Exhibit B

US008843641B2

(12) **United States Patent**
Falk

(10) **Patent No.: US 8,843,641 B2**
(45) **Date of Patent: Sep. 23, 2014**

(54) **PLUG-IN CONNECTOR SYSTEM FOR PROTECTED ESTABLISHMENT OF A NETWORK CONNECTION**

(75) Inventor: **Rainer Falk**, Erding (DE)

(73) Assignee: **Siemens Aktiengesellschaft**, Munich (DE)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 262 days.

(21) Appl. No.: **13/110,690**

(22) Filed: **May 18, 2011**

(65) **Prior Publication Data**

US 2011/0289231 A1 Nov. 24, 2011

(30) **Foreign Application Priority Data**

May 21, 2010 (DE) 10 2010 021 257

(51) **Int. Cl.**
G06F 13/00 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/10*** (2013.01); *H04L 63/0853* (2013.01)
USPC **709/227**; 709/229

(58) **Field of Classification Search**
CPC H04L 63/10; H04L 63/0853
USPC 709/227–229; 726/3–10, 16–21, 34; 713/160–163, 168–174, 184–186, 192, 713/194
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,167,078	B2 *	1/2007	Pourchot	340/5.61
7,509,676	B2 *	3/2009	Trueba	726/22
7,565,529	B2 *	7/2009	Beck et al.	713/156
8,146,072	B2 *	3/2012	Trueba	717/170
8,458,293	B1 *	6/2013	Lemaitre et al.	709/218
2005/0184856	A1	8/2005	Pourchot	
2006/0026283	A1 *	2/2006	Trueba	709/225
2006/0026686	A1 *	2/2006	Trueba	726/24
2006/0072527	A1 *	4/2006	Beck et al.	370/338
2007/0186099	A1 *	8/2007	Beck et al.	713/159
2009/0061678	A1	3/2009	Minoo et al.	
2009/0183233	A1 *	7/2009	Trueba	726/3

FOREIGN PATENT DOCUMENTS

DE	10 2005 040 984	3/2007
DE	10 2009 044 140	4/2010
EP	2034423	3/2009
WO	WO 2009/086937	7/2009
WO	WO 2010/040703	4/2010

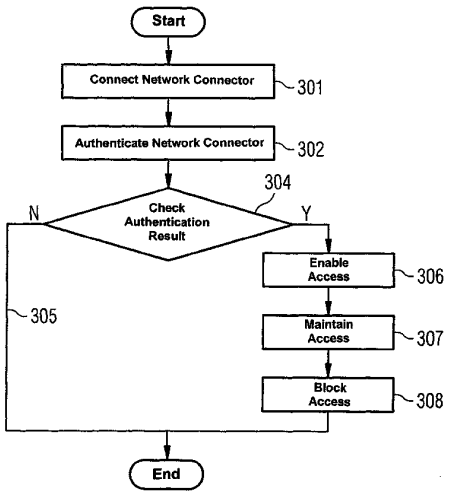
* cited by examiner

Primary Examiner — Kenneth Coulter
(74) *Attorney, Agent, or Firm* — Cozen O'Connor

(57) **ABSTRACT**

A plug-in connector system for a data communication interface comprising a network connector and a network socket is equipped with an integrated authentication function that is independent of network communication. The authentication is undertaken independently of the data transmission or the data communication. The enabling is undertaken by a physical connection between the contacts of the network socket, where the network connector associated therewith is established after successful authentication.

7 Claims, 2 Drawing Sheets



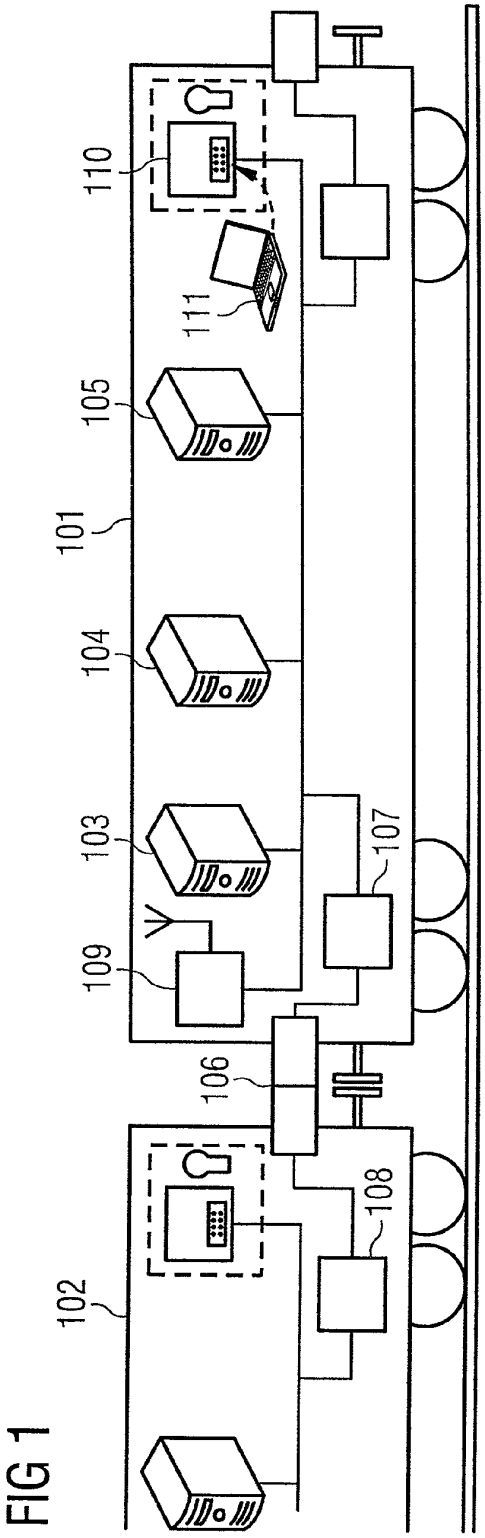


FIG 1

FIG 2

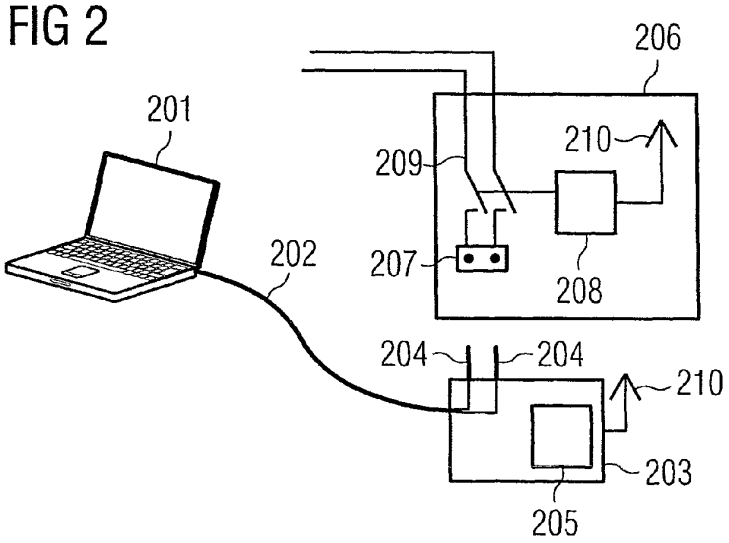
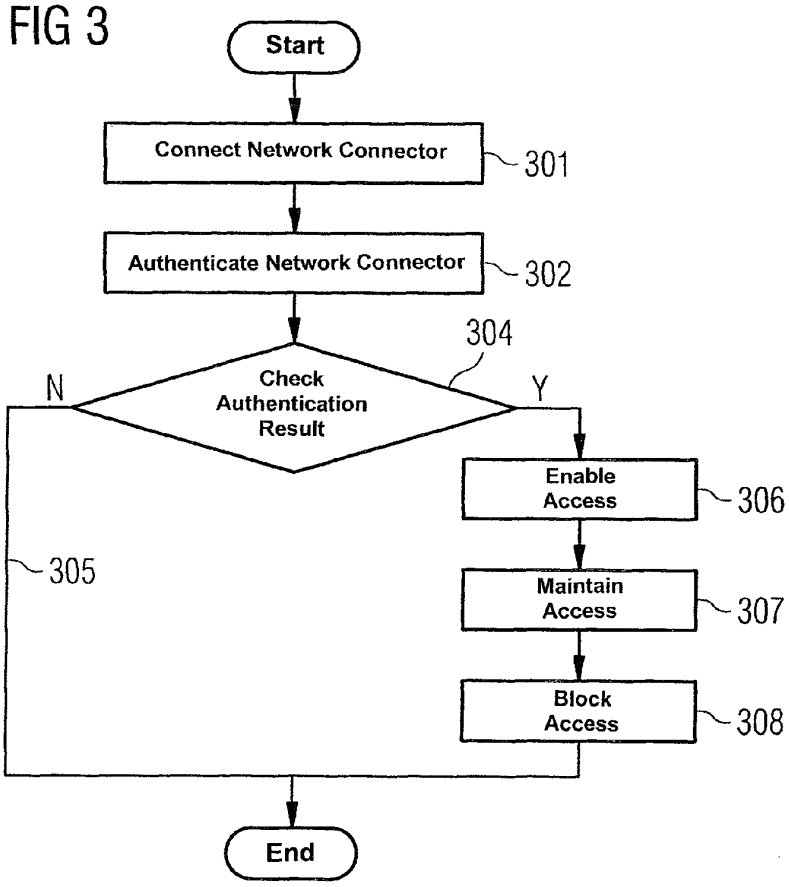


FIG 3



PLUG-IN CONNECTOR SYSTEM FOR PROTECTED ESTABLISHMENT OF A NETWORK CONNECTION

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a plug-in connector system, and a network plug and a network socket for protected establishment of a network connection, which is especially suitable for granting previously defined maintenance companies or maintenance technicians access to a system that is to be maintained.

2. Description of the Related Art

Technical devices require maintenance at regular intervals or in the event of malfunctions. To guarantee operational security, the maintenance should only be undertaken by authorized personnel. Consequently, it is necessary to allow only appropriately authorized personnel access to the maintenance functionality of the machine or system. For example, an owner of a machine can make it possible that only maintenance personnel who have completed the appropriate training have access to the machine to be maintained. Thus, on the one hand, the safety of the maintenance technician and, on the other hand, the correct operation of the machine to be maintained can be guaranteed.

In such cases, mobile maintenance devices, such as notebooks or PDAs (Personal Digital Assistants), are normally used, which obtain maintenance access by a locally accessible interface to a specific industrial device, such as a train, an interlocking system, an automation controller or a medical device. The connection to the locally accessible interface is made by wire or wirelessly. Diagnostic functions can be called up through the maintenance access, error memories read out, configuration settings of the industrial system modified or software updates uploaded.

To grant access rights, an authentication check is usually performed in which a claimed identity is verified and thus the authorization for accessing the respective maintenance interface is checked. If the authentication check is successful, the access rights previously allocated to the respective user are granted.

Most known authentication methods are based on the entity to be authorized having to prove, in relation to a checking entity, that it is in possession of a secret and/or of an object. The best known authentication method is the transmission of a password in which the authenticating entity transmits a secret password directly to a checking entity. The checking entity or the authentication checking unit respectively then check the correctness of the transmitted password.

For administration of maintenance accesses in large systems, however, such a method involves a significant administrative overhead. In particular, when temporary maintenance technicians or freelancers are used, the respective maintenance passwords should be changed again once maintenance on the system to be maintained has been completed so that future maintenance access is no longer possible for said persons.

A further known option for secure administration of maintenance accesses is to provide the respective network sockets for maintenance access in an area to which access is physically protected. For example, the network socket can be secured with a lockable maintenance flap or can be located in a lockable room. Such a method is, however, associated with uncertainties because a physical access protection can be overcome with little effort in most cases. In addition, this type of solution also demands significant administrative outlay, for example, for distributing and collecting the mechanical keys.

SUMMARY OF THE INVENTION

It is therefore in the object of the present invention to provide a system for administering and implementing access rights to maintenance functionalities that is operable securely and with little effort.

This and other objects and advantages are achieved in accordance with the invention by a plug-in connector system, a network plug and a network socket, wherein the inventive plug-in connector system for protected establishment of a network connection comprises a network plug featuring an authentication unit and a network socket featuring an authentication checking unit and an enabling unit. The authentication unit, the authentication checking unit and the enabling unit include devices for performing the following steps:

A checking command is transferred by the authentication checking unit to the authentication unit. Based the checking command, a checking response is determined by the authentication unit and transferred to the authentication checking unit. The checking response is checked by the authentication checking unit. In the event of a successful check of the checking response, a physical connection is enabled between the network plug and network socket for protected establishment of the network connection by the enabling device.

In the preferred embodiment, a plug-in connection for a data communication interface is equipped with an integrated authentication function independent of network communication. The data communication connection typically involves an RJ45 or M12 plug-in connection. Consequently, the network connector fulfils the function of a key, without a mechanical key being needed, however. The authentication is undertaken independently of data transmission or data communication, so that neither a maintenance device nor a device to be maintained has to support this functionality. The enabling is undertaken by a physical connection being established between the contacts of the network socket and the network plug connected to it.

In an embodiment of the present plug-in connector, after the establishment of a network connection for a network connector by a physically access-protected network socket, identification information of the network connector is stored. Based on the identification information, the network connector is checked at a predeterminable number of further network sockets. In other words, an inventive maintenance cable with authentication function is connected to a physically access-protected maintenance access. In this case, identification information of the network connector is captured and stored by the system to be maintained. Thereafter, further maintenance accesses of the same system will typically be used with this network connector for a certain predeterminable period of time, in which case only the identification information is checked. As a result, a physical access protection only present at some maintenance interfaces can be used to indirectly secure maintenance access by openly accessible maintenance interfaces.

In accordance with an embodiment of the present connector system, the network connector is allowed to set up a network connection for a predeterminable period of time and/or for a predeterminable scope of access rights. Accordingly, the authentication information of a network connector includes information about the maintenance accesses or the period of time for which the respective network connector is authorized and thus able to be used. This allows definition of the systems to which maintenance access is possible with a

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.