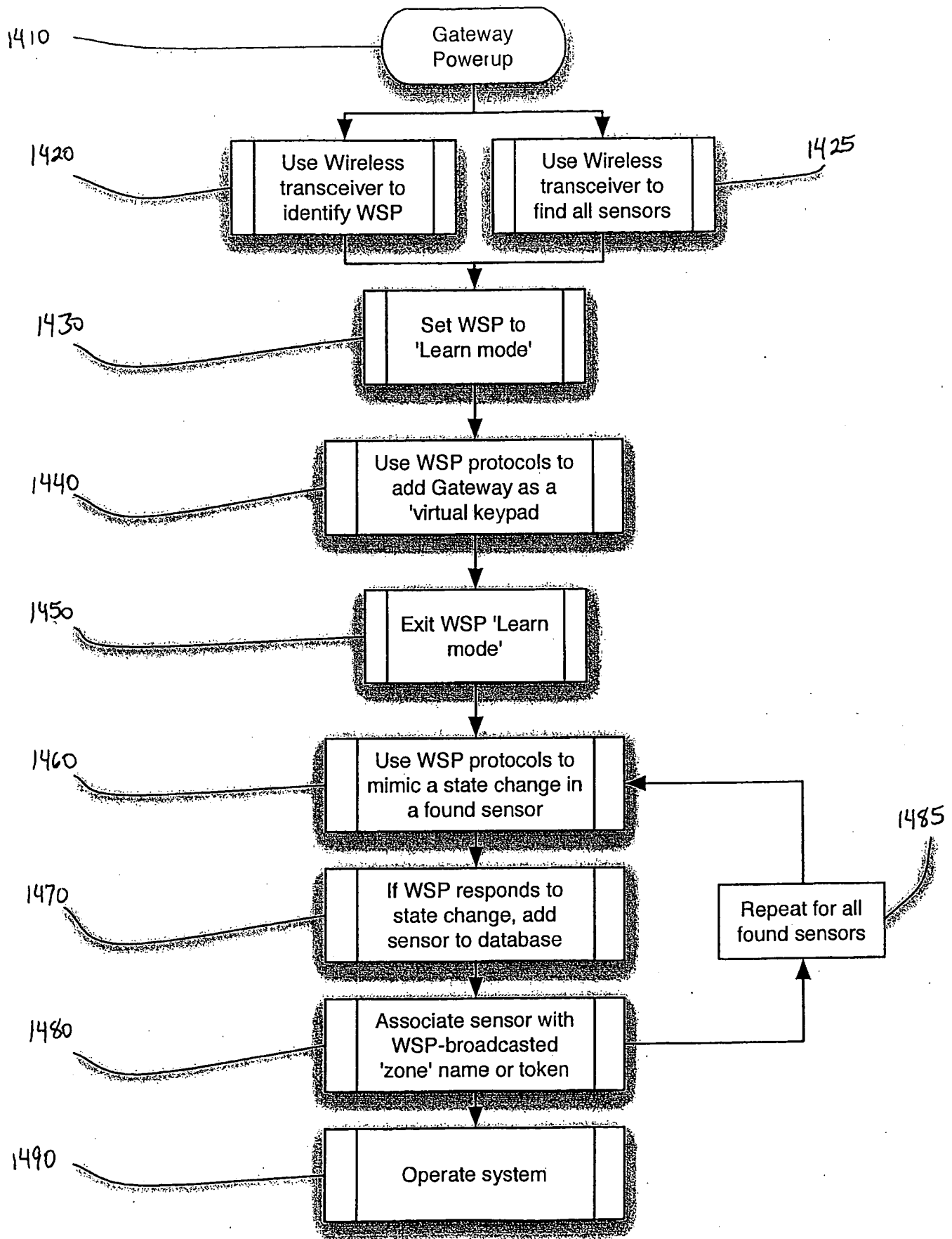


FIG. 14