(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 392 191 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
24.10.2018 Bulletin 2018/43

(51) Int Cl.:
B66B 25/00 *(2006.01)* ***B66B 1/34*** *(2006.01)*

(21) Application number: **17167610.9**

(22) Date of filing: **21.04.2017**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA MD

(71) Applicant: **Inventio AG**
6052 Hergiswil (CH)

(72) Inventor: **BÜNTER, Adrian**
6074 Giswil (CH)

(54) **ELEVATOR CONTROL SYSTEM**

(57) Communication apparatus comprising: a communication device (1) with at least one microprocessor (101); at least one cryptoprocessor (102); and memory (103) having instructions stored thereon that, when executed by the at least one microprocessor and the at least one cryptoprocessor, cause the communication device to at least one of:
Receive from the cloud (5) encrypted data that is configured to control at least core operations associated with an elevator or escalator device (34, 35, 36),
decrypt the data, and distribute the data over at least one data connection between the communication device (1) and at least one core controller (24) associated with said elevator or escalator device (34, 35, 36) to said at least one core controller (24) to be used by said core controller (24) to control at least core operations associated with said elevator or escalator device (34, 35, 36), or
receive control feedback data over at least one data connection between the communication device (1) and at least one core controller (24) associated with an elevator or escalator device (34, 35, 36) to said at least one core controller (1), encrypt the data, and send the encrypted data to the cloud (5).
Encrypting the data which is communicated between the communication devices allows to maintain the security level obtained with conventionally controlled elevator and escalator devices even when control over non-core functionalities are moved or relocated to remote devices or into the cloud in general.

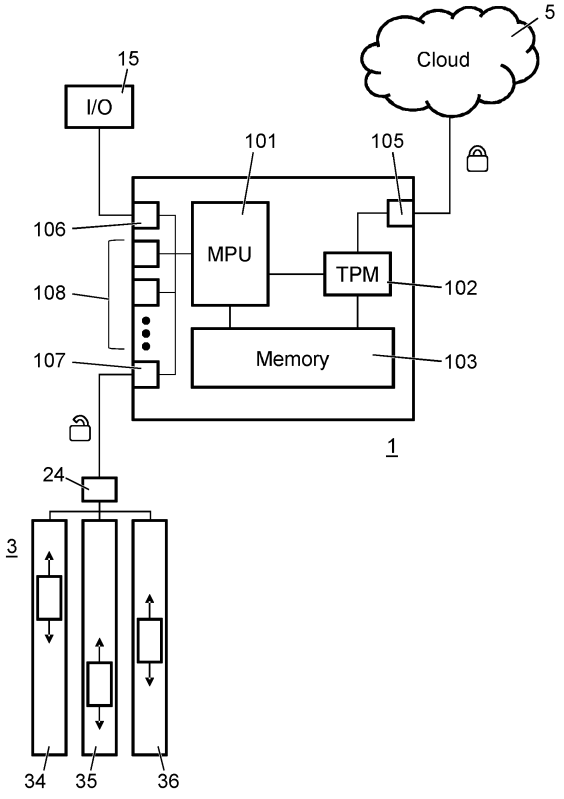

Fig. 2

EP 3 392 191 A1

Description

BACKGROUND

[0001] The present invention relates to the field of elevator and escalator devices. More specifically, it relates to a communication device, a method and a system for communicating between a core controller associated with an elevator or escalator device and a cloud server.

[0002] In conventional elevator or escalator systems, control software is stored and operated locally on a control board at each instance or installation. Adding or modifying functionality requires service personnel to manually update the software on the control board or download the software to a local unit via a remote connection. A software upgrade may require a corresponding processor and memory upgrade.

[0003] Functions and capabilities continue to be added to elevator controllers. Controller software might not be automatically upgraded unless manually executed at a user's request. Future functionality may someday reach the memory and computing power resource limitations in the existing control boards. At that point, a user may have to elect to forego incorporating additional functionality or otherwise incur large expenses upgrading a supporting hardware platform.

[0004] US 9067760 B2 describes a method for communication between an elevator system and a remote control center, that includes establishing a communication connection in a communication network. A first signal of the elevator system is received by a communication device of the elevator system through a signal network, and a second signal is transmitted by the communication device in the communication network to a computing apparatus of the remote control center. The communication connection is permanently maintained.

BRIEF SUMMARY

[0005] It is an object of the invention to improve an elevator or escalator system with a controller that comprises a core controller for core functionalities and has non-core functionalities moved or relocated from the core controller to another entity. Such improvements shall in particular concern integrity of the systems communication devices as well as security of data that is communicated between the different communication entities of the system.

[0006] An embodiment of the disclosure is directed to a method comprising: receiving, by a communication device linked to at least one core controller associated with an elevator or escalator device from a cloud server, encrypted data that is configured to control operations associated with the at least one elevator or escalator device, decrypting the data on the communication device; and forwarding the decrypted data from the communication device to the at least one core controller associated with the elevator or escalator device.

[0007] An embodiment of the disclosure is directed to a communication device with at least one microprocessor; at least one cryptoprocessor; and memory having instructions stored thereon that, when executed by the at least one microprocessor and the at least one cryptoprocessor, cause the communication device to at least one of: receive from a cloud server or a backend computer encrypted data that is configured to at least control core operations associated with an elevator or escalator device, decrypt the data, and distribute the data over at least one data connection between the communication device and at least one core controller associated with an elevator or escalator device to said at least one core controller to be used by said controller to control core operations associated with said elevator or escalator device, or receive control feedback data over at least one data connection between the communication device and at least one core controller associated with an elevator or escalator device to said at least one core controller, encrypt the data, and send the encrypted data to a cloud server or a backend computer.

[0008] An embodiment of the disclosure is directed to a system comprising: a first plurality of elevator or escalator devices; at least one core controller configured to control operations associated with the first plurality of elevator or escalator devices; a cloud server; and a first communication device linked to the at least one first core controller.

[0009] Encrypting the data which is communicated between the communication devices allows to maintain the security level obtained with conventionally controlled elevator and escalator devices even when control over non-core functionalities are moved or relocated to remote devices or into the cloud in general.

[0010] Additional embodiments are described below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Exemplary embodiments of the disclosed technologies are explained in detail with reference to the figures, in which:

FIG. 1 schematically shows a view of a portion of an elevator system which communicates with a cloud server and/ or a backend computer connected to the cloud; and

FIG. 2 schematically shows a view of a portion of a communication device in an elevator system as shown in Fig. 1.

DETAILED DESCRIPTION

[0012] It is noted that various connections are set forth between elements in the following description and in the drawings (the contents of which are included in this disclosure by way of reference). It is noted that these connections in general and, unless specified otherwise, may be direct or indirect and that this specification is not in-

tended to be limiting in this respect. In this respect, a coupling between entities may refer to either a direct or an indirect connection. Some connections are marked with an open or closed lock symbol, exemplarily indicating that information and data transported over these connections is encrypted (locked) or unencrypted (open).

[0013] Exemplary embodiments of apparatuses, systems, and methods are described for maintaining, updating/modifying, and upgrading an elevator system. In some embodiments, functionality typically associated with an elevator controller may be located in another device or entity, such as a smart communication gateway or on a cloud server. The elevator controller may communicate with the smart communication gateway and the cloud server to support selected control functions.

[0014] The term cloud or cloud computing shall in this specification have the meaning of internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. A cloud server is a computer device (server) that is connected to and can be contacted over the internet or any other comparable dedicated or open communication network.

[0015] Fig 1 shows an exemplary elevator system comprising several elevators 31 through 36 grouped in two exemplary groups of elevators.

[0016] On the left side of the drawing, a first group of elevators comprises an exemplary number of three elevators 31, 32 and 33, with dedicated core controllers 21, 22, 23. Each core controller controls at least core functionalities of the elevator that it is connected to. The three core controllers 21, 22 and 23 are connected to a first smart communication gateway, which is a communication device 11 with a memory, at least one microprocessor and interfaces to connect to input/ output (I/O) devices and/or a cloud 5 and at least one remote cloud server 6 or at least one backend computer device 4.

[0017] On the right side of the drawing, a second group of elevators comprises again an exemplary number of three elevators 34, 35 and 36, with one common core controller 24.

[0018] The common core controller controls at least core functionalities of the three elevators. The common core controller 24 is connected to a second smart communication gateway, which again is a communication device 12 with a memory, at least one microprocessor and interfaces to connect to I/O devices and/ or a cloud 5 and at least one remote cloud server 6 or at least one backend computer device 4.

[0019] The elevator system as shown if Fig. 1 is illustrative. In some embodiments, one or more of the entities may be optional. In some embodiments, additional entities not shown may be included. For example, in some embodiments the elevator system may be associated with one or more networks, such as one or more computer or telephone networks. In some embodiments, the entities may be arranged or organized in a manner different from what is shown in FIG. 2.

[0020] The system may include one or more elevators, such as elevators 31 to 36. The elevators 31, 32 and 33 may be included in a first elevator group 3. The elevators 34, 35 and 36 may be included in a second elevator group. For example, the first elevator group may include some or all of the elevators at a particular location, such as a building and the second elevator group may include some or all of the elevators at another particular location, such as another building.

[0021] While three elevators 31, 32 and 33 and 34, 35 and 36 are shown in FIG. 1 in respective groups, an elevator group may include more or less than three elevators.

[0022] The elevator group may include one or more core controllers, such as dedicated core controllers 21, 22 and 23 for the first elevator group and a common core controller 24 for the second elevator group. In the first elevator group, core controller 21 may be associated with elevator 31, core controller 22 may be associated with elevator 32 and core controller 23 may be associated with elevator 33. In the second group of elevators, core controllers are combined, such that a common core controller 24 may be associated with all of the three elevators 34, 35 and 36.

[0023] In conventional systems, a controller may have been responsible for the operation of an elevator or a group of elevators. In this respect, in conventional systems a controller includes all the hardware and software needed to implement control functionality with respect to elevators that were overseen or regulated by the controller.

[0024] In accordance with one or more embodiments of this disclosure, selected controller functionality, especially non-core functionality or not security relevant functionality, may be moved or relocated from a controller to another entity, such as a communication device or a cloud server. By moving non-core functionality to another entity, a reduction in hardware within the controller included in an elevator or an elevator group may be realized. In this respect, controller design may be simplified, which may result in a more reliable core controller. Changes in functionality may also be made at one central location, the cloud server, resulting in a consistent implementation across multiple controllers and/or elevator groups simultaneously and without requiring manual intervention at a local site, at the elevator or the elevator group. In some embodiments, elevator groups may be remotely located from one another, for example in different buildings.

[0025] The core controllers of the elevators or the elevator groups may communicate with the cloud server via a communication device (smart communication gateway) over one or more connections, channels, or links. Such connections may adhere to one or more communication protocols, standards, or the like. For example, the connections may adhere to landline telephone, cellular (GSM, UMTS, LTE or any future mobile cellular system standard), wireless local area networking (Wi-Fi),

Ethernet (local (LAN), metropolitan (MAN) or wide (WAN) area network), satellite, or cable communications. In some embodiments, the connections may be constant or persistent.

[0026] In accordance with one or more embodiments of this disclosure, the communication device 1, 11, 12 may take over some of the functionality of the controller known from the conventional systems and thereby become part of the controller itself. The communication device may receive encrypted data from the cloud or a cloud server, which data is, when decrypted by the communication device and executed on the communication, configured to control core operations associated with an elevator or an elevator group. Therefore, and in accordance with an embodiment of this disclosure, control data is forwarded to the at least one core controller by the communication device.

[0027] Controller functionality other than core controller functionality may be executed on a cloud server. Such functionality may include non-core functions for an elevator or a group of elevators, operational mode determinations, diagnostic functions, special contract features, etc. Regarding non-core functions, in some embodiments a user request for service received at, e.g., a hall box located on a particular floor of a building may be communicated to the cloud server and the cloud server may transmit a command to the core controller that eventually directs a specified elevator car to relocate to that particular floor to fulfill the service request.

[0028] A local core controller associated with an elevator or a group of elevators may maintain some functionality, and as such, may include hardware and computing resources to support such functionality, especially core functionality like accelerating, decelerating, braking, resulting in movement at specific speeds in upward or downward directions, other core functionality like opening and closing doors and, in particular, safety relevant functionality.

[0029] A core controller may include hardware and/or software to communicate with a cloud server via a communication device (smart communication gateway). For example, a core controller may exchange data and commands with the cloud server to perform control functions. The cloud server may store contract setup parameters for select functions. In some embodiments, the contract setup parameters may be stored in the core controller. In some embodiments, there may be a simplified failover functionality located in the core controller in the event that there is a connection loss between the core controller and the communication device and/ or the communication device and the cloud server.

[0030] In some embodiments, operational metrics from elevators may be collected at a cloud server across a portfolio of multiple units, sites, or groups. The metrics may be filtered at a communication device linked to the core controller of an elevator or a group of elevators, encrypted for secure communication by the communication device, forwarded to, decrypted and analyzed by cloud services or a backend computer to provide a broad view of the portfolio. Metrics may be used to create insights that can be turned into actions that provide real business outcomes. For example, the analysis may indicate trends and may be used to respond to needs. The analysis may also be used to facilitate diagnostic or troubleshooting capabilities. Metrics may be used to trigger or enhance the accuracy of sales proposals. Metrics may be used to provide or schedule maintenance activities, such as preventative maintenance activities.

[0031] In some embodiments, interface protocols for, e.g., new devices may be stored in a cloud server and used by a communication device and/ or a local core controller.

[0032] In some embodiments, functional upgrades for diagnostics, prognostics, and remote repair/rescue functions can be deployed to customers as they are released and deployed into a cloud server. Functionality may be developed at the backend computer and deployed to the cloud server. One or more tests may be executed to ensure that the functionality satisfies operational or safety requirements.

[0033] In some embodiments, a modernization of cloud supported core controllers may be provided. Core controllers may utilize a cloud or cloud server to enable new features or support new devices/equipment. Before or during the modernization, the communication device linked to the core controller may receive updates via the cloud to support interface protocols to new equipment and/or add new functions/capabilities. For example, if a new fixture is added requiring a new interface, a core controller may enable the new functionality from the cloud once the new fixture has been integrated into the system without requiring an upgrade of software on the core controller. As yet another example, a new core algorithm may be implemented from the cloud to optimize traffic during the modernization phase of the project.

[0034] Fig 2 shows an exemplary communication system which includes a communication device 1, above also referred to as smart communication gateway. The communication device 1 comprises memory 103 for storing executable instructions and data. The executable instructions may be stored or organized in any manner and at any level of abstraction, such as in connection with one or more processes, routines, procedures, methods, functions, etc.

[0035] The instructions stored in the memory 103 may be executed by one or more microprocessors, such as a main processor unit 101. The processor may be coupled to one or more I/O devices 15 by means of exemplary first communication interface 106. In some embodiments, the I/O device(s) 15 may include one or more of a keyboard or keypad, a touchscreen or touch panel, a display screen, a microphone, a speaker, a mouse, a button, a remote control, a joystick, a printer, a telephone or mobile device (e.g., a smartphone), etc. The I/O device(s) 15 may be configured to provide an interface to allow a user to interact with the communication device 1.

[0036] To allow communication to and through the communication device 1 the device has several communication interfaces 105 to 107. An exemplary second communication interface 105 connects the communication device to the cloud. Exemplary third communication interface 107 connect the communication device to the at least one core controller of an associated elevator or group of elevators.

[0037] The communication device 1 further comprises a cryptoprocessor 102, which is a dedicated microcontroller designed to secure the hardware of the communication device 1 by integrating cryptographic keys into the device. Such a cryptoprocessor is commonly known as Trusted Platform Module. The cryptoprocessor has the primary scope to assure integrity of the communication device within an elevator communication system comprising several components in remote locations, such as elevators, groups of elevators, core controllers of elevators, core controllers of groups of elevators, communication devices (smart communication gateways), cloud servers, backend computers, etc.

[0038] Communication to and from the elevator core controller(s) through the communication device 1 is encrypted/ decrypted using the cryptoprocessor 102. Communication content integrity and security, as well as system components identity authentication can be further improved with the use of cryptoprocessors. In this context "integrity" means "behave as intended". Also, with the use of secure cryptoprocessors, or dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices in general, access to the communication system is less prone to "dictionary attacks" compared to pure software implemented authentication mechanisms. With the implementation of cryptograpfic keys in a dedicated hardware module, a dictionary attack prevention mechanism is created, which effectively protects against guessing or automated dictionary attacks. Without this level of protection, only passwords with high complexity would provide sufficient protection.

[0039] While some of the examples described herein related to elevators, aspects of this disclosure may be applied in connection with other types of conveyor devices, such as an escalator, a moving sidewalk, a wheelchair lift, or groups of such conveyor devices, etc.

[0040] Embodiments of the disclosure may be used to reduce local controller hardware and/or software. For example, functionality may be at least partially supported by one or more servers, such as one or more cloud servers. Increased or upgraded functionality may be provided without impacting local controller memory or processing requirements/capacities.

[0041] Embodiments of the disclosure may have high-level control functionality implemented remote from an elevator. Functionality may be modified off-line. Functionality may be pushed from a cloud server to one or more elevators once the functionality is available. In some embodiments, an elevator may be configured to request functionality via, e.g., a pull-model.

[0042] Embodiments of the disclosure may be tied to one or more particular machines. For example, a controller may be configured to communicate with a cloud server. The cloud server may store data that may be used to control one or more functions associated with an environment or application. The data may be communicated from the cloud server to the controller to support operations within the environment or application.

[0043] As described herein, in some embodiments various functions or acts may take place at a given location and/or in connection with the operation of one or more apparatuses, systems, or devices. For example, in some embodiments, a portion of a given function or act may be performed at a first device or location, and the remainder of the function or act may be performed at one or more additional devices or locations.

[0044] Embodiments may be implemented using one or more technologies. In some embodiments, an apparatus or system may include one or more processors, and memory storing instructions that, when executed by the one or more processors, cause the apparatus or system to perform one or more methodological acts as described herein. Various mechanical components known to those of skill in the art may be used in some embodiments.

[0045] Embodiments may be implemented as one or more apparatuses, systems, and/or methods. In some embodiments, instructions may be stored on one or more computer program products or computer-readable media, such as a transitory and/or non-transitory computer-readable medium. The instructions, when executed, may cause an entity (e.g., an apparatus or system) to perform one or more methodological acts as described herein.

Claims

1. A method comprising the steps of:

receiving, by a communication device (1, 11, 12) linked to at least one core controller (21, 22, 23, 24) associated with an elevator or escalator device (31, 32,..., 36) from a cloud server (6), encrypted data that is configured to control operations associated with the at least one elevator or escalator device (31, 32, ..., 36,),
decrypting the data with a cryptoprocessor (102) on the communication device (1, 11, 12); and
forwarding the decrypted data from the communication device (1, 11,12) to the at least one core controller (21, 22, 23, 24) associated with the elevator or escalator device (31, 32, ..., 36).

2. The method of claim 1, further comprising the step of:

receiving, by the cloud server (6), the encrypted data from a backend computer (4).

3. The method of claim 1, wherein the elevator or escalator device (31, 32, ..., 36) is included in a group of elevator or escalator devices (31, 32,..., 36).

4. The method of claim 3, wherein the core controller (21, 22, 23, 24) controls each of the elevator or escalator devices (31, 32,..., 36) in accordance with the data.

5. The method of claim 1, further comprising the steps of:

obtaining, by the communication device (1, 11, 12), second data regarding a status of an implementation of the data and/ or second data regarding the use of the data from the core controller (21, 22, 23, 24);
encrypting the second data with a cryptoprocessor (102) on the communication device (1, 11, 12); and
forwarding the decrypted second data from the communication device (1, 11, 12) to a cloud server (6) and/ or a backend computer (4).

6. The method of claim 1, further comprising the step of:

manipulating and/ or analyzing and/ or filtering the second data.

7. The method of claim 6, wherein manipulating and/ or analyzing and/ or filtering the second data is done by the communication device (1, 11, 12) and/ or the cloud server (6).

8. Communication device (1, 11, 12) with at least one microprocessor; at least one cryptoprocessor (102); and memory having instructions stored thereon that, when executed by the at least one microprocessor and the at least one cryptoprocessor (102), cause the communication device (1, 11, 12) to at least one of:

receive from a cloud server (6) or a backend computer (4) encrypted data that is configured to at least control core operations associated with an elevator or escalator device (31, 32,..., 36),
decrypt the data, and
distribute the data over at least one data connection between the communication device (1, 11, 12) and at least one core controller (21, 22, 23, 24) associated with an elevator or escalator device (31, 32, ..., 36) to said at least one core controller (21, 22, 23, 24) to be used by said controller to control core operations associated with said elevator or escalator device (31, 32, ..., 36), or
receive control feedback data over at least one data connection between the communication device (1, 11, 12) and at least one core controller (21, 22, 23, 24) associated with an elevator or escalator device (31, 32, ..., 36) to said at least one core controller (21, 22, 23, 24),
encrypt the data, and
send the encrypted data to a cloud server (6) or a backend computer (4).

9. Communication apparatus comprising a communication device (1, 11, 12) of claim 8, wherein the apparatus further comprises a cloud server (6).

10. Communication apparatus of claim 9, wherein the data is implemented as a software program, and wherein the apparatus receives the software program from a backend computer (4).

11. Communication apparatus of claim 10, wherein the software program is used to alter the instructions stored in the memory of the communication device (1, 11, 12).

12. Communication apparatus comprising a communication device (1, 11, 12) of claim 8, wherein the data connection to distribute the data to the core controller is at least one of:an analogue phone connection, a digital cellular communications connection, a Wi-Fi connection, an Ethernet connection, a satellite connection, and a cable communications connection.

13. A system comprising:

a first plurality of elevator or escalator devices (31, 32, ..., 36);
at least one core controller (21, 22, 23, 24) configured to control operations associated with the first plurality of elevator or escalator devices (31, 32, ..., 36);
a cloud server (6); and
a first communication device (1, 11, 12) of Claims 8 linked to the at least one first core controller (21, 22, 23, 24).

14. The system of claim 13, further comprising:

a second plurality of elevator or escalator devices (31, 32,..., 36) remotely located from the first plurality of elevator or escalator device (31, 32, ..., 36); and
a second communication device (1, 11, 12) linked to at least one second core controller configured to control at least core operations associated with the second plurality of elevator or escalator devices (31, 32, ..., 36).

15. The system of claim 14, wherein the cloud server (6) is configured to distribute encrypted data to the sec-

ond communication device (1, 11, 12) substantially the same time that the cloud server (6) distributes the encrypted data to the first communication device (1, 11, 12).

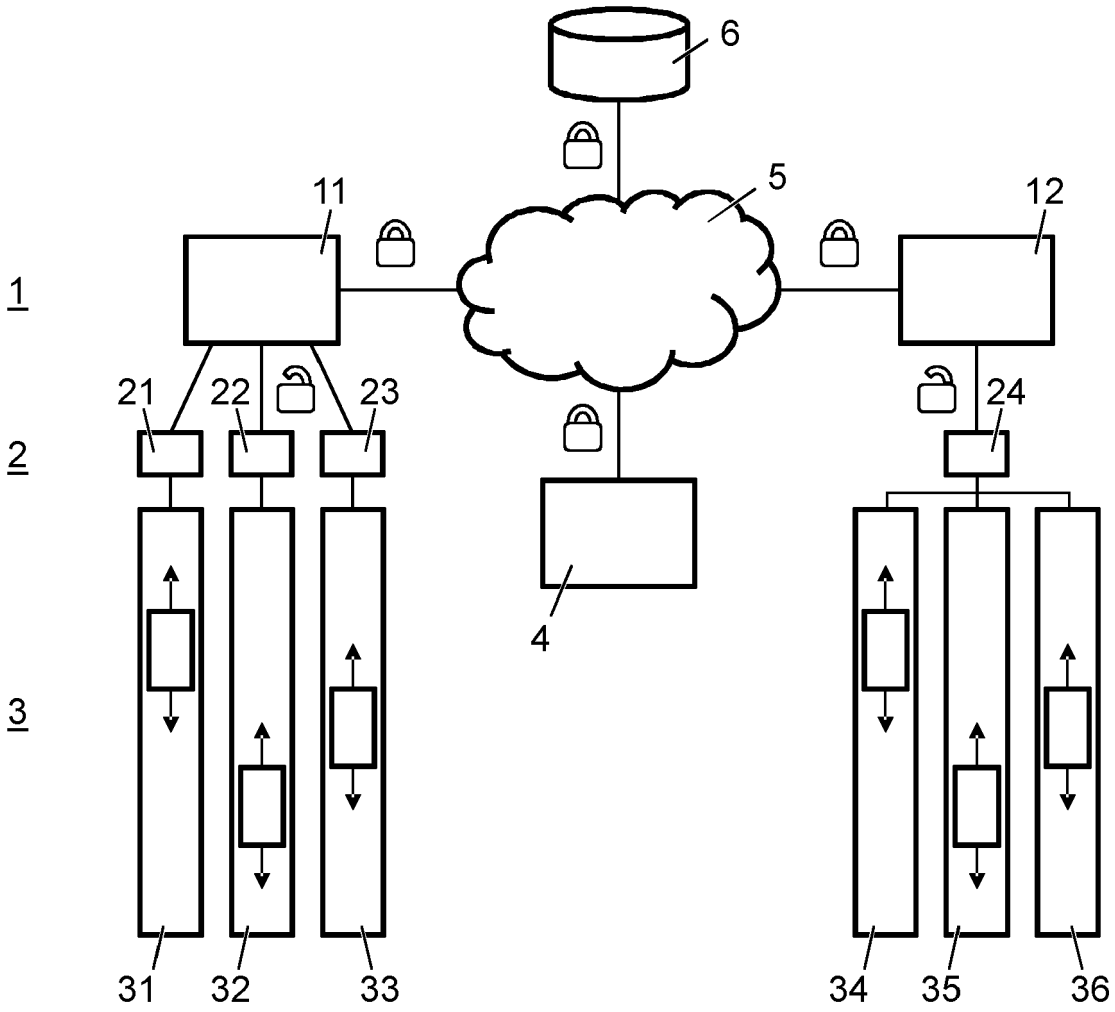

Fig. 1

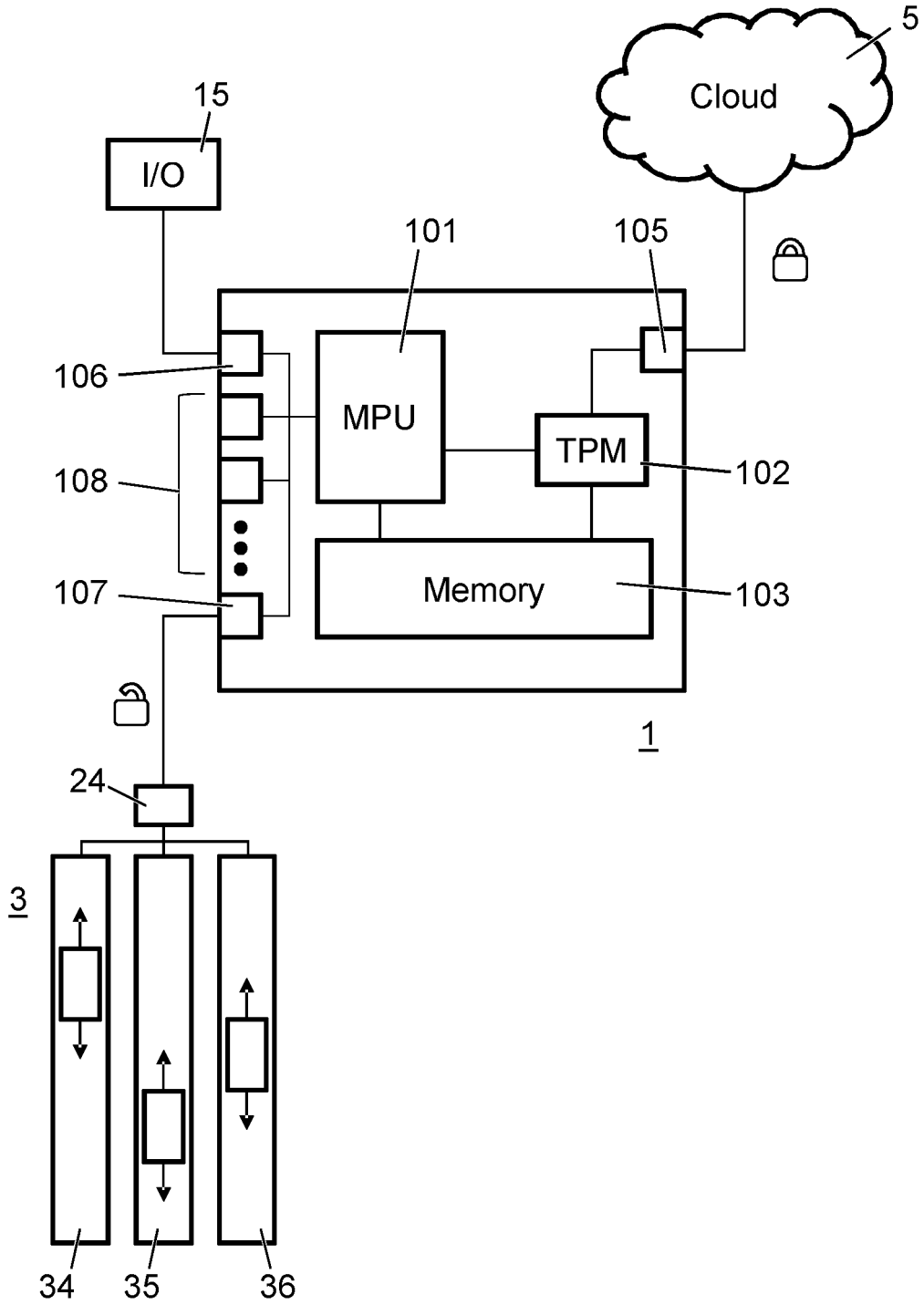
5
Cloud
15
I/O
101
105
106
MPU
TPM
102
108
Memory
103
107
1
24
3
34
35
36

Fig. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 17 16 7610

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	JP 2014 172714 A (HITACHI LTD) 22 September 2014 (2014-09-22) * paragraphs [0021], [0027], [0028], [0036], [0038], [0041], [0043]; figure 1 * -----	1-15	INV. B66B25/00 B66B1/34
A	CN 104 986 634 A (GUANGZHOU GUANGRI ELEVATOR INDUSTRY CO LTD) 21 October 2015 (2015-10-21) * figure 1 * -----	1-15	
A	& DATABASE WPI Week 201581 Thomson Scientific, London, GB; AN 2015-70540G & CN 104 986 634 A (GUANGZHOU CANTON ELEVATOR IND CO LTD) 21 October 2015 (2015-10-21) * abstract * -----	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

B66B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	3 October 2017	Janssens, Gerd

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 17 16 7610

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

03-10-2017

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2014172714 A	22-09-2014	CN 104030102 A	10-09-2014
		JP 2014172714 A	22-09-2014
CN 104986634 A	21-10-2015	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 9067760 B2 **[0004]**