



(12)

EUROPEAN PATENT APPLICATION

(43)

Date of publication:

18.12.2013 Bulletin 2013/51

(51)

Int Cl.:

G07C 9/00 (2006.01) E05B 17/00 (2006.01)

(21)

Application number: 12305666.5

(22)

Date of filing: 11.06.2012

(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	(72) Inventors: - Pontois, Cedric 91620 Nozay (FR) - Faucheux, Frédéric 91620 Nozay (FR)
(71) Applicant: Alcatel Lucent 75007 Paris (FR)	(74) Representative: Lebkiri, Alexandre et al Cabinet Camus Lebkiri 87 Rue Taitbout 75009 Paris (FR)

(54)

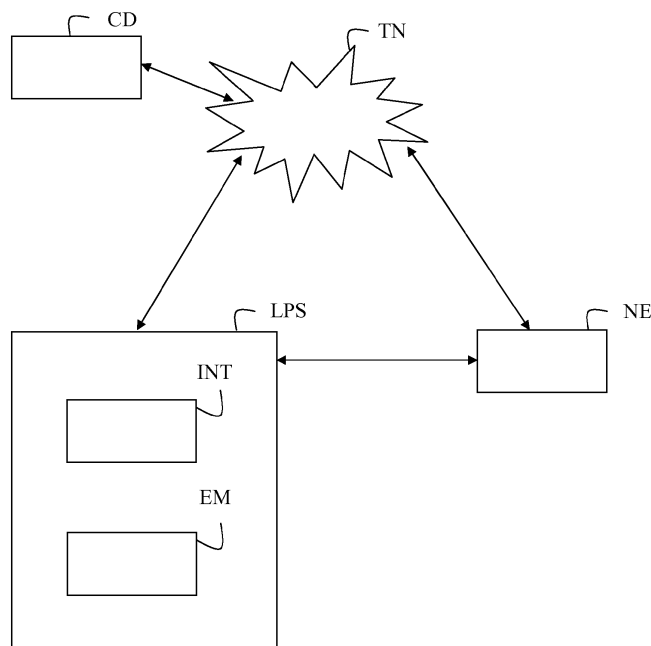
Protection at network element location

(57)

For protecting physical access through a lock mechanism to a network element (NE) in a telecommunication network (TN), a system (LPS) coupled to the lock mechanism comprises an interface (INT) for checking information about whether the network element (NE) is connected or not to the telecommunication network

(TN) and for checking information about a value of a software parameter (SP) indicating if the lock mechanism should be inhibited or not. The system activates an electromagnet for inhibiting the lock mechanism if the network element (NE) is connected to the telecommunication network (TN) and if the value of the software parameter (SP) indicates that the lock mechanism should be inhibited.

FIG. 1



Description

FIELD OF THE INVENTION

[0001] The present invention relates to a protection at network element location, especially at a base station of a telecommunication network or at a data center.

BACKGROUND

[0002] In general, access to a connected site is done through a door using a lock controlled by a key. Current solution to lock a site is to use basic cylinder sash lock that is easy to force for example with a screwdriver resulting in many door alarms for operators.

[0003] There is therefore a need to improve physical access security to connected sites such as base stations or data centers.

SUMMARY

[0004] To remedy the problems referred to hereinabove, a system for protecting physical access through a lock mechanism to a network element in a telecommunication network, the system being coupled to the lock mechanism and comprising:

means for checking information about whether the network element is connected or not to the telecommunication network,

means for checking information about a value of a software parameter indicating if the lock mechanism should be inhibited or not,

means for inhibiting the lock mechanism if the network element is connected to the telecommunication network and if the value of the software parameter indicates that the lock mechanism should be inhibited.

[0005] Advantageously, the mechanical lock of the network element, for example a base station, is automatically inhibited once the communication is established with the operator network. In this manner operator will be able to re-activate the mechanical lock if on-site maintenance is needed. If the network communication is broken between operator and base station, the mechanical lock is by default active.

[0006] Furthermore, the system prevents breaking on network element like base station by forcing the door lock resulting in many less alarm for operators, hence a reduction of maintenance costs. By consequence, preventing open doors will avoid at least the following problems:

- theft of hardware or other material present on site,
- vandalism
- overheating or too cooling of electronic boards,
- rain falling inside the network element like base station resulting in short circuit and outage.

[0007] Today, for a network element like base station, the lock mechanism like the door cylinder sash lock is visible and easy to force with a screw driver. By inhibiting the sash lock (either by hiding it behind a metal plate or by mechanically disconnecting the sash), the process to force the base station will be really more complicated.

[0008] In an embodiment, means for inhibiting the lock mechanism is an electromagnet that is linked to the lock mechanism and cooperates with a metallic object preventing the lock mechanism to work.

[0009] In an embodiment, the electromagnet is powered on by the system to cooperate with the metallic object.

[0010] In an embodiment, the system is connected to a device able to command the system and to attribute the value of the software parameter.

[0011] In an embodiment, the network element is a base station or a data center.

[0012] In an embodiment, physical access to the network element is access to a room inside the network element where hardware or electronic devices are located.

[0013] A further object of the invention is method for protecting physical access through a lock mechanism to a network element in a telecommunication network, comprising the following steps executed in a system coupled to the lock mechanism:

checking information about whether the network element is connected or not to the telecommunication network,

checking information about a value of a software parameter indicating if the lock mechanism should be inhibited or not,

inhibiting the lock mechanism if the network element is connected to the telecommunication network and if the value of the software parameter indicates that the lock mechanism should be inhibited.

[0014] The invention relates further to a computer program adapted to be executed in a system for a physical access protection of a network element in a telecommunication network, said program including instructions which, when the program is executed in said system, execute the steps of the method of the invention.

BRIEF DESCRIPTION OF THE FIGURES

[0015] Some embodiments of the present invention are now described, by way of example only, and with reference to the accompanying drawings, in which:

- FIG. 1 is a schematic block-diagram of a network element NE coupled to a lock protection system LPS,
- FIG. 2 is a flowchart showing steps performed to execute a process of physical access protection of a network element in a telecommunication network according to an embodiment of the invention,
- FIG. 3a is a schematic block-diagram of a lock pro-

tection system of a network element in a telecommunication network with keyhole protected according to an embodiment of the invention,

- FIG. 3b is a schematic block-diagram of a lock protection system of a network element in a telecommunication network with keyhole accessible according to an embodiment of the invention,
- FIG. 4a is a schematic block-diagram of a lock protection system of a network element in a telecommunication network in an inhibited lock state according to an embodiment of the invention, and
- FIG. 4b is a schematic block-diagram of a lock protection system of a network element in a telecommunication network in an active lock state according to an embodiment of the invention,

[0016] The same reference number represents the same element or the same type of element on all drawings.

DESCRIPTION OF EMBODIMENTS

[0017] The figures and the following description illustrate specific exemplary embodiments of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the invention and are included within the scope of the invention. Furthermore, any examples described herein are intended to aid in understanding the principles of the invention, and are to be construed as being without limitation to such specifically recited examples and conditions. As a result, the invention is not limited to the specific embodiments or examples described below, but by the claims and their equivalents.

[0018] Referring to FIG. 1, a network element NE included in a telecommunication network TN is associated with a lock protection system LPS including an electromagnet EM and an interface INT. The lock protection system LPS is a mechanical system whose function is to protect or inhibit physical access to the network element NE. The lock protection system LPS is coupled to a lock mechanism allowing physical access to the network element NE, more specifically to a room where at least a communicating device of the network element is located.

[0019] The lock protection system LPS is connected to a command device CD, that can be a server or any communicating device, able to command the lock protection system LPS.

[0020] The electromagnet EM is linked to the lock mechanism of the network element and cooperates with a metallic object in order to inhibit or not the lock mechanism. In all cases, the metallic object prevents the lock mechanism to work, for example by impeding access to the lock mechanism by human.

[0021] The lock mechanism can feature various ways to access it as non limited examples: key hole, mechan-

ical combination lock, or electronic keypads, that all need to be hidden or inhibited so that a malicious intruder will not be able to use them.

[0022] The interface INT checks signal information about whether the network element NE is connected or not to the telecommunication network TN.

[0023] In one embodiment, the signal information comes from the network element itself. In this case, the network element comprises also an interface to communicate with the lock protection system LPS.

[0024] In another embodiment, the signal information comes from the command device CD which retrieves information if the network element NE is connected or not to the telecommunication network TN from an entity of the telecommunication network.

[0025] By default, the lock protection system LPS is not active, in order to cover cases where the network element is powered-off or has a broken connection with the telecommunication network. Thus, as the electromagnet EM is powered by the same power source as the network element NE, the lock protection system LPS is automatically deactivated in case of a power-off situation.

[0026] The lock protection system LPS is activated if two conditions are satisfied: a connection with the operator of the telecommunication network and a feature activated by software. Once the electromagnet is power on, the lock is inhibited.

[0027] The electromagnet EM is controlled by the lock protection system LPS that follows the process according to FIG. 1 comprising steps S1 to S4.

[0028] At step S1, the electromagnet EM is not powered, meaning that lock protection system LPS is not activated.

[0029] At step S2, the interface INT of the lock protection system LPS checks information about whether the network element NE is connected or not to the telecommunication network.

[0030] If the network element NE is connected to the telecommunication network, the process continues with step S3, otherwise the process goes back to step S1.

[0031] The information checked by the interface INT at step S2 can come from the network element itself or from the command device CD connected to the lock protection system LPS.

[0032] At step S3, the interface INT of the lock protection system LPS checks information about a value of a software parameter SP indicating if the lock mechanism should be inhibited or not. For example, the software parameter SP is the following parameter DOOR_LOCK_INHIBIT being a Boolean parameter, having a state with value of "1" meaning the lock mechanism should be inhibited and another state with value of "0" meaning the lock mechanism should not be inhibited.

[0033] If the value of the software parameter SP is "1", the process continues with step S4, otherwise if the value of the software parameter SP is "0", the process goes back to step S1.

[0034] The information checked by the interface INT

at step S3 comes from the command device CD that is connected to the lock protection system LPS and attributes the value of the software parameter.

[0035] At step S4, the electromagnet EM is powered on to cooperate with a metallic object, meaning that lock protection system LPS is activated to inhibit the lock mechanism and protect physical access to the network element NE. By physical access to the network element NE, it is meant for example access to a room inside the network element where hardware or electronic devices are located, like a server.

[0036] At this step, the lock protection system LPS is thus activated as the both conditions are satisfied: the network element NE is connected to the telecommunication network and software parameter SP at state with value of "1".

[0037] In reference to FIG. 3a and 3b, a metallic plate can be lifted thanks to a knob only if the electromagnet EM does not lock this metallic plate, i.e. the electromagnet is not powered.

[0038] In FIG. 3a, the electromagnet EM is powered on and the metallic plate protects the keyhole that is not accessible, the metallic plate being attracted by the electromagnet.

[0039] In FIG. 3b, the electromagnet EM is powered off and the metallic plate lets the keyhole accessible, the metallic plate being free to move.

[0040] In reference to FIG. 4a and 4b, the electromagnet EM does not aim to protect the lock cylinder, but to inhibit the multi-lock mechanism. Once inhibited, the lock cylinder can be turned but it does not act on the multi-lock mechanism. Opening the door can only be done if the electromagnet EM is powered off. Then, the multi-lock mechanism is released and engaged with the lock cylinder.

[0041] In FIG. 4a, the electromagnet EM is powered on, the spring around it being compressed, and metal moving part of the multi-lock mechanism is attracted by the electromagnet and moved away from the lock cylinder.

[0042] In FIG. 4b, the electromagnet EM is powered off and the spring around it is released, pushing the metal moving part of the multi-lock mechanism back toward the lock cylinder.

[0043] The lock protection system LPS may also be used directly on a door lock mechanism itself, for example in the case when the room containing the network element to be protected is already inside a secure building. In this case there is no need to have a specific key or combination to know to enter the room: an operator agent can enter the room when the network element is powered off, when it is not connected to the operator network. Otherwise the agent has to modify the value of the DOOR_LOCK_INHIBIT software parameter to "0" and the door will unlock.

[0044] Advantageously, the lock protection system LPS solution is lighter and cheaper than a security door:

- lighter: some embodiments described above weigh less than a kilogram when a security door adds many kilograms; the weight aspect is important when considering the network deployment (handling) and hosting infrastructure (foundation slab or other);
- cheaper: due to the increasing cost of metal, a security door represent a highly cost compared to the limited list of elements required by the lock protection system LPS.

[0045] In some of its embodiments, the lock protection system LPS is also very simple to add to an already installed equipment (possibly without a service interruption).

[0046] The invention described here relates to a method and a system for a physical access protection of a network element in a telecommunication network. In an embodiment, the steps of the method of the invention are determined by the instructions of a computer program incorporated in a system such as the lock protection system LPS. The program includes program instructions which, when said program is executed in a processor of the system the operation whereof is then controlled by the execution of the program, execute the steps of the method according to the invention.

[0047] As a consequence, the invention applies also to a computer program, in particular a computer program on or in an information medium readable by a data processing device, adapted to implement the invention. That program may use any programming language and be in the form of source code, object code or an intermediate code between source code and object code, such as a partially compiled form, or in any other desirable form for implementing the method according to the invention.

[0048] The information medium may be any entity or device capable of storing the program. For example, the medium may include storage means or a recording medium on which the computer program according to the invention is recorded, such as a ROM, for example a CD ROM or a microelectronic circuit ROM, or a USB key, or magnetic recording means, for example a diskette (floppy disk) or a hard disk.

Claims

1. A system (LPS) for protecting physical access through a lock mechanism to a network element (NE) in a telecommunication network (TN), the system (LPS) being coupled to the lock mechanism and comprising:

means (INT) for checking information about whether the network element (NE) is connected or not to the telecommunication network (TN),
means (INT) for checking information about a value of a software parameter (SP) indicating if

the lock mechanism should be inhibited or not, means (EM) for inhibiting the lock mechanism if the network element (NE) is connected to the telecommunication network (TN) and if the value of the software parameter (SP) indicates that the lock mechanism should be inhibited. 5

2. A system according to claim 1, wherein means (EM) for inhibiting the lock mechanism is an electromagnet that is linked to the lock mechanism and cooperates with a metallic object preventing the lock mechanism to work. 10
3. A system according to claim 2, wherein the electromagnet is powered on by the system (LPS) to cooperate with the metallic object. 15
4. A system according to any of claims 1 to 3, wherein the system (LPS) is connected to a device (CD) able to command the system (LPS) and to attribute the value of the software parameter (SP). 20
5. A system according to any of claims 1 to 4, wherein the network element is a base station. 25
6. A system according to any of claims 1 to 4, wherein the network element is a data center.
7. A system according to any of claims 1 to 6, wherein physical access to the network element (NE) is access to a room inside the network element where hardware or electronic devices are located. 30
8. A method for protecting physical access through a lock mechanism to a network element (NE) in a telecommunication network (TN), comprising the following steps executed in a system (LPS) coupled to the lock mechanism: 35

checking (S2) information about whether the network element (NE) is connected or not to the telecommunication network (TN), 40
 checking (S3) information about a value of a software parameter (SP) indicating if the lock mechanism should be inhibited or not, 45
 inhibiting (S4) the lock mechanism if the network element (NE) is connected to the telecommunication network (TN) and if the value of the software parameter (SP) indicates that the lock mechanism should be inhibited. 50

9. A computer program adapted to be executed in a system (LPS) for protecting physical access through a lock mechanism to a network element (NE) in a telecommunication network (TN), the system (LPS) being coupled to the lock mechanism, said program including instructions which, when said program is executed in said system, execute the following steps: 55

checking (S2) information about whether the network element (NE) is connected or not to the telecommunication network (TN),
 checking (S3) information about a value of a software parameter (SP) indicating if the lock mechanism should be inhibited or not,
 inhibiting (S4) the lock mechanism if the network element (NE) is connected to the telecommunication network (TN) and if the value of the software parameter (SP) indicates that the lock mechanism should be inhibited.

FIG. 1

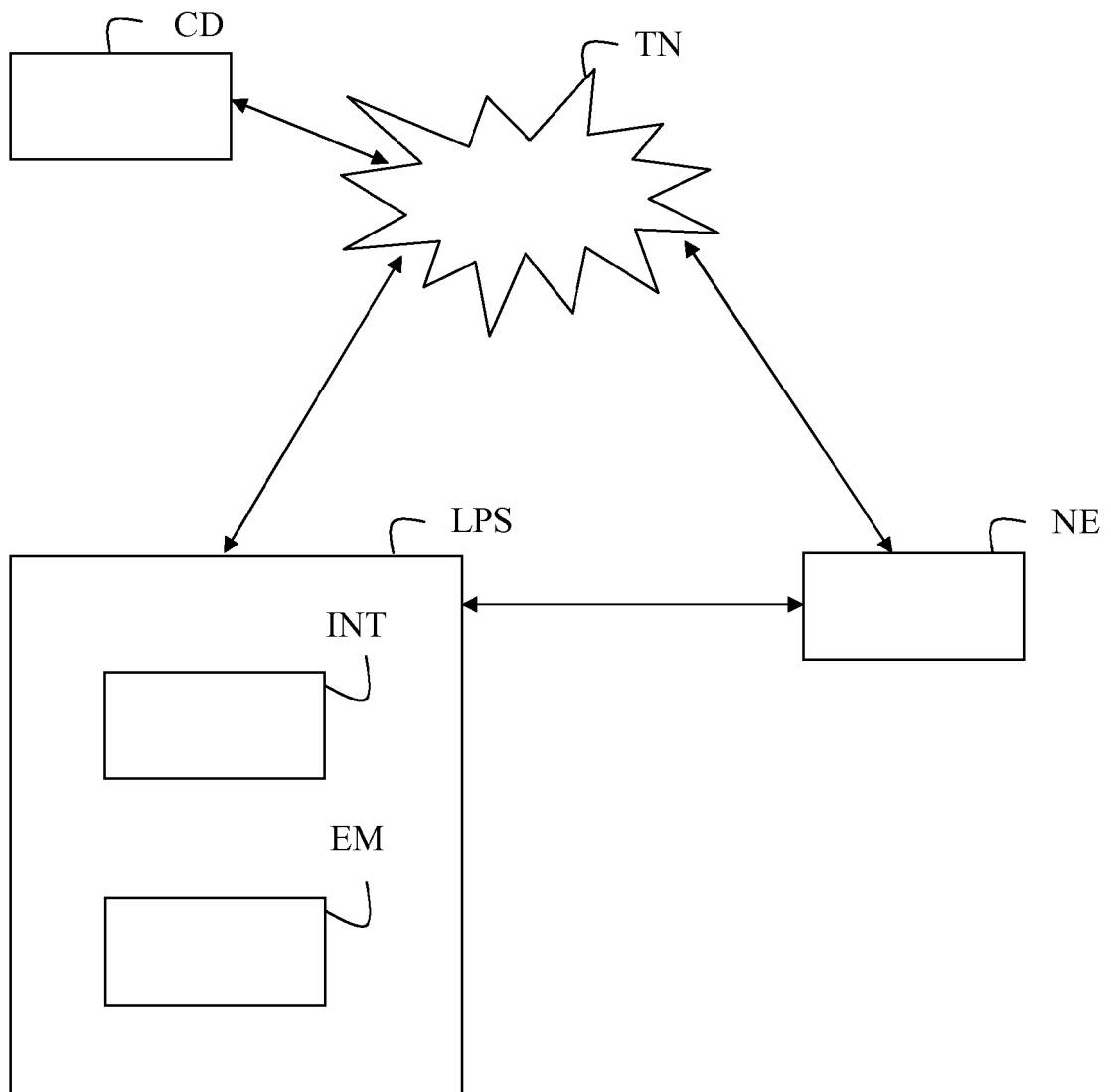


FIG. 2

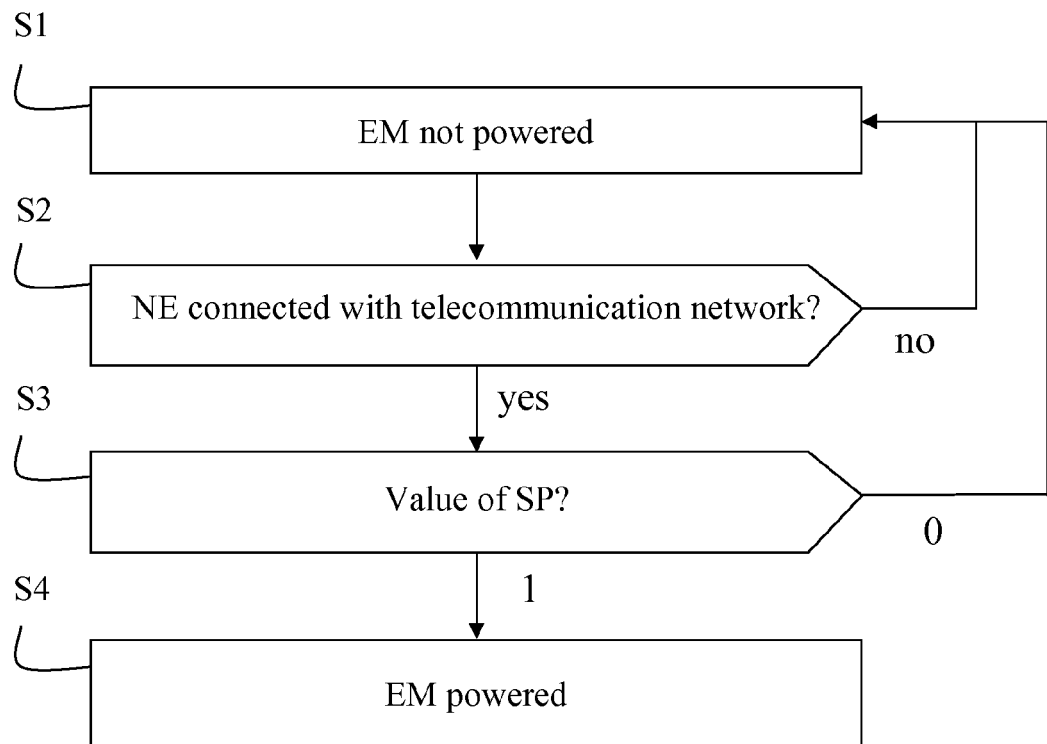


FIG. 3a

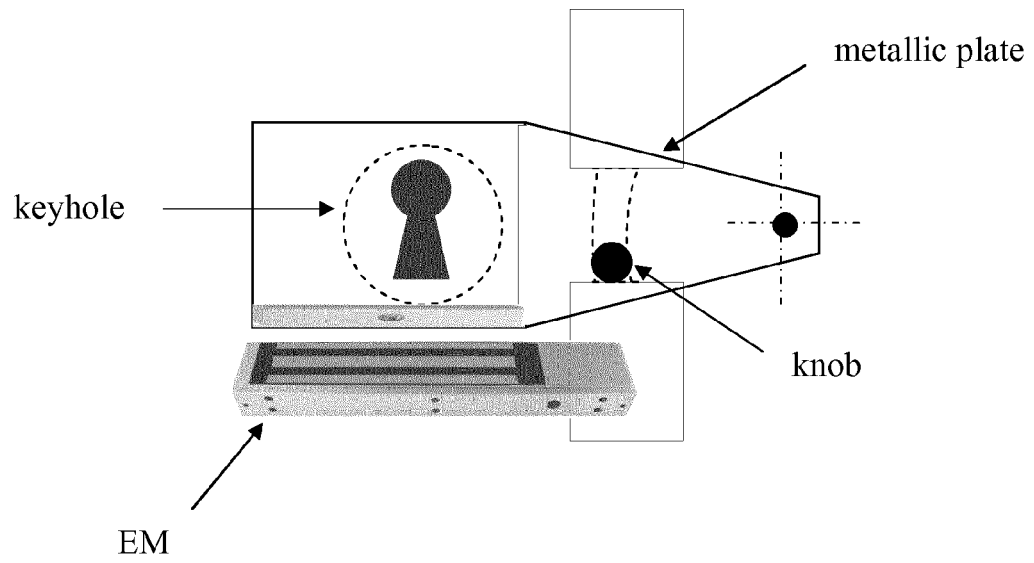


FIG. 3b

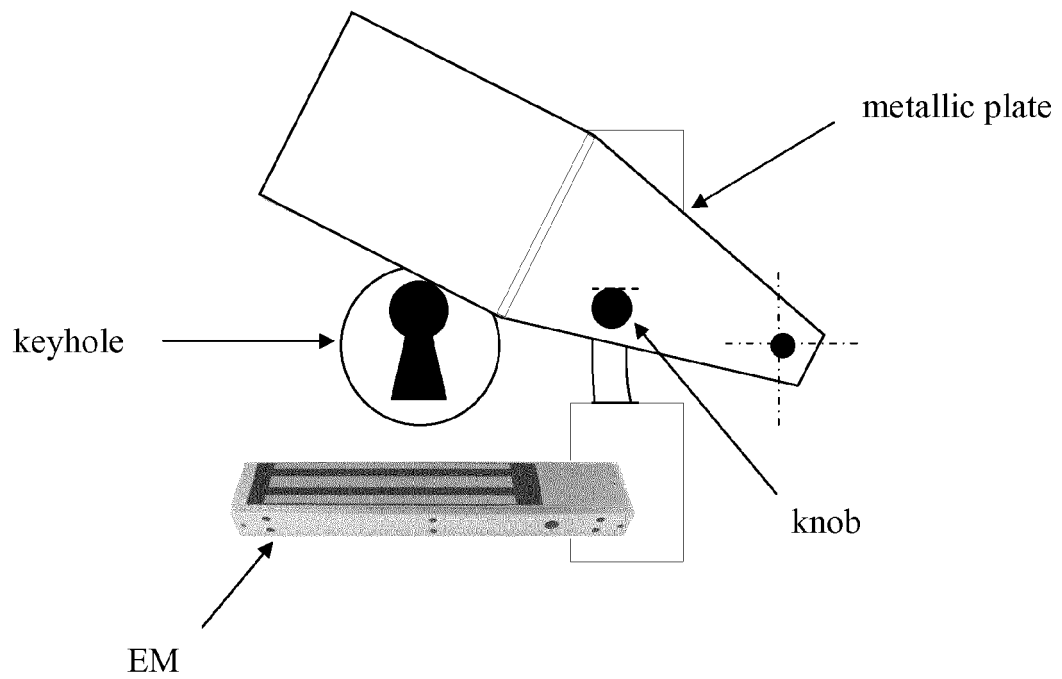


FIG. 4a

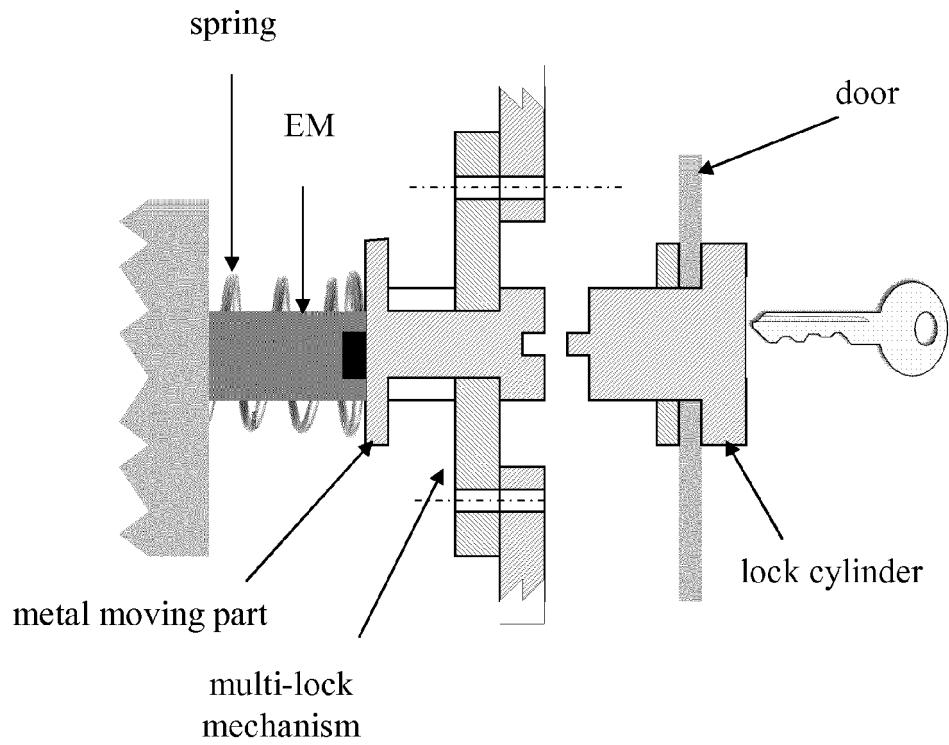
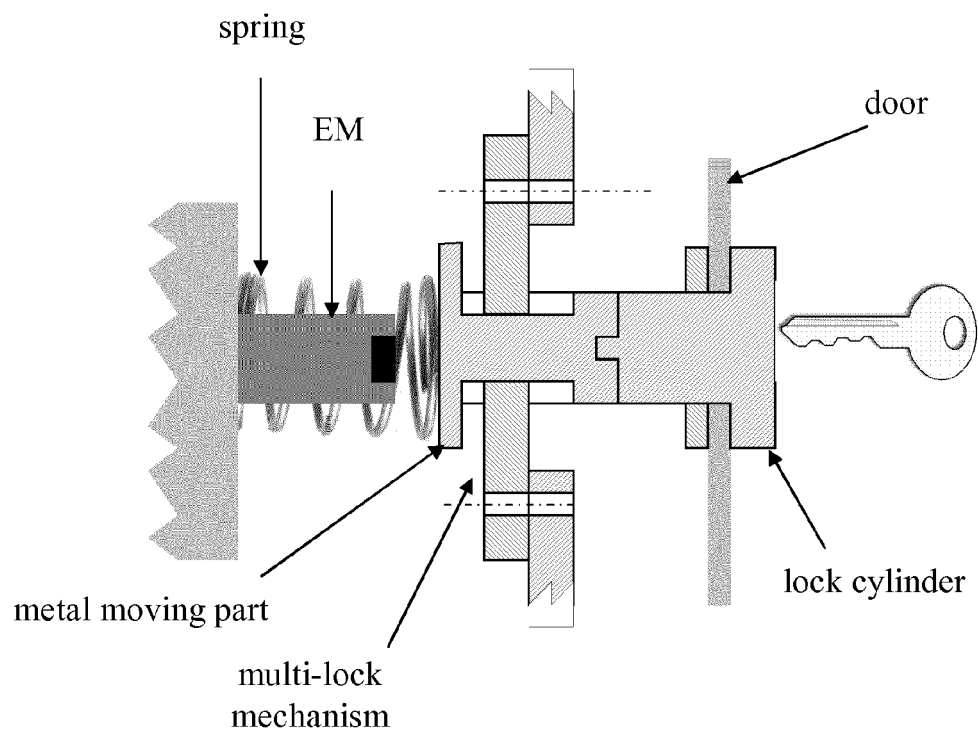


FIG. 4b





EUROPEAN SEARCH REPORT

Application Number
EP 12 30 5666

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	US 2004/189439 A1 (CANSINO JUAN MIGUEL DOMINGUEZ [ES]) 30 September 2004 (2004-09-30)	1,4-9	INV. G07C9/00 E05B17/00
Y	* abstract * * * figures 1a-8bb * * paragraph [0022] - paragraph [0055] * * paragraph [0078] * * paragraph [0102] - paragraph [0107] * * paragraph [0162] - paragraph [0194] * * paragraph [0219] - paragraph [0242] * * claims 1-12 *	2,3	
Y	----- US 2010/236303 A1 (RAMSAUER DIETER [DE] ET AL) 23 September 2010 (2010-09-23)	2,3	
A	* abstract * * * paragraph [0008] - paragraph [0023] * * paragraph [0042] * * paragraph [0054] * * figures 1-13c *	4	
X	----- US 5 602 536 A (HENDERSON WALTER G [US] ET AL) 11 February 1997 (1997-02-11)	1,4-9	TECHNICAL FIELDS SEARCHED (IPC)
	* abstract * * * column 19, line 16 - column 22, line 42 *		G07C E05B
X	----- WO 97/22772 A1 (ELECTRONIC LOCKING SYSTEMS LIM [NZ]; POGSON STANLEY ERNEST [NZ]; THOMA) 26 June 1997 (1997-06-26)	1,4-9	
	* abstract * * * page 8, paragraph 2 - page 13, paragraph 3 * * figures 1-4 *		

The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 14 November 2012	Examiner Pañeda Fernández, J
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	

2
EPO FORM 1503 03.02 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 12 30 5666

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.

14-11-2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004189439 A1	30-09-2004	BR PI0408855 A	04-04-2006
		CA 2520777 A1	04-11-2004
		CN 1871830 A	29-11-2006
		EP 1614272 A1	11-01-2006
		NZ 543290 A	27-07-2007
		RU 2356175 C2	20-05-2009
		US 2004189439 A1	30-09-2004
		WO 2004095804 A1	04-11-2004
		ZA 200507837 A	26-09-2007
US 2010236303 A1	23-09-2010	DE 112008002318 A5	11-11-2010
		DE 202007013103 U1	19-02-2009
		EP 2188471 A1	26-05-2010
		US 2010236303 A1	23-09-2010
		WO 2009039933 A1	02-04-2009
US 5602536 A	11-02-1997	US 5602536 A	11-02-1997
		US 6822553 B1	23-11-2004
		US 6842105 B1	11-01-2005
		US 2005168320 A1	04-08-2005
WO 9722772 A1	26-06-1997	AU 709083 B2	19-08-1999
		AU 1214297 A	14-07-1997
		EP 0874945 A1	04-11-1998
		WO 9722772 A1	26-06-1997

EPO FORM P0459

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