(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 October 2011 (13.10.2011)

PCT

(10) International Publication Number
WO 2011/124256 A1

(51) International Patent Classification:
G06F 21/20 (2006.01)

(21) International Application Number:
PCT/EP2010/054658

(22) International Filing Date:
8 April 2010 (08.04.2010)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **AREVA T&D UK LTD** [GB/GB]; St Leonards Avenue, Stafford Staffordshire ST17 4LX (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RICHARDS, Simon** [GB/GB]; 7 Salter Grange, Abbots Bromley, Staffordshire WS15 3DZ (GB). **BENHADDOU, Anas** [MA/FR]; Résidence sun city II, Appartement B207, 59, rue Vaissières, F-34000 Montpellier (FR).

(74) Agent: **ILGART, Jean-Christophe**; Brevalex, 95, rue d'Amsterdam, F-75378 Paris Cedex 8 (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD FOR ENSURING SAFE ACCESS TO AN INDUSTRIAL SITE

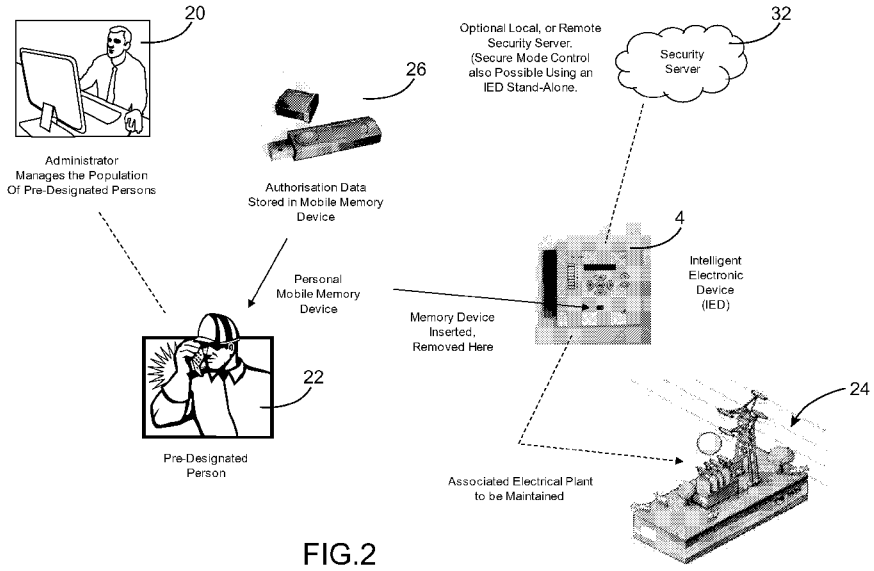

FIG.2

(57) Abstract: The invention concerns a method to ensure safe access to a critical Intelligent Electronic Device (4) connected to an industrial site (24) to perform maintenance operations of said critical IED (4), wherein only few pre-designated persons (22) are allowed to perform said maintenance operations. The method according to the invention comprises the step of providing the pre-designated persons (22) with exclusive authorisation data to maintain the IED (4) in a secure mode for safety of personnel during the maintenance operations and to put the IED (4) in its normal operational state after completion of said maintenance operations.

WO 2011/124256 A1

METHOD FOR ENSURING SAFE ACCESS TO AN INDUSTRIAL SITE

TECHNICAL DOMAIN

The invention pertains to the field of industrial process control, and more specifically, and concerns a method to ensure safe access to a critical devices connected to an Intelligent Electronic Devices (IED) in an industrial site to perform maintenance operations of said critical devices, wherein only a few pre-designated persons are allowed to perform said maintenance operations.

The invention also concerns architecture for managing safe access to a critical device connected to an Intelligent Electronic Devices (IED) in an industrial site to perform maintenance operations of said critical devices, wherein only a few pre-designated persons are allowed to perform said maintenance operations...

The term "industrial site" is used generically here, to include any utility or industrial station or substation, which houses electricity supply plant.

STATE OF PRIOR ART

Intelligent electronic devices (IEDs) are installed in electrical substations of electrical power systems, typically in an electricity generation, transmission, distribution, industrial or transport system. Their purpose is to measure, protect, control and monitor the system to which they are connected.

Today's IEDs are sophisticated software processing devices, and often each performs multiple

functions concurrently. In order to interface with the IEDs for configuration, setting, control, testing and interrogation purposes, a few pre-designated individuals need to gain access to the industrial site to perform specific maintenance operations.

In safety-critical applications, for example maintenance switching operations, it can be necessary for a suitably trained and authorised individual to prepare a safe environment within the industrial site to perform maintenance operations. As the location of the work is in or around low, medium or high voltage electrical apparatus, it may be necessary to temporarily disable or enhance some of the IED functionality, possibly to include:

- preventing close or open operations for the circuit breaker(s) associated with the apparatus,
- switching circuit breaker automatic reclosing functionality out of service,
- enabling faster or enhanced fault protection capability to limit the duration and energy of faults near staff as they perform their work, and/or
- Remove remote control capabilities to avoid distant control personnel operating the local apparatus.

In each case there is a need to verify that the individual concerned is authorised to make the change (authentication and authorisation, hereinafter abbreviated as "AA"), to log that change, and then when the temporary condition is required to be reset, to ensure that a suitably authorised individual can return the IED back to its normal operational state.

The Authentication, Authorisation and Accounting (AAA) of users' access to critical devices within the system is often performed by a specific security server AAA which provides these AAA services to all critical devices in the system. Typically the security server AAA is present on the same local area network as the devices that use it, but may also be located remotely from these devices and may be accessed through gateways and routers to a communications infrastructure connected to the process control system's LAN.

Figure 1, schematically illustrates a typical local network (LAN) 2 comprising a critical device 4 and a user station 6 locally connected to the LAN 2, a security server AAA 8 with local connection to the LAN 2. A security server AAA 10 may be remotely connected to the LAN 2 through a public network 12 such as Internet.

Known techniques of prior art by which user authentication or access control can be attempted in IEDs are:

- Restricting access to the substation only to specified authorised personnel,
- Requiring the entering of passwords,
- Use of a removable mechanical key switch,
- Requiring a remote control operator to take action to lift any barring of access, typically after a telephone call.

When access to the substation is not only restricted to specifically-authorised personnel, it can no longer be assumed that those who are permitted to

enter the substation are by default deemed capable to work safely on, in or around substation IEDs. Thus, an additional level of authentication of the user's role is required, to ensure that he/she is permitted to undertake certain interactions with the IED.

Passwording is commonplace, but passwords are often assigned to a group of individuals, and then become widely known due to staff turnover. Consequently, security is then jeopardised.

Mechanical keyswitches are a physical item that can be activated, then the key extracted and either kept on the person of the authorised individual, or in a safe "lock-off" box. This can ensure that the IED return to normal operation is only possible when the key itself has been replaced and turned first. However, a mechanical key is not conducive to advances in IED technology, such as reductions in physical size.

In some conditions, remote access to the security servers may be impractical or impossible. In this situation, one of the reasons to seek IED access may be due to a failure or anomaly in the remote control interface, so a purely local means for an operator to authenticate is highly preferable.

An object of the present invention is to provide an authorized person with means to put the equipment in a "safe" operational state during the maintenance operations until completion of the work.

PRESENTATION OF THE INVENTION

The aim of the invention is achieved by means of a method to ensure safe access to a critical

Intelligent Electronic Device connected to an industrial site to perform maintenance operations of said critical IED, wherein only few pre-designated persons are allowed to perform said maintenance operations.

said method characterized by

The method according to the invention comprises the step of providing the pre-designated persons with exclusive authorisation data to maintain the IED in a secure mode for safety of personnel during the maintenance operations and to put the IED in its normal operational state after completion of said maintenance operations.

In a preferred embodiment of the invention, the method comprises the steps of:

- storing said authorization data in a mobile memory device,

and, before performing said maintenance operations,

- said pre-designated persons physically connect the mobile memory device to the Intelligent Electronic Device (4) in order to be authenticated,

- the Intelligent Electronic Device checks whether or not said pre-designated persons are authorized to perform said specific maintenance operations,

- if said pre-designated persons are authorized to perform said specific maintenance operations, the Intelligent Electronic Device allows said pre-designated persons to perform said maintenance operations,

- else, said pre-designated persons are not authorized to perform said specific maintenance operations.

Thanks to the invention, once placed in maintenance mode, the pre-designated person who instigated the maintenance has exclusive control over when the IED can be reverted to normal service.

In a preferred embodiment of the invention, the authorization data are managed by an administrator device capable to download said authorization data for a specific pre-designated person onto said mobile memory device.

According to another aspect of the invention, whilst the mobile memory device is connected to the IED, said IED periodically requests refreshment of said authorization data.

In a first variant of the invention, the mobile memory device is configured to spontaneously transfer said authorization data to the IED upon connection of said mobile memory device to said IED.

The authorization data transferred from the mobile memory device to the IED may be persistent and non-volatile.

In the method according to the invention, full control of the persistence of the secure condition is vested with a specific pre-designated person who instigated the Intelligent Electronic Device placement in secure mode.

The method according to the invention further comprises a restriction configuration according to which the administrator device may revoke

permanently or temporarily the authorization of interaction between the mobile memory device and the IED, and may restrict the number of IEDs to which access rights are authorised.

The mobile memory device may be a USB stick, a mobile phone or a PDA.

The method according to the invention is implemented by means of an architecture for ensuring safe access to a critical IED connected to an industrial site to perform maintenance operations of said critical IED, wherein only a few pre-designated persons are allowed to perform said maintenance operations.

According to the invention, said architecture comprises means for providing the pre-designated persons with exclusive authorisation data to maintain the IED in a secure mode for safety of personnel during the maintenance operations and to put the IED in its normal operational state after completion of said maintenance operations

:

Said architecture further comprises:

- means for storing said authorization data in a mobile memory device,
- means for allowing said pre-designated persons to perform said maintenance operations only if said pre-designated persons are actually authorised to perform said specific maintenance operations,
- means for putting the IED in a secure mode for safety of personnel, the public, and equipment, during the course of the maintenance work.

Said architecture further comprises means for transferring authorisation data from the mobile memory device to the IED upon physical connection of said mobile memory device to said IED and means for periodically checking the pre-designated person authorisation data.

Preferably, the architecture comprises means for retaining the credentials of who placed an IED in its secure condition, means for persisting the IED's residence in a secure test or maintenance mode, and means for ensuring exclusivity of the reversal of the secure mode, such that the return to normal service remains at the behest of the original initiator of the work.

In the architecture according to the invention, a mobile memory device which has remained inserted in the Intelligent Electronic Device during the maintenance work, or a mobile memory device which has been later inserted on completion of the work can be used to ascertain that the return to normal service can be permitted.

In another embodiment of the invention, a senior individual within an organisation may exceptionally take charge of the return to normal operation, for example in the event of loss of a memory device, staff absence, or staff shift changes.

BRIEF DESCRIPTION OF THE FIGURES

The forgoing summary, as well as the following detailed description, will be better understood when read in conjunction with the appended

figures illustrating an exemplary embodiment of the invention in which:

- figure 1 schematically illustrates a typical network (LAN) with local/remote connections,
- figure 2 schematically illustrates a functional architecture in which the method according to the invention is implemented,
- Figure 3 is a flow chart illustrating the primary steps of the method according to the invention.

DESCRIPTION OF A DETAILED EMBODIMENT OF THE INVENTION

Referring now to figure 2, an administrator 20 manages the population of pre-designated persons 22 that may be allowed to perform maintenance operations of a critical IED 4 (figure 1) located at an industrial site 24.

The administrator may be located in the industrial site 24 or in remote premises connected to said industrial site 24 via a secure communication link.

Each pre-designated person 22 is provided with a user station 6 (Figure 1) comprising a reception device for receiving from the administrator authorization data comprising a definition of the specific maintenance operations to perform in the critical IED 4, and with personal mobile memory device 26 capable of communicating with said user station 6 to recover the authorization data.

The user station 6 may be a laptop and the personal mobile memory device 26 may be a USB memory stick, for example.

In a first embodiment, the pre-designated person 22 stores in the mobile memory device 26 the authorization data received by the laptop from the manager 20 and connects said mobile memory device 26 to the IED 4 for transferring said data to the IED 30.

In a second embodiment, the IED 4 is configured to communicate with said laptop via a secure Wi-Fi link or a secure Bluetooth link in order to recover the authorization data transmitted to the laptop by the manager 20.

In both embodiments, after verification of the authorization data, the IED 4 is placed in a secure mode.

The steps of the first embodiment of the methods according to the invention will be described by reference to figure 3.

When a specific maintenance operation concerning a critical IED 4 must be performed in the industrial site 24, the administrator 20 designates a person or a group of persons 22 for this purpose by allocating authorization data to said person or group of persons. To do so, the administrator associates an identifier of each designated person 22 with said authorization data in an appropriate data set and transmits the data set through a secure link to the user stations 6 of the designated persons. Each designated person 22 stores the received data set in its personal mobile memory device 26.

Before starting the maintenance operations, each designated person 22 connects its mobile memory device 26 to the IED 4 (step 40) to transfer said authorization data to said IED 4.

At step 42, the IED 4 transmits said authorization data to the security server AAA 8 (figure 1) for verification.

At step 44, if the designated persons 22 are authenticated, the IED 4 is placed in a secure mode to allow said designated persons 22 to do maintenance operations.

At step 46, the authorized persons 22 access the IED 4 or to associated electrical plant to perform maintenance operations. At the end of said maintenance operations, the authorized persons 22 who accessed the IED 4 re-connect (step 48) the mobile memory device 26 to the IED 4 in order to transmit to said IED 4 a command intended to put back the IED 4 in a normal state.

At step 50, the IED 4 transmits said command to the security server AAA 8 to verify that the command comes from the the authorized persons 22 who accessed to the IED 4.

After the verification of step 50, only if the command is initiated by the authorized persons 22, the IED 4 returns to the normal state at step 52.

Optionally, after step 44, the authorized persons 22 may remove the mobile memory device 26 from the IED 4 and may keep it (step 62) in a private or secure place to prohibit non-authorized person from placing the IED 4 in a normal state while the

designated persons are still performing maintenance operations.

Only the authorized persons 22 may re-connect (step 64) the mobile memory device 26 to the IED 4 to transmit to said IED 4 a command intended to put back the IED 4 in a normal state.

Thanks to the invention, only the authorized persons designated by the administrator 20 have an exclusive responsibility for the time when to put the device in a secure mode and for the time when to put it back to a normal state.

CLAIMS

1. A method to ensure safe access to a critical Intelligent Electronic Device (4) connected to an industrial site (24) to perform maintenance operations of said critical IED (4), wherein only few pre-designated persons (22) are allowed to perform said maintenance operations, said method characterized by providing the pre-designated persons (22) with exclusive authorisation data to maintain the IED (4) in a secure mode for safety of personnel during the maintenance operations and to put the IED (4) in its normal operational state after completion of said maintenance operations.

2. A method according to claim 1, further comprising the steps of:

- storing said authorization data in a mobile memory device (26),

and, before performing said maintenance operations,

- said pre-designated persons (22) physically connect the mobile memory device (26) to the Intelligent Electronic Device (4) in order to be authenticated,

- the Intelligent Electronic Device (4) checks whether or not said pre-designated persons (22) are authorized to perform said specific maintenance operations,

- if said pre-designated persons (22) are authorized to perform said specific maintenance

operations, the Intelligent Electronic Device (4) allows said pre-designated persons (22) to perform said maintenance operations,

- else, said pre-designated persons (22) are not authorized to perform said specific maintenance operations.

3. A method according to claim 2, wherein the authorization data are managed by an administrator device (20) capable to download said authorization data for a specific pre-designated person (22) onto said mobile memory device (26).

4. A method according to claim 2, wherein, whilst the mobile memory device (26) is connected to the IED (4), said IED (4) periodically requests refreshment of said authorization data.

5. A method according to claim 2, wherein the mobile memory device (26) is configured to spontaneously transfer said authorization data to the IED (4) upon connection of said mobile memory device (26) to said IED (4).

6. A method according to claim 2, wherein full control of the persistence of the secure condition is vested with a specific pre-designated person (22) who instigated the IED (4) placement in secure mode.

7. A method according to claim 6 further comprising a restriction configuration according to

which the administrator device (20) may revoke permanently or temporarily the authorization of interaction between the mobile memory device (26) and the IED (4), and may restrict the number of IEDs (4) to which access rights are authorised.

8. A method according to claim 1, wherein the mobile memory device (26) is a USB stick.

9. A method according to claim 1, wherein the mobile memory device (26) is mobile phone Or a PDA (personal Digital Assistant).

10. An architecture for ensuring safe access to a critical IED (4) connected to an industrial site (24) to perform maintenance operations of said critical IED (4), wherein only a few pre-designated persons (22) are allowed to perform said maintenance operations, said architecture characterized by:

-means for providing the pre-designated persons (22) with exclusive authorisation data to maintain the IED (4) in a secure mode for safety of personnel during the maintenance operations and to put the IED (4) in its normal operational state after completion of said maintenance operations

11. An architecture according to claim 10 further comprising:

-

- means for storing said authorization data in a mobile memory device (26),

- means for allowing said pre-designated persons (22) to perform said maintenance operations only if said pre-designated persons (22) are actually

authorised to perform said specific maintenance operations,

- means for putting the IED (4) in a secure mode for safety of personnel, the public, and equipment, during the course of the maintenance work.

12. An architecture according to claim 11 further comprising means for transferring authorisation data from the mobile memory device (26) to the IED (4) upon physical connection of said mobile memory device (26) to said IED (4).

13. An architecture according to claim 12 comprising means for periodically checking the pre-designated person authorisation data.

14. An architecture according to claim 12 comprising means for retaining the credentials of who placed an IED (4) in its secure condition.

15. An architecture according to claim 12 comprising means for persisting the IED's residence in a secure test or maintenance mode.

16. An architecture according to claim 12 comprising means for ensuring exclusivity of the reversal of the secure mode, such that the return to normal service remains at the behest of the original initiator of the maintenance work.

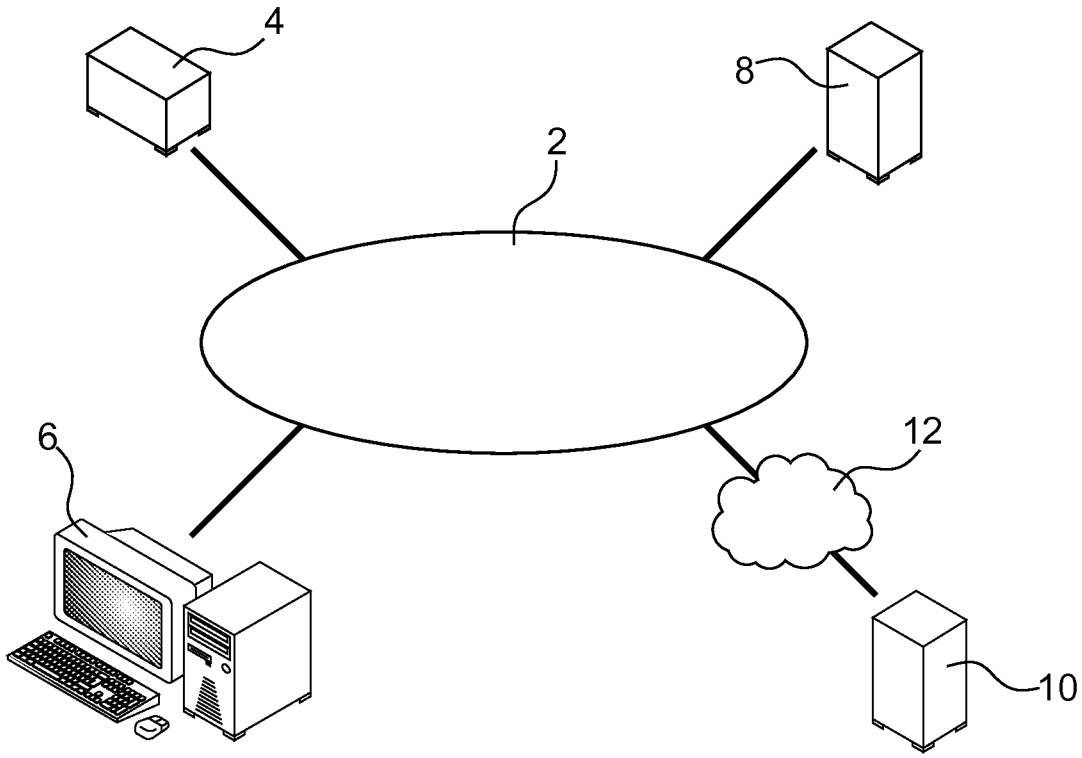

FIG.1

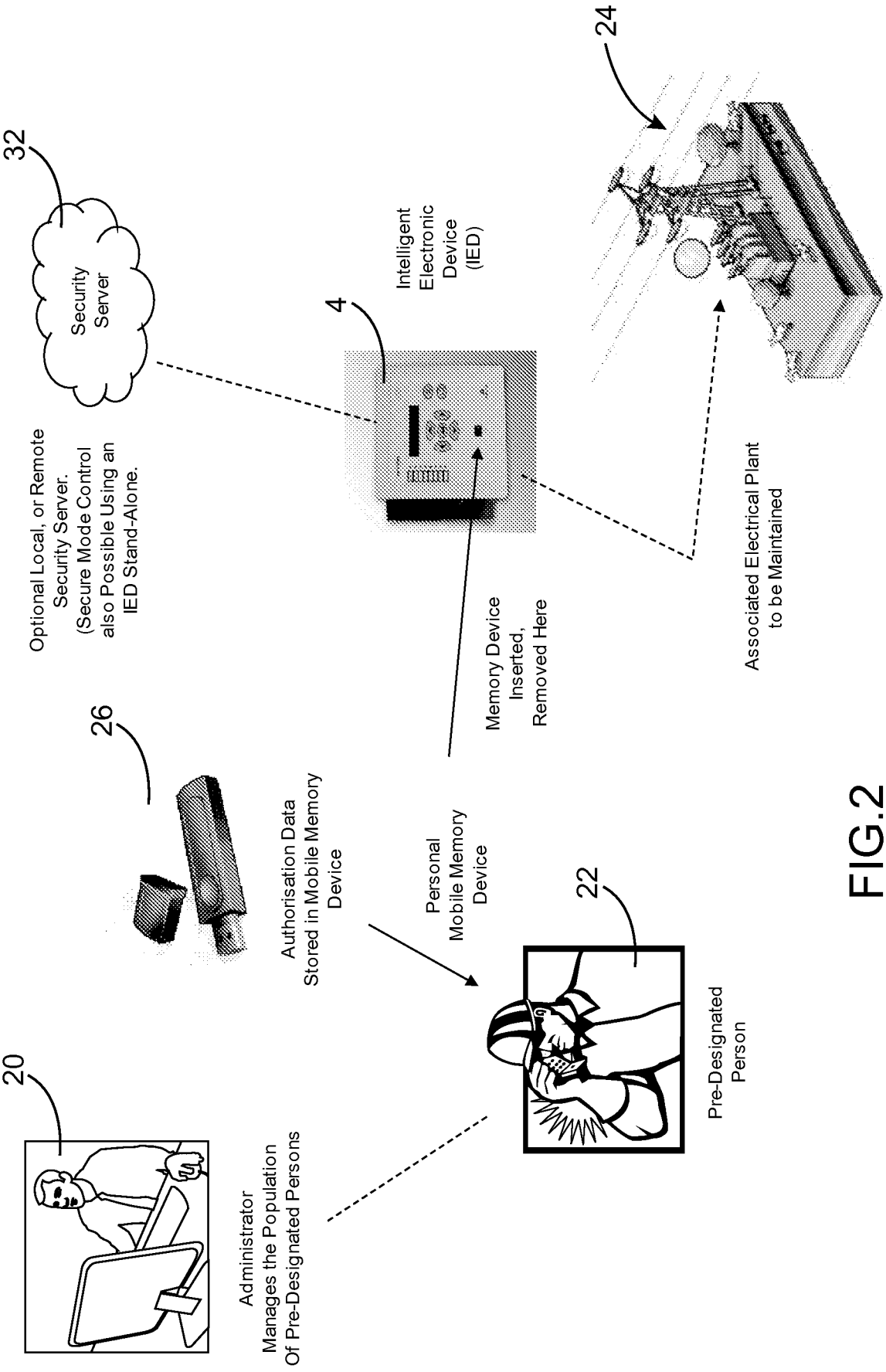
32
Security Server
Optional Local, or Remote Security Server. (Secure Mode Control also Possible Using an IED Stand-Alone.
4
Intelligent Electronic Device (IED)
24
Memory Device Inserted, Removed Here
Associated Electrical Plant to be Maintained
26
Authorisation Data Stored in Mobile Memory Device
Personal Mobile Memory Device
22
Pre-Designated Person
20
Administrator Manages the Population Of Pre-Designated Persons

FIG.2

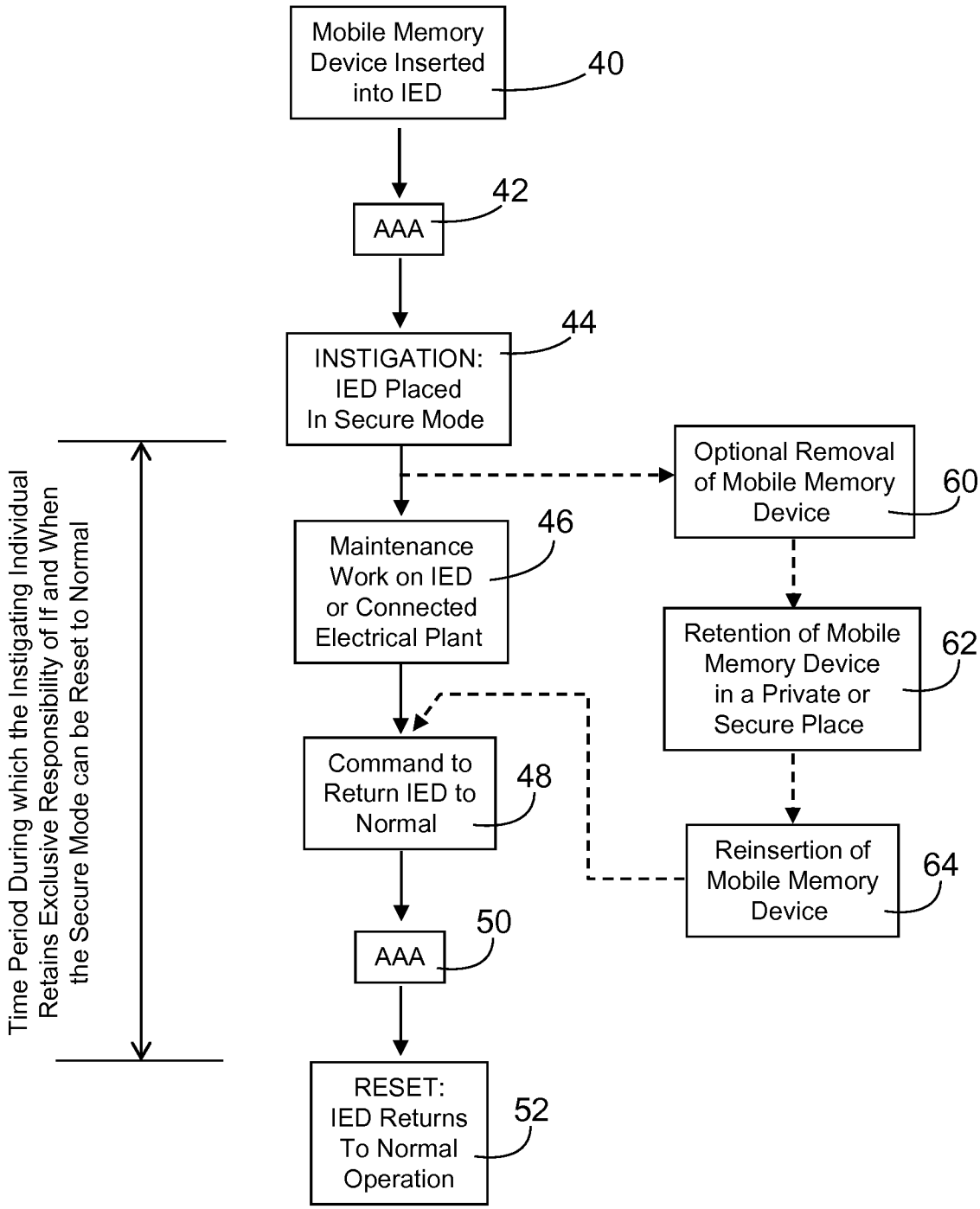
Mobile Memory Device Inserted into IED
40
AAA
42
INSTIGATION: IED Placed In Secure Mode
44
Optional Removal of Mobile Memory Device
60
Maintenance Work on IED or Connected Electrical Plant
46
Retention of Mobile Memory Device in a Private or Secure Place
62
Command to Return IED to Normal
48
Reinsertion of Mobile Memory Device
64
AAA
50
RESET: IED Returns To Normal Operation
52
Time Period During which the Instigating Individual Retains Exclusive Responsibility of If and When the Secure Mode can be Reset to Normal

FIG.3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/054658

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/20
ADD.

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)
G06F

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)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 037 651 A1 (ABB TECHNOLOGY AG [CH]) 18 March 2009 (2009-03-18) page 2, paragraphs 2,8 page 4, paragraph 17 page 4, paragraph 20 - paragraph 28 claim 1	1-16
A	MARTIN NAEDELE ED - ANONYMOUS: "An Access Control Protocol for Embedded Devices" INDUSTRIAL INFORMATICS, 2006 IEEE INTERNATIONAL CONFERENCE ON, IEEE, PI, 1 August 2006 (2006-08-01), pages 565-569, XP031003414 ISBN: 978-0-7803-9700-2 page 566, left-hand column, line 1 - line 18	7,14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family 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	Date of mailing of the international search report
21 September 2010	29/09/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Arbutina, Ljiljana

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/054658

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2037651 A1	18-03-2009	CN 101803331 A	11-08-2010
		EP 2186298 A1	19-05-2010
		WO 2009034018 A1	19-03-2009
		US 2010186075 A1	22-07-2010