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

(11) EP 2 933 782 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.10.2015 Bulletin 2015/43

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Application number: **14165305.5**

(22) Date of filing: **18.04.2014**

(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

(71) Applicant: **Altel**
Laval, Québec H7L 4S8 (CA)

(72) Inventor: **Paquin, Yves**
Rosemère, Québec J7B 1R5 (CA)

(74) Representative: **Debay, Yves**
Cabinet Debay
126, Elysee 2
78170 La Celle Saint Cloud (FR)

(54) Electronic door access control system

(57) An electronic door lock system comprising a door control unit, a key reader and an encrypted binding between the key reader and the door control unit. When tampering is detected the encrypted binding is terminated thereby preventing the door from being opened. There is also disclosed a method for retrofitting a door comprising a key reader with a door control unit. The door control unit, key reader and the latch release mechanism may also be powered by a key comprising a power supply, the key also supplying a coded sequence to the door control unit.

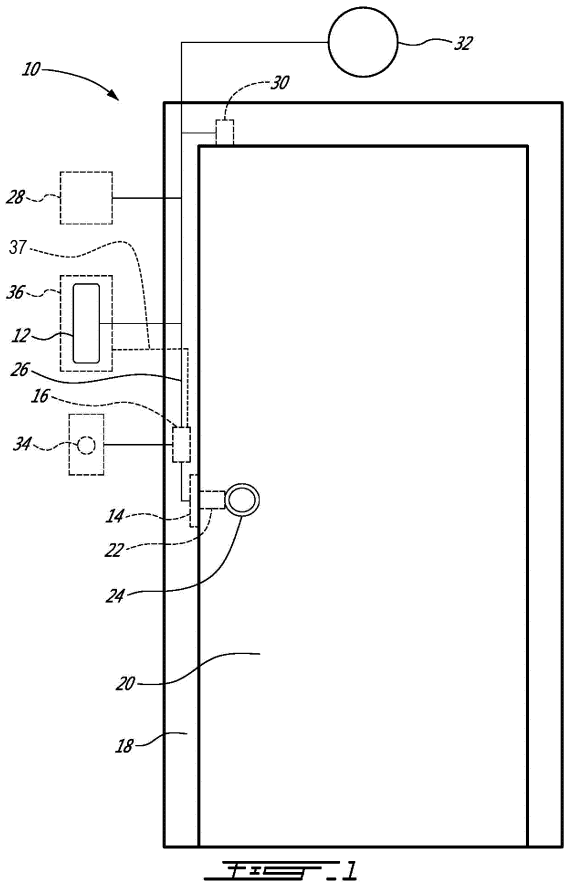

Fig. 1

EP 2 933 782 A1

Description

FIELD OF THE INVENTION

[0001] The present invention relates to an electronic door access control system. In particular, the present invention relates to a system comprising a door control unit (DCU) for restricting access via a selectively lockable door way.

BACKGROUND TO THE INVENTION

[0002] One drawback with prior art electronic door access systems is that many of the elements necessary to open the door are collocated with either the key reader, the door lock or the striker plate. This means that the prior art door locks are relatively easy to compromise. Another drawback, often linked to the first one, is the general lack of tracking of access by users. Another drawback shown in the art is that in order to operate, the door must be supplied with a source of power, which is typically by means of a collocated battery or power supply attached to the mains.

SUMMARY OF THE INVENTION

[0003] A purpose of the present invention is to overcome at least part of the above and/or other drawbacks by providing a safe electronic door access control apparatus.

[0004] Such aim is achieved by an electronic door access control apparatus for restricting access via a door installed in a door frame and comprising a lock mechanism having a latch bolt and using a key comprising a unique coded ID sequence. The apparatus comprises a key reader for reading the key and comprising a tamper switch, a latch release mechanism, a door control unit separate from the key reader and the latch release mechanism, installed in the door frame proximate to the key reader and the latch release mechanism and comprising a controller and memory comprising a plurality of predetermined allowed coded ID sequences, wherein the door control unit is in communication with the tamper switch, and the apparatus further comprises an encrypted binding between the key reader and the door control unit. The apparatus is thereby configured such that : When the key is positioned proximate to the key reader, the coded ID sequence is read by the key card reader and relayed to the door control unit via an encrypted communication channel for processing, wherein when the coded ID sequence matches one of the plurality of predetermined allowed coded ID sequences, the door control unit actuates the latch release mechanism, thereby allowing the door to be opened, and further wherein when the DCU detects tampering of the key reader via the tamper switch, the encrypted binding between the key reader and the door control unit is terminated.

[0005] According to other features, said key reader comprises a screen and an input interface for manually entering a password and further wherein said password is relayed to said door control unit via said encrypted communication channel for processing with the unique coded ID, and wherein said input interface preferably comprises at least one of a key pad and a proximity sensor using an electric field for sensing and recognizing the motion of a user's hand or finger.

[0006] According to other features, the lock mechanism comprises a latch bolt and wherein said latch release mechanism is configured for receiving said latch bolt and comprises a striker plate and a solenoid and further wherein said door control unit actuates said latch release mechanism by activating the solenoid, thereby releasing said striker plate.

[0007] According to other features, said door control unit can only be reestablished by reprogramming said door control unit once said encrypted binding between said key reader and said door control unit is terminated.

[0008] According to other features, said key reader is interconnected with said door control unit via a wired connection.

[0009] Another purpose of the present invention is to overcome at least part of the drawbacks of the prior art by providing a safe electronic door access control method.

[0010] Such aim is achieved by a method for retrofitting an existing electronic door access control system for restricting access via a door and comprising a lock mechanism having a key reader for reading a key comprising a unique coded ID sequence, a latch release mechanism and a power supply. The method comprises associating a tamper detector having an output with the key reader, interconnecting the key reader and the latch release mechanism using a relay, wherein the relay is normally closed, and controlling opening and closing the relay with a resettable door control unit powered by the power supply, wherein the tamper detector output is input into the door control unit. When tampering is detected via the input, the door control unit opens the normally closed relay and thereby preventing the key reader from actuating the latch release mechanism.

[0011] According to other features, once open, said relay can only be closed by reprogramming said door control unit and wherein said door control unit preferably comprises a USB interface and further comprising reprogramming said door control unit via said USB interface using an external reprogramming device.

[0012] Another purpose of the present invention is to overcome at least part of the drawbacks of the prior art by providing a safe electronic door access control system.

[0013] Such aim is achieved by an electronic door access control system for restricting access via a door comprising a lock mechanism having a latch bolt. The system comprises a key comprising a unique coded ID sequence and a key memory, a key reader for reading the key, a latch release mechanism, and a door control unit com-

prising a controller, a real time clock, a door control unit memory and a door identifier. This system is configured such that : When the key is positioned proximate to the key reader, the coded ID sequence is read by the key card reader and relayed to the door control unit and further wherein when the coded ID sequence matches one of the plurality of predetermined allowed coded ID sequences, the door control unit actuates the latch release mechanism, thereby allowing the door to be opened, and further wherein a time stamp and the door identifier is relayed to the key for storage in the key memory.

[0014] According to other features, said key comprises a power source and further wherein when the key is positioned proximate to said key reader, said power source provides power for operating said key reader, said latch release mechanism and said door control unit.

[0015] According to other features, the lock mechanism comprises a latch bolt and said latch release mechanism is configured for receiving the latch bolt and comprises a striker plate and a solenoid, and further wherein said door control unit actuates said latch release mechanism by activating the solenoid, thereby releasing said striker plate.

[0016] Such aim is also achieved by an electronic door access control system for restricting access via a door installed in a door frame and comprising a lock mechanism having a latch bolt. The system comprises a key comprising a unique coded ID sequence and a power source having a key voltage, a key reader for reading the key, a latch release mechanism configured for receiving the latch bolt and comprising a striker plate and a solenoid only actuatable using an actuating voltage greater than the key voltage, and a door control unit comprising a controller, a door control unit memory and a charge pump, an output of the charge pump connected across an input of the solenoid. Said system is configured such that, when the key is positioned proximate to the key reader, the key power source supplies power for operating the key reader and the door control unit and further wherein once powered the coded ID sequence is received by the key card reader and relayed to the door control unit and further wherein when the coded ID sequence matches one of the plurality of predetermined allowed coded ID sequences, the door control unit activates the charge pump using the key voltage, the charge pump raising the key voltage to the actuating voltage thereby actuating the solenoid and allowing the door to be opened.

[0017] According to other features, said power source is a battery, wherein said key and said key reader each comprise a pair of contacts, wherein positioning said key proximate to said key reader comprises interconnecting said respective pairs of contacts such that said battery supplies power for operating said key reader and said door control unit via said pairs of contacts and wherein said key preferably comprises a normally open microswitch between said power source and at least one of said pair of contacts such that when said microswitch is closed by contact with said key reader an electrical circuit is completed between said power supply and said contacts.

[0018] According to other features, said key is held removeably against said key reader by a magnet.

[0019] According to other features, once said solenoid is actuated, a voltage across said output of said charge pump is lowered to a holding voltage lower than said actuating voltage.

[0020] According to other features, said key voltage is less than 5 volts and said actuating voltage is greater than 12 volts.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021]

- Figure 1 provides a schematic view of an electronic door access control system in accordance with an illustrative embodiment of the present invention;
- Figure 2A provides a detailed perspective view of a section of a door frame and striker plate;
- Figure 2B provides a sectional view along IIB-IIB of the door frame of Figure 2A;
- Figure 3 provides a block diagram of a Door Control Unit (DCU) in accordance with an illustrative embodiment of the present invention;
- Figure 4A provides a block diagram of a key reader in accordance with an illustrative embodiment of the present invention;
- Figure 4B provides a front perspective view of the key reader in Figure 4A;
- Figure 4C provides a schematic view of an electronic door access control system in accordance with an alternative illustrative embodiment of the present invention;
- Figure 5A provides a block diagram of a key reader and key in accordance with an alternative illustrative embodiment of the present invention;
- Figure 5B provides a block diagram of a key in accordance with an alternative illustrative embodiment of the present invention;
- Figure 5C provides a front perspective view of the key reader and key in Figure 5A;
- Figures 6A and 6B provide an orthonormal view of a door latch and a side plan view of a solenoid in accordance with a an illustrative embodiment of the present invention;
- Figure 7 provides a block diagram of an electronic door access control system installed within an elevator and in accordance with an alternative illustrative embodiment of the present invention; and
- Figures 8A to 8E provide a series of views of the key shown in Figure 5A.

DETAILED DESCRIPTION OF THE ILLUSTRATIVE EMBODIMENTS

[0022] In some embodiments, an illustrative and non-limiting example of which is shown on Figure 1, an elec-

tronic door access control system, generally referred to using the reference numeral 10, will now be described. The door access control system 10 comprises a key reader 12 and latch release mechanism 14 interconnected by a Door Control Unit (DCU) 16, for example using conductive wires or the like. The system is illustratively for use on a standard doorway comprising a metal door frame 18, door 20 and bored cylindrical lock 22 comprising a handle 24, or mortise lock, or the like. The DCU 16 is separate from the key reader 12 and, as will be discussed in more detail below, installed embedded in the door frame 18. The DCU 16 is interconnected with the key reader 12 illustratively via a communication cable 26 and an encrypted communications protocol. In a first illustrative embodiment the system 10 comprises an external power source 28, such as a power supply connected to the mains (not shown). Alternatively, the key reader 12 or DCU 16 could comprise an Ethernet interface (for example for connection to an external computer network or the like, not shown) and the power necessary for system operation provided via an appropriate network switch and a Power over Ethernet (PoE) connection.

[0023] In some particular embodiments, an illustrative and non-limiting example of which is still shown on Figure 1, other peripheral devices could be included, for example a contact switch 30 for providing input to the DCU 16 that the door 20 is open or closed, an external alarm 32 for indicating that the door is ajar or has been forced, and a Request to Exit (REX) release 34 for generating a REX signal for disengaging the latch release mechanism 14 (from inside the restricted access area, for example) such that the restricted access area can be easily exited. Additionally, and as will be discussed in more detail below, a tamper switch/detector 36 can be provided that senses if the key reader has been tampered with, for example by attempted removal of the keypad 12 or the like, and communicates this event to an input of the DCU 16, for example via a dedicated pair of conductive wires 37 or the like. Note that, although the key reader 12 is shown as being installed on the wall adjacent the door frame 18, in a particular embodiment the key reader 12 and tamper switch/detector 36 are mounted to the door frame 18 immediately above the latch release mechanism 14 but might be installed according to the needs.

[0024] In some embodiments, illustrative and non-limiting examples of which are shown on Figures 2A and 2B, the frame 18 is typically manufactured from a hard rigid material such as sheet steel or the like and illustratively shaped to include a door rabbet 38, door stop 40 and opposed flanges as in 42. The flanges 42 provide for installation onto a conventional wall 44, for example constructed of brick or wood or metal studs 46 covered in a paneling material 48, such as plaster or sheets of gyp rock or the like. Once the frame 18 is installed on the wall 44, a gap or space is typically left between the frame 18 and the studs 46. In some particular embodiments, for example to improve security, a reinforcing plate 50 is provided extending several inches along the frame 18 at the height of the striker plate 52 and providing an enclosed region 54 about the striker plate 52. Also, in some similar particular embodiments, the region 54 can be completely enclosed by welding or otherwise joining an appropriate plate/cap (not shown) to the top and bottom of the enclosed region 54 above and below the striker plate 52.

[0025] In some embodiments, illustrative and non-limiting examples of which are still shown Figures 2A and 2B, the striker plate 52 is installed at lock level, typically between 38" and 42" above floor level, by means of screws as in 55 or the like. In this regard, many prefabricated metal door frames as in 18 include a small precut slot 56 in the door rabbet 38 over which the striker plate 52 is installed. A typical such slot 56 is cut to an ANSI standard for receiving a standardized dust box therein.

[0026] In some embodiments, illustrative and non-limiting examples of which are still shown on Figures 2A and 2B, in order to retrofit the electronic door access control system 10 of the present invention to a previously installed door frame 18, the DCU 16 is designed to fit through the precut slot 56. For example small hole (not shown) is cut in the outer flange 42 of the door frame 18 above the precut slot 56 and at the level the key reader 12 and tamper switch 36, if required, is to be installed at. The communication cable 26 is fed via the hole to the precut slot 56, connected to the DCU 16 which is then inserted into the enclosed region 54 or gap. The latch release mechanism 14 can then be installed, covering the enclosed region 54 or gap and the DCU 16. Power for energizing the system, including the DCU 16 can be provided by an external power supply, for example by pulling an appropriate power cable from the power supply (reference 28 on Figure 1), or battery or the like in various embodiments.

[0027] In some embodiments, illustrative and non-limiting examples of which are shown on Figures 1 and 3, the DCU 16 comprises a microprocessor/controller 58 which, using programs and predetermined allowed coded ID sequences stored in non-volatile memory 60, generates signals for enabling the latch release mechanism 14, for example via the strike plate output 62.

[0028] In some embodiments, when the system is battery operated, the latch release mechanism 14 typically requires voltage and current at levels greater than that provided by the power source 64 (in this case, the battery) and used by the DCU 16 for correct operation of its electronic circuits, and therefore a charge pump 66 is provided. As known in the art, the charge pump, such as a mono-stable multi-vibrator or the like, can raise DC voltages above those of a supplied voltage in order to address differing operating requirements.

[0029] In some embodiments, the microprocessor 58 receives external inputs 68 from the various input devices, such as the door contact sensor 30 and the latch mechanism disengaging push button 34, the tamper switch 36 as well as communications from the key reader 12 via the I/O interface 70, and enables the appropriate

strike plate output 62 and/or activates an appropriate auxiliary output 72, such as an alarm 32. A LED 74 or other means is also provided to indicate mode of operation of the DCU 16. A Real Time Clock (RTC) 76 can also be provided in order to provide time stamps or the like.

[0030] In some particular embodiments, an illustrative and non-limiting example of which is still shown on Figure 3, as the DCU 16 has a limited number of outputs, the DCU 16 can communicate with other similar DCUs as in 16 via the I/O interface 70. In this regard, the physical connections (for example conductive wires or the like) between the key reader(s) as in 12 and the DCUs as in 16 provide a bus for the communications protocol(s) used by the key reader(s) as in 12 and the DCU(s) as in 16 to communicate. As will be discussed in more detail below, this provides additional versatility thereby allowing the DCU 16 to be used in a variety of different settings. Also, for monitoring purposes or the like, a wireless (not shown) interface could be provided.

[0031] In some embodiments, an illustrative and non-limiting example of which is shown on Figure 4A in addition to Figure 1, the key reader 12 comprises a microprocessor/controller 78, a coded key receiver 80, for example with an associated antenna 82, and a DCU I/O interface 94 for communicating with the DCU(s) 16. A user interface, such as a small OLED screen 84 and/or a three button keypad 86, for example using infrared sensors or the like and/or a buzzer 90 and/or status LED 92 can be provided, possibly with a USB interface 88. A memory 96 is also preferably provided which can include Flash Memory 98, EEPROMs 100, SRAM 102, SD Memory Cards 104 and the like. Additionally, in some embodiments, a Real Time Clock (RTC) and supercap circuit 106 are provided for generating appropriate time stamps and memory backup during power down or the like. Although the key reader 12 may be powered via the DCU I/O interface 94, in some particular embodiments a power regulator 108 is also provided to condition the voltage of power being supplied, for example, via a Power over Ethernet connection 110 or battery or the like, such that it is at appropriate levels for correct operation of the key reader 12. Of note is that in these particular embodiments, power received via the Power over Ethernet connection 110 and conditioned by the power regulator 108 may also be provided to the DCU 16 via the DCU I/O interface 94. In some particular embodiments the USB interface 88 may also be used to power the key reader 12 and DCU 16 with provision of an appropriate USB power supply (not shown).

[0032] In some embodiments, an illustrative and non-limiting example of which is still shown on Figure 4A in addition to Figure 1, using programs stored in the Flash memory 98, EEPROM 100 and/or SRAM 102, for example, the microprocessor 78 receives IDs of coded key cards (not shown) held in proximity to the Key Reader interface 80 and communicates the appropriate information to the DCU 16, for example using an encrypted protocol or the like. In this regard, use of an encrypted communication between the key reader 12 and the DCU 16 is useful in that it further reduces the likelihood that the door opening mechanism can be compromised, for example by installing a protocol reader between the key reader 12 and the DCU 16. The user interface, such as OLED screen 84 can be used to provide appropriate feed back to the user, for example to prompt the user to enter a pin number via the keypad 86. The status LED 92 provides system status as well as useful feedback, for example during servicing of the key reader 12 or the like. The user interface such as the buzzer 90 may provides audio cues to the user that the door 20 can be opened, or that the user's coded key card (not shown) has been refused.

[0033] In some embodiments, an illustrative and non-limiting example of which is still shown on Figure 4A in addition to Figure 1, as will be discussed in more detail below, access to the memory can be provided, for example by a SD Memory card interface 104 (or alternatively the USB interface 88 with provision of a USB flash drive or the like, not shown), which can be used to retrieve data stored by the DCU 16 for administrative purposes, for example as to coded IDs which have attempted to gain access or gained access to the restricted area via the door 20, as well as time stamps and the like. Additionally, such memory access like the SD Memory card interface 104 (or alternatively the USB interface 88 with provision of a USB flash drive or the like) can be used to provide a convenient mechanism to provide software updates for the key reader 12 and the DCU 16. In this regard, software updates may include not only operating software for ensuring correct functioning of the electronic door access control system 10, but also access control information, such as allowed coded IDs, hours and dates when users associated with the coded IDs are entitled to enter the restricted area via the door 20 and the like.

[0034] In some embodiments, an illustrative and non-limiting example of which is shown on Figure 4B in addition to Figure 1, the key reader 12 comprises a housing 112 which is secured in proximity to the door 20, for example on the door frame 18 or the wall adjacent the door frame 18. As discussed above a communications cable 26 (not shown) is provided, for example fed through a hole bored in the frame 18 or the like, to interconnect the key reader 12 with the DCU 16 via their respective I/O interfaces 70, 94. In order to improve the security of the installed system, preferably at this point of the installation process the key reader 12 and DCU 16 are typically prompted, for example using an external programming device or master key card (both not shown), to exchange an encrypted or coded sequence in order to bind them to one another. Binding in such a manner ensures that a given key reader 12 and DCU 16 communicate using an encrypted protocol which is only known to them, and such that they can only communicate with one another. This ensures that a given key reader 12 and/or DCU 16 cannot be used elsewhere, for example in an attempt to tamper with another system or the like.

[0035] In some particular embodiments, once the key reader 12 and DCU 16 have been bound to one another, in the event an indication is received via the tamper switch 36 that the keypad 12 (or other parts of the system) is being tampered with, the DCU 16 wipes or otherwise disables the bindings, effectively blocking the system from being used to operate the latch release mechanism 14. In order to use the electronic door access control system subsequently, the binding between the key reader 12 and DCU 16 would have to be reestablished, for example using an external programming device or master key card.

[0036] In some embodiments, an illustrative and non-limiting example of which is still shown on Figure 4B in addition to Figure 1, as discussed above, in a first embodiment, the key reader 12 comprises an antenna 82 and a user interface such as an OLED screen 84 and/or a key pad 86 comprising three keys as in 114. In this regard, the keys as in 114 are programmable and allow the user to migrate menus displayed on the screen 84, that is the programming of the keys 114 is able to change dependent on the screen, context and/or particular menu entry selected. Illustratively, the keys could be programmed to comprise an "up" key and a "down" key for scrolling through a series of numeric or alphanumeric characters, and a select key for selecting one of the characters when arrived at during scrolling. In this way the user can construct a Personal Identification Number (PIN) or Alphanumeric password or the like to further limit the possibility that access to the restricted area is compromised, for example by inappropriate use of another user's coded ID card or the like. A status LED 87 may also be provided.

[0037] In some particular embodiments of the user interface, the three button keypad 86 can be replaced or combined with a proximity sensor 113 which uses an electric field for sensing and recognizing the motion of a user's hand or finger. A particular embodiment of such a sensor is manufactured under the GestIC™ brand. The proximity sensor tracks the user's hand or finger motion in free-space and in a 3D coordinate system (x-y-z). For example moving a finger above the proximity sensor in a circular motion can be used to scroll through screen selections, which can be selected by tapping the screen. As per the keypad 86 this allows the user to enter additional security information such as pin numbers or passwords and the like.

[0038] In some embodiments, an illustrative and non-limiting example of which is still shown on Figure 4C, the electronic door access control system 10 has the advantage that it can be used to protect existing systems without affecting their method of control or requiring integration into their respective control systems or the like.

[0039] In some of these embodiments of the electronic door access control system 10, an illustrative and non-limiting example of which is shown on Figure 4C, the DCU 16 can be used to retrofit a preexisting key reader 12', such as a Wiegand key reader, magnetic card strip reader or any other suitable type of key reader. In this regard, the DCU 16 is preferably not in direct communication with the preexisting key reader 12'. Illustratively, the DCU 16 is generally supplied current from the power supply 28 used to supply the preexisting key reader 12'. Preferably, the tamper switch 36 is similarly installed behind preexisting key reader 12' and connected to an input of the DCU 16, the output of which is, preferably, in turn connected to a relay 115, for example also installed within the enclosed region 54 or gap, which controls the connection between the preexisting key reader 12'and the latch release mechanism 14. Initially, the DCU 16 is enabled, for example using a programming cable or the like and a programming device (both not shown), such that the DCU 16 controls the relay 115 to interconnect the preexisting key reader 12' with the latch release mechanism 14. As such, the preexisting key reader 12' can be used normally to actuate the latch release mechanism 14 thereby opening the door. In the event a tampering event is detected via the tamper switch 36, the DCU 16 disables the relay 115 thereby severing the connection between the preexisting key reader 12' and the latch release mechanism 14, and as a result entry via the door 20 is prohibited until such time as the DCU 16 is reprogrammed, for example using the programming cable or the like and programming device.

[0040] In some particular embodiments, a plurality of tamper switches as in 36 can be provided, for example attached to different components of the system susceptible to tampering, such as the buzzer or power supply or the like.

[0041] In some embodiments, the key card or the key 116 has stored thereon a coded ID or the like which is used to identify the key holder. In some embodiments of the key reader 12, illustrative and non-limiting examples of which are shown on Figures 5A, 5B and 5C, instead of a coded key card, the key 116 comprises a small fob like device which is received in a complementary keyport 118 in the key reader 12. When the key 116 is inserted into the keyport 118, the coded ID is transferred between the key 116 and the key reader 12 via an interface 120, for example comprising a plurality of small conductive pins as in 122 which contact a complementary set of conductive contact plates as in 124 positioned within the keyport 118. Illustratively, the interface is bidirectional and can also be used to transfer information back to the key 116 from the key reader 12, for example confirmation of access which can be fed later into an appropriate administrative system or the like (not shown), as well as power, as discussed below.

[0042] In some of these embodiments, illustrative and non-limiting examples of which are shown on Figures 5A, 5B and 5C, in order to retain the key 116 within the keyport 118, a magnet 126 is provided within the key housing 128 which attracts a ferrous plate 130 or complementary magnet (not shown) or the like positioned within the key reader housing 132. An additional small magnet 134 is preferably provided in the key reader housing 132 which

is attracted to a corresponding ferrous plate or complementary magnet (neither shown) or like embedded in the key housing 128 and ensures correct alignment of the key 116 in the key port 118.

[0043] In various embodiments, the card reader comprises means for sensing the key or key card. In some of these embodiments, illustrative and non-limiting examples of which are shown on Figures 5A, 5B and 5C, the key 116 comprises a small battery 136 (not shown), typically rechargeable. When proximate, magnetic attraction causes the key 116 to be anchored within the key port 118, thereby interconnecting the small conductive pins as in 122 with the complementary set of conductive contact plates as in 124. At the same time, a micro switch 138 on the key housing is depressed thereby completing an electrical circuit, however in an alternative embodiment the completion of the interconnection between key 226 and reader 26 can be sensed by other means, for example via interconnection of the small conductive pins as in 122 with the complementary set of conductive contact plates as in 124. Of note is that in the present illustrative embodiment or similar powered-key embodiments, the key 116 can be used to power not only the key 116 but also the key reader 12, the DCU 16 and the door latch mechanism 14 via the interface 120. One particular advantage of this configuration is that the door access control system 10 requires no additional source of power, thereby eliminating the requirement for powering the door access control system 10 by other means, such as by providing a PoE, USB connection or mains current and transformer or the like. This allows the door access control system 10 to be used in places where such a system would otherwise typically not be able to be used, for example in cases where other sources of power are generally not available or in remote areas and the like.

[0044] In some embodiments, an illustrative and non-limiting example of which is shown on Figure 5A, the key reader 12 additionally comprises a microprocessor/controller 140, a small OLED screen 142, a three button keypad 144, a power regulator 145, a USB interface 146, a status LED 148 and a DCU I/O interface 150 for communicating with the DCU(s) 16. A memory 152 is also provided which can include Flash Memory 154, EEPROMs 156, SRAM 158 and the like. Additionally, a Real Time Clock (RTC) and supercap circuit 160 are provided for.

[0045] In some embodiments, an illustrative and non-limiting example of which is shown on Figure 5B, the key 116 comprises a microprocessor/controller 162and a non-volatile memory 166, possibly with a USB interface 164, for example in addition to the magnets 126, 134 and battery 136. Memory 166 can be used for storing access codes and the like as well as other information such as time stamps received from the DCU 16 via the key reader 12. The USB interface 164 can also be conveniently used for battery recharging, for example through provision of an appropriate base station (not shown) which can also be used to conveniently transfer information stored within the key 116 to an external administration system or the like (also not shown). Additionally the USB interface 164 can be used by the administration system to update access rights stored on the key, for example during transfer of a key from one user to another or when the access rights of a particular user are modified. In some particular embodiments, the key could also include a wireless interface (not shown), such as WiFi, for programming and update purposes.

[0046] In some embodiments, illustrative and non-limiting examples of which are shown on Figures 1 and 5C, the keypad comprises three buttons 168 which, as described above, can be used to input an alphanumeric PIN number (not shown) or the like. The key reader 12 comprises a housing 170 which is preferably secured to the door frame 18 or on a wall in proximity to the door 20. A communication cable (not shown) is provided, for example fed through a hole bored in the frame or wall, to interconnect the key reader 12 with the DCU 16 via their respective I/O interfaces 70, 150.

[0047] In some embodiments, an illustrative and non-limiting example of which is shown on Figure 5C, in still another alternative embodiment, the key comprises a biometric key, such as a fingerprint, handprint, retina scan or the like, typically in combination with a pin number. In this regard, the key reader is equipped with an appropriate sensor and processing (both not shown) for acquiring the biometric key, and the pin number can be entered via the key pad 86, which are subsequently transferred to the DCU for verification.

[0048] In some embodiments, illustrative and non-limiting examples of which are shown on Figures 6A and 6B in addition to Figure 1, the latch release mechanism 14 comprises a solenoid 172 wherein application of a suitable DC current across a pair of input terminals 174 causes a ferrous shaft 176 to retract within a magnetic coil 178, thereby disengaging the striker plate 180 and allowing the door 20 to be opened freely.

[0049] In some embodiments, illustrative and non-limiting examples of which are shown on Figure 2 in addition to Figure 3, as discussed above, in order to ensure that the input voltage is sufficient to operate the latch release mechanism 14, a charge pump 66 is provided. In particular when the requisite operating power is provided by the key 116, the charge pump 66 serves to raise the relatively low (3VDC for example) input voltage to the voltage necessary to operate the solenoid of the latch mechanism, typically between 12VDC or 24VDC but in particular cases between 3VDC and 28VDC or others. Illustratively, and in order to supply the requisite current the input voltage is converted into the requisite output DC voltage (for example from 3VDC to 12VDC or 24VDC) and generally used to charge a capacitor bank (not shown). Once charged, the capacitor bank is discharged over the inputs of the solenoid, thereby providing sufficient current of sufficient voltage for sufficient time to allow the user to open the door. In particular, the charge pump preferably provides a short pulse current of several

milliseconds duration and of voltage (respectively 12V and 24V for example) sufficient to cause the solenoid to move to release the latch mechanism, and then provides a hold current (for example obtained by a voltage of about 5V) until the door is opened by the user or a preprogrammed time limit reached.

[0050] In some embodiments for particular applications, an illustrative and non-limiting example of which is shown on Figure 7, as discussed briefly above, one or more key readers as in 12 can be combined with a number of DCUs as in 16 to provide access to a multiple limited access areas. In a particular embodiment, the door access control system 10 is used within an elevator and works in concert with the elevator control panel 182 to selectively enable a plurality of buttons as in 184, thereby allowing the coded ID cards to allow restricted access to individual floors. The door access control system 10 can also conveniently take advantage of the power (24V generally) supply 186 which is typically found within the elevator cabin thereby providing for easy retrofit without requiring additional wires and the like to be installed and/or fed into the elevator cabin.

[0051] In some of these embodiments, an illustrative and non-limiting example of which is still shown on Figure 7, one DCU as in 16 is associated with each area (typically a floor or group of floors) of limited access. In operation, a user's key card or key (not shown) is read by the key reader 12 (for example including any PIN numbers or other identification information required) and its details communicated to the DCUs as in 16. The DCU(s) as in 16 associated with the area(s) for which the key card provides access subsequently enable their associated button(s) as in 184 which can then be selected by the user.

[0052] Referring now to Figures 8A through 8E in addition to Figure 5B, different illustrative and non-limiting views of the key 116 are provided.

[0053] While this invention has been described with reference to the illustrative embodiments, this description is not intended to be construed to a limiting sense. Various modifications or combinations of the illustrative embodiment of the invention will be apparent to persons skilled in the art upon reference to the description. It is therefore intended that the described invention encompass any such modifications or embodiments.

Claims

1. An electronic door access control apparatus for restricting access via a door (20) installed in a door frame (18) and comprising a lock mechanism having a latch bolt (22) and using a key comprising a unique coded ID sequence, the apparatus comprising:

   a key reader (12) for reading the key and comprising a tamper switch (36);
   a latch release mechanism (14); and
   a door control unit (16) separate from said key reader and said latch release mechanism, installed in the door frame proximate to said key reader and said latch release mechanism and comprising a controller (58) and memory comprising a plurality of predetermined allowed coded ID sequences, wherein said door control unit is in communication with said tamper switch;
   characterized in that the apparatus further comprises an encrypted binding between said key reader and said door control unit and is configured such thatwhen the key is positioned proximate to said key reader, the coded ID sequence is read by the key card reader and relayed to said door control unit via an encrypted communication channel for processing, wherein when the coded ID sequence matches one of said plurality of predetermined allowed coded ID sequences, said door control unit actuates said latch release mechanism, thereby allowing the door to be opened, and further wherein when said DCU detects tampering of said key reader via said tamper switch, said encrypted binding between said key reader and said door control unit is terminated, thereby preventing actuation of said latch release mechanism.

2. The apparatus of Claim 1, wherein said key reader comprises a screen and an input interface for manually entering a password and further wherein said password is relayed to said door control unit via said encrypted communication channel for processing with the unique coded ID, and wherein said input interface preferably comprises at least one of a key pad and a proximity sensor using an electric field for sensing and recognizing the motion of a user's hand or finger.

3. The apparatus of Claim 1 or 2, wherein the lock mechanism comprises a latch bolt and wherein said latch release mechanism is configured for receiving said latch bolt and comprises a striker plate and a solenoid and further wherein said door control unit actuates said latch release mechanism by activating the solenoid, thereby releasing said striker plate.

4. The apparatus of Claim 1 to 3, wherein said door control unit can only be reestablished by reprogramming said door control unit once said encrypted binding between said key reader and said door control unit is terminated.

5. The apparatus of Claim 1 to 4, wherein said key reader is interconnected with said door control unit via a wired connection.

6. A method for retrofitting an existing electronic door access control system for restricting access via a

door (20) and comprising a lock mechanism having a key reader (12) for reading a key comprising a unique coded ID sequence, a latch release mechanism (14) and a power supply (28), **characterized in that** the method comprises:

associating a tamper detector (36) having an output with the key reader;
interconnecting the key reader and the latch release mechanism using a relay (115), wherein said relay is normally closed; and
controlling opening and closing said relay with a resettable door control unit (16) powered by the power supply, wherein said tamper detector output is input into said door control unit;
wherein when tampering is detected via said input, said door control unit opens said normally closed relay and thereby preventing the key reader from actuating the latch release mechanism.

7. The method of Claim 6, wherein once open, said relay can only be closed by reprogramming said door control unit and wherein said door control unit preferably comprises a USB interface and further comprising reprogramming said door control unit via said USB interface using an external reprogramming device.

8. An electronic door access control system for restricting access via a door (20) comprising a lock mechanism having a latch bolt (22), the system comprising:

a key (116) comprising a unique coded ID sequence and a key memory;
a key reader (132) for reading said key;
a latch release mechanism (14); and
a door control unit (16) comprising a controller (140), a real time clock (160), a door control unit memory (152) and a door identifier;
wherein said system is configured such that, when said key is positioned proximate to said key reader, the coded ID sequence is read by said key card reader and relayed to said door control unit and further wherein when the coded ID sequence matches one of said plurality of predetermined allowed coded ID sequences, said door control unit actuates said latch release mechanism, thereby allowing the door to be opened, and further wherein a time stamp and said door identifier is relayed to said key for storage in said key memory.

9. The system of Claim 8, wherein said key comprises a power source and further wherein when the key is positioned proximate to said key reader, said power source provides power for operating said key reader, said latch release mechanism and said door control unit.

10. The system of Claim 8 or 9, wherein the lock mechanism comprises a latch bolt and said latch release mechanism is configured for receiving the latch bolt and comprises a striker plate and a solenoid, and further wherein said door control unit actuates said latch release mechanism by activating the solenoid, thereby releasing said striker plate.

11. An electronic door access control system for restricting access via a door (20) installed in a door frame (18) and comprising a lock mechanism having a latch bolt (22), **characterized in that** the system comprises:

a key (116) comprising a unique coded ID sequence and a power source (136) having a key voltage;
a key reader (132) for reading said key;
a latch release mechanism (14) configured for receiving the latch bolt and comprising a striker plate and a solenoid (172) only actuatable using an actuating voltage greater than said key voltage; and
a door control unit (16) comprising a controller (58), a door control unit memory (60) and a charge pump (66), an output of said charge pump connected across an input of said solenoid;
wherein said system is configured such that, when said key is positioned proximate to said key reader, said key power source supplies power for operating said key reader and said door control unit and further wherein once powered said coded ID sequence is received by said key card reader and relayed to said door control unit and further wherein when said coded ID sequence matches one of said plurality of predetermined allowed coded ID sequences, said door control unit activates said charge pump using said key voltage, said charge pump raising said key voltage to said actuating voltage thereby actuating said solenoid and allowing the door to be opened.

12. The system of Claim 11, wherein said power source is a battery, wherein said key and said key reader each comprise a pair of contacts, wherein positioning said key proximate to said key reader comprises interconnecting said respective pairs of contacts such that said battery supplies power for operating said key reader and said door control unit via said pairs of contacts and wherein said key preferably comprises a normally open microswitch between said power source and at least one of said pair of contacts such that when said microswitch is closed by contact with

said key reader an electrical circuit is completed between said power supply and said contacts.

13. The system of Claim 11 or 12, wherein said key is held removeably against said key reader by a magnet.

14. The system of Claim 11 to 13 wherein once said solenoid is actuated, a voltage across said output of said charge pump is lowered to a holding voltage lower than said actuating voltage.

15. The system of Claim 11 to 14, wherein said key voltage is less than 5 volts and said actuating voltage is greater than 12 volts.

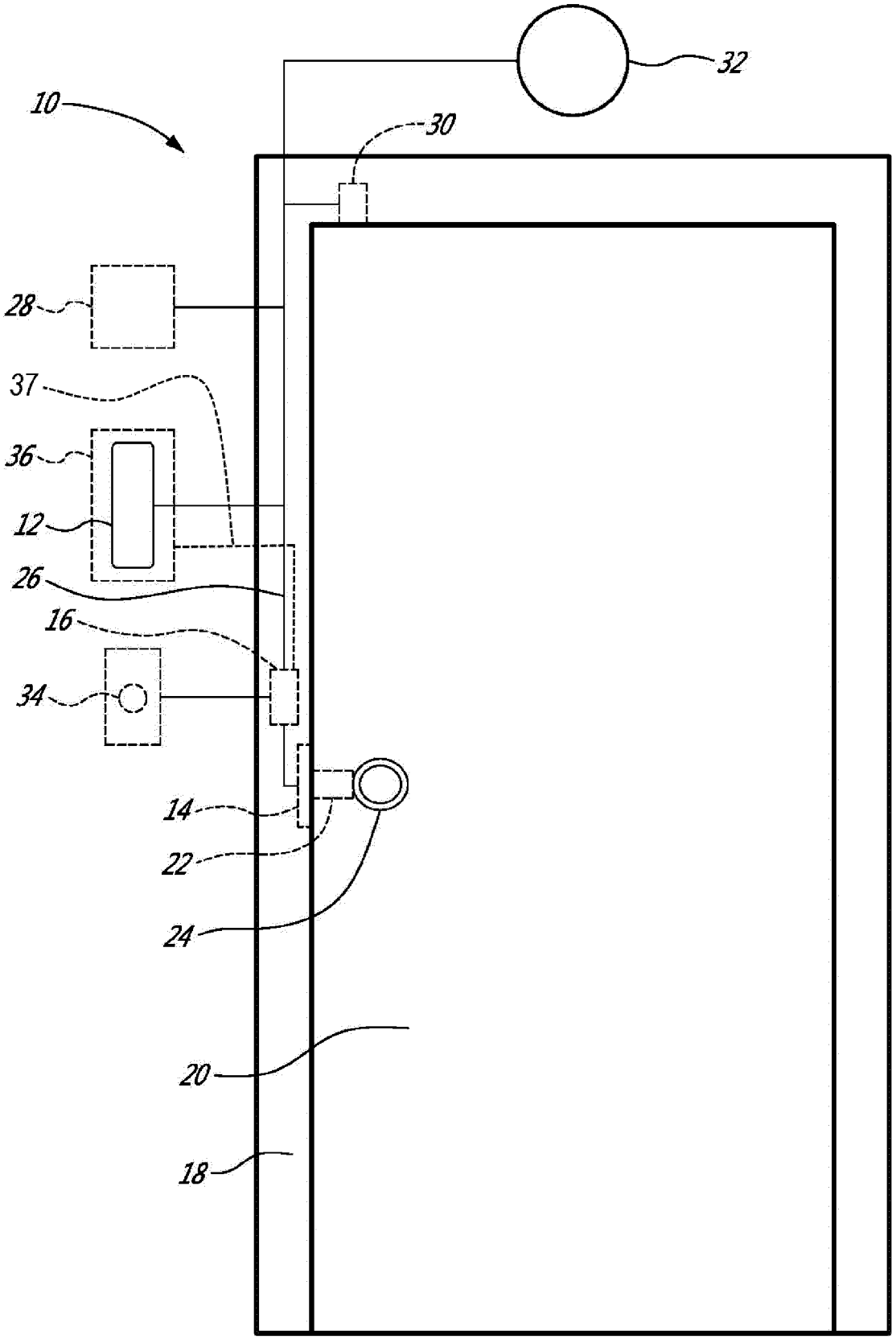

Fig. 1

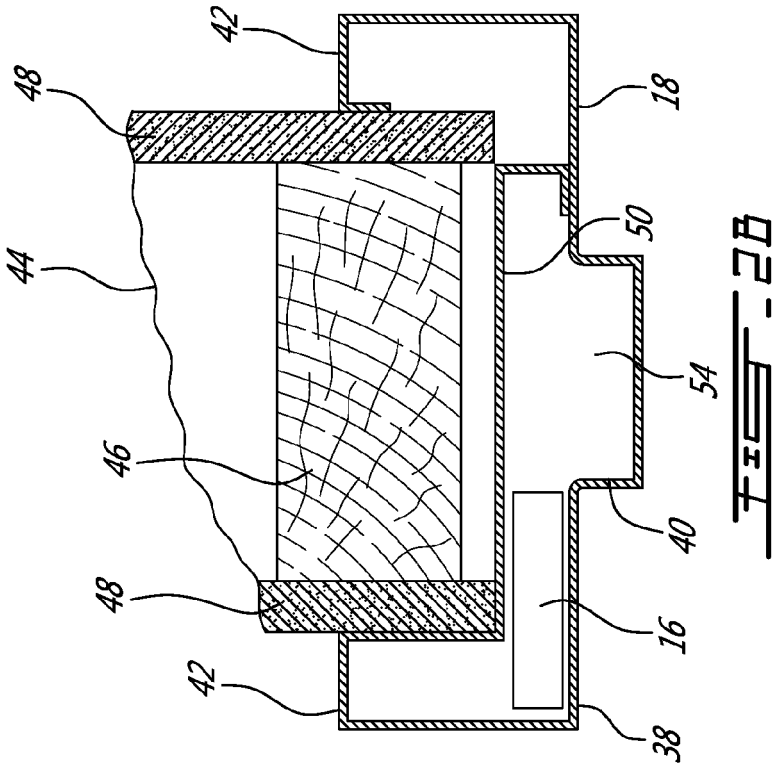
42
48
18
44
50
54
46
40
48
16
42
38

FIG - 2B

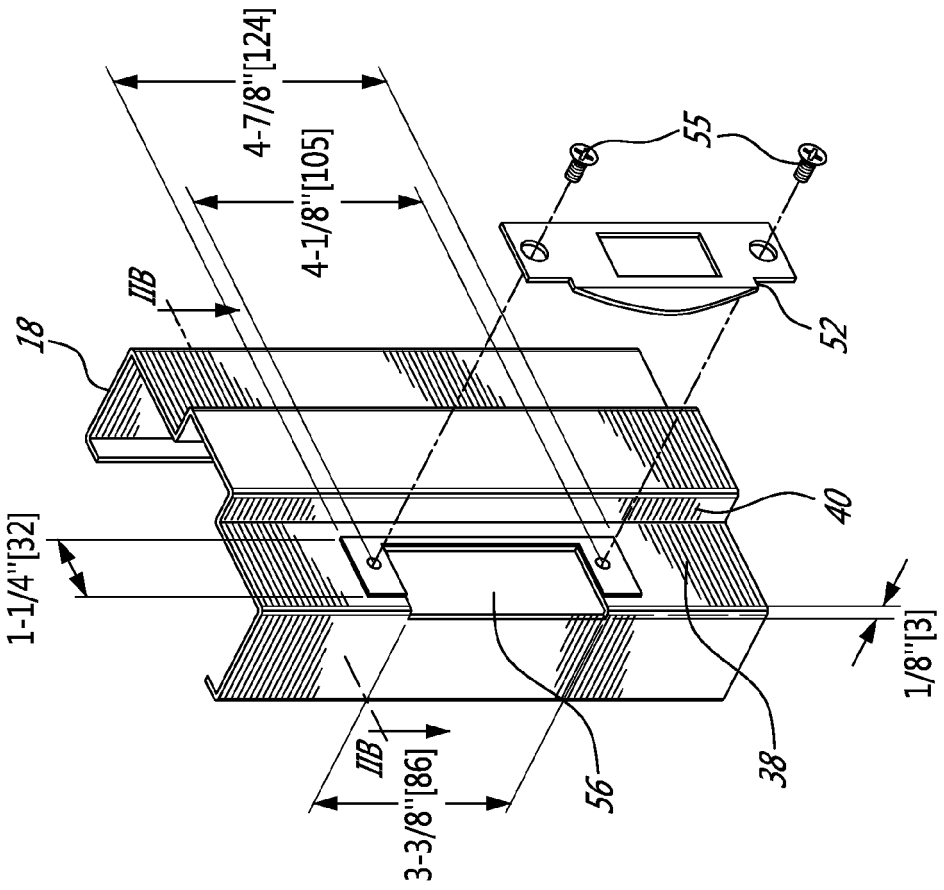
4-7/8"[124]
4-1/8"[105]
IIB
18
55
52
40
1-1/4"[32]
1/8"[3]
IIB
3-3/8"[86]
56
38

FIG - 2A

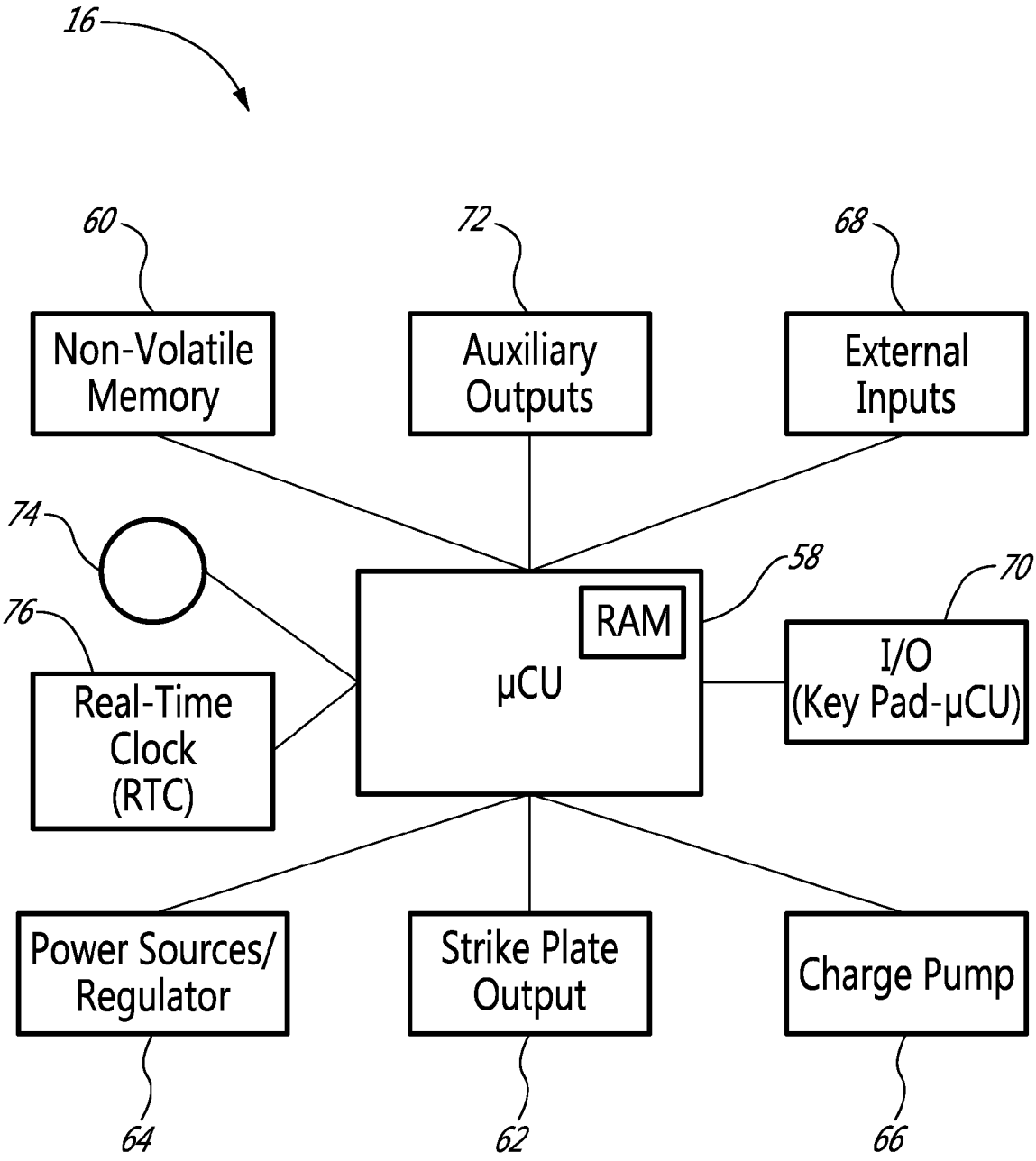
16
60
Non-Volatile Memory
72
Auxiliary Outputs
68
External Inputs
74
76
Real-Time Clock (RTC)
RAM
µCU
58
70
I/O (Key Pad-µCU)
Power Sources/ Regulator
64
Strike Plate Output
62
Charge Pump
66

Fig. 3

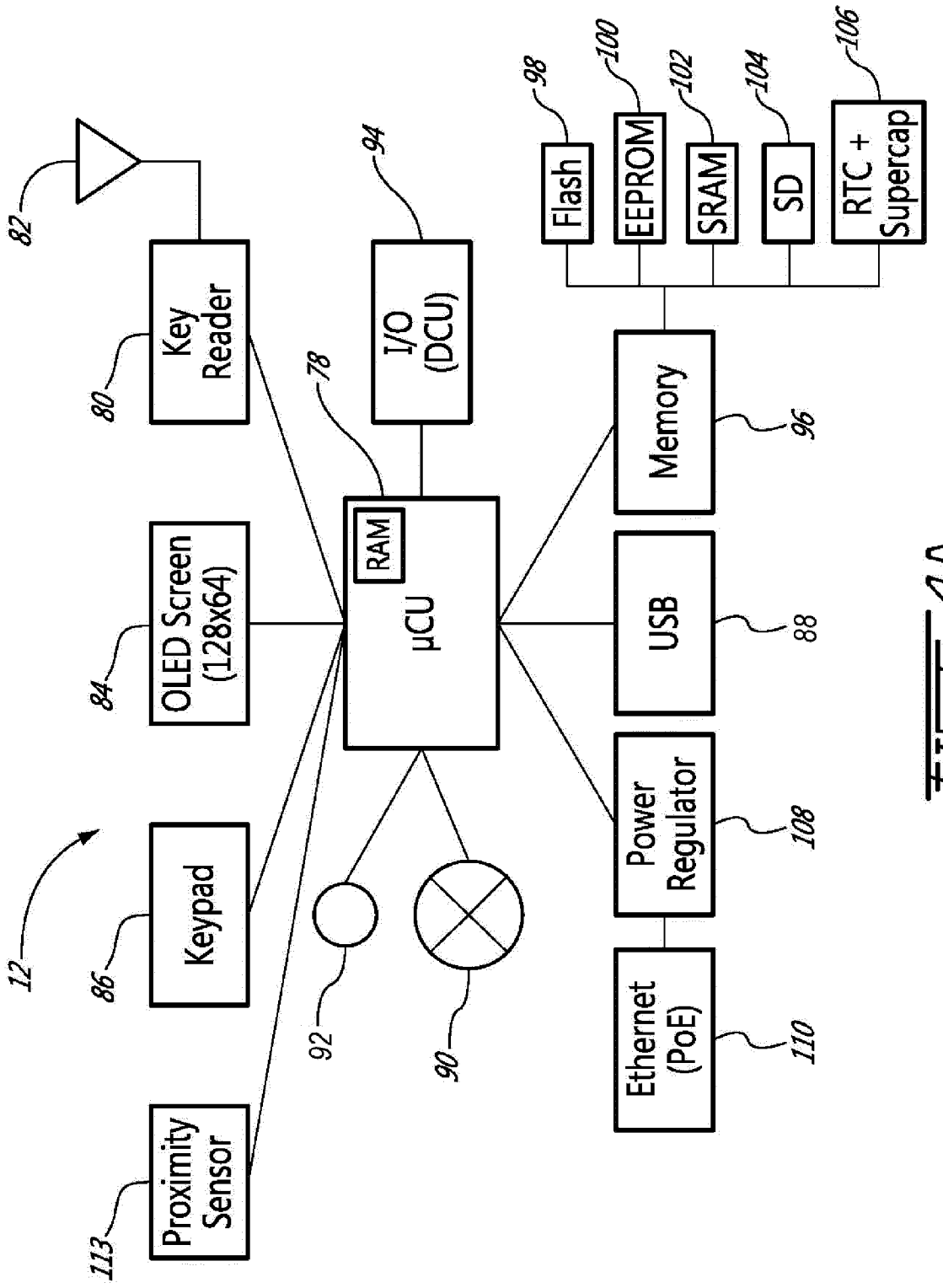
82
Key Reader
80
I/O (DCU)
94
78
RAM
µCU
OLED Screen (128x64)
84
Keypad
86
12
Proximity Sensor
113
92
90
Flash
98
EEPROM
100
SRAM
102
SD
104
RTC + Supercap
106
Memory
96
USB
88
Power Regulator
108
Ethernet (PoE)
110

Fig. 4A

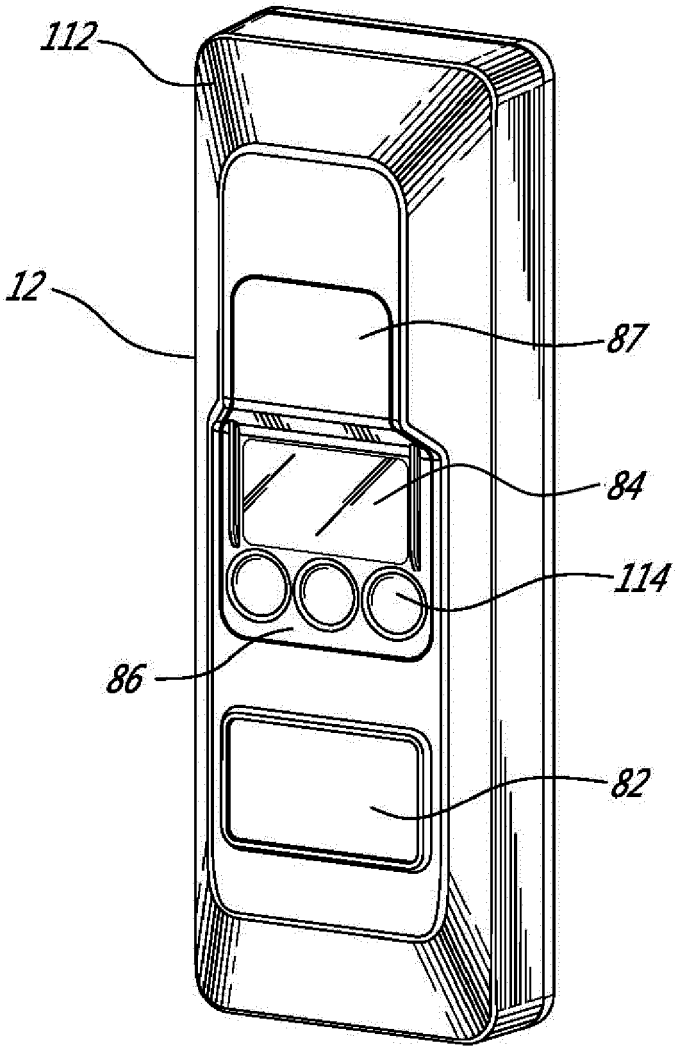

Fig. 4B

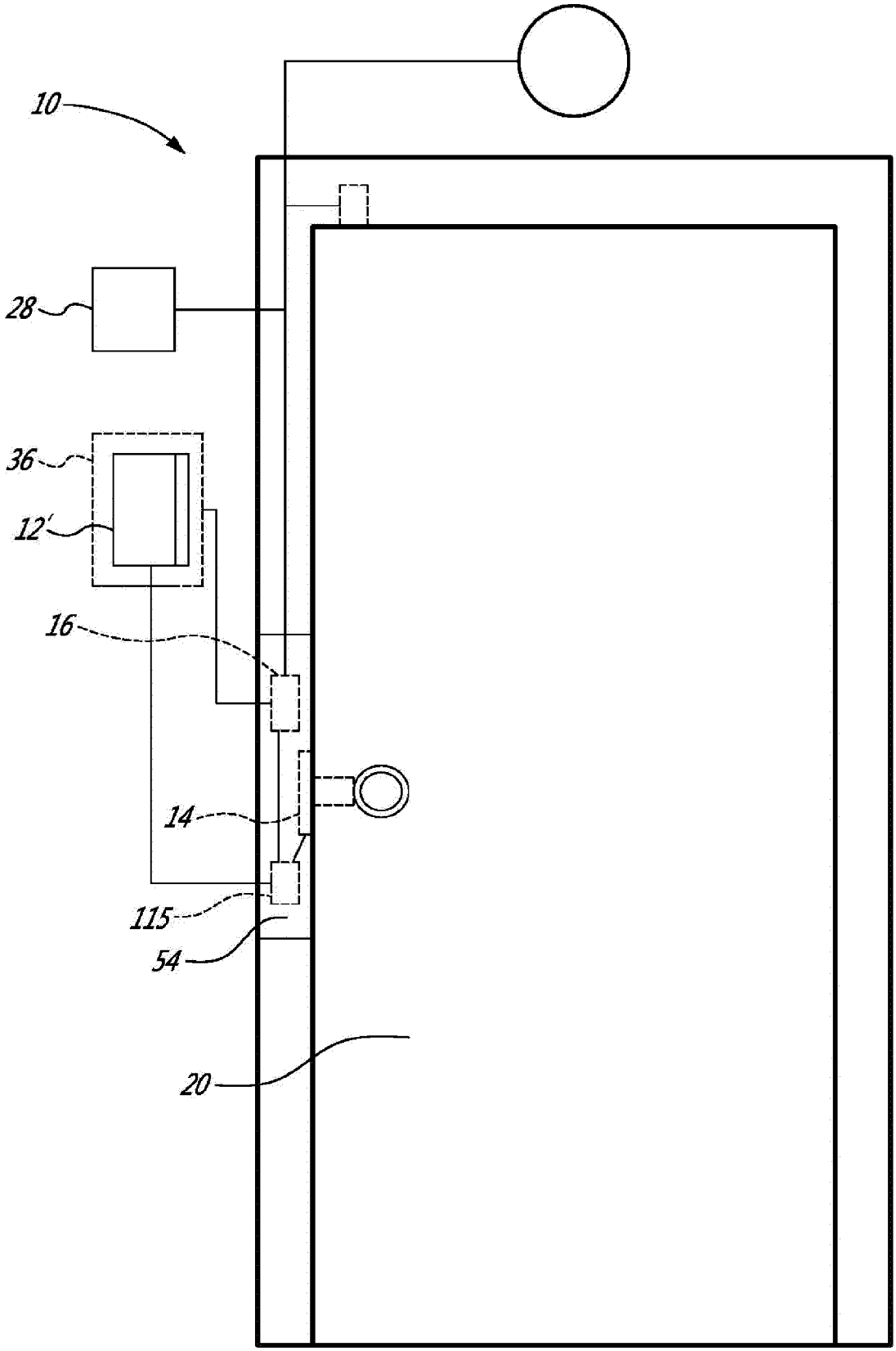

Fig. 4C

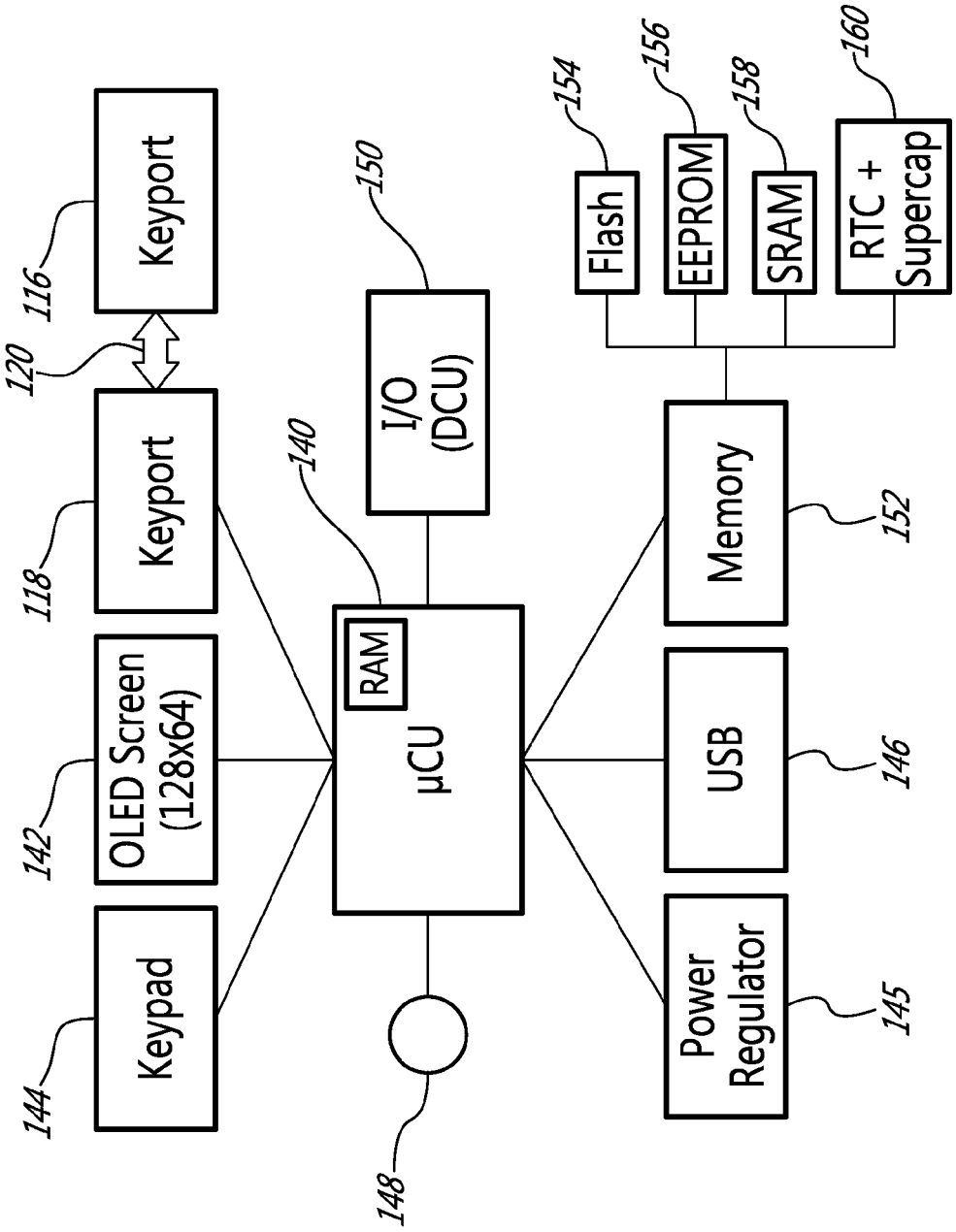
Keyport
116
120
Keyport
118
OLED Screen (128x64)
142
Keypad
144
RAM
µCU
140
I/O (DCU)
150
148
154
Flash
156
EEPROM
158
SRAM
160
RTC + Supercap
Memory
152
USB
146
Power Regulator
145

FIG. 5A

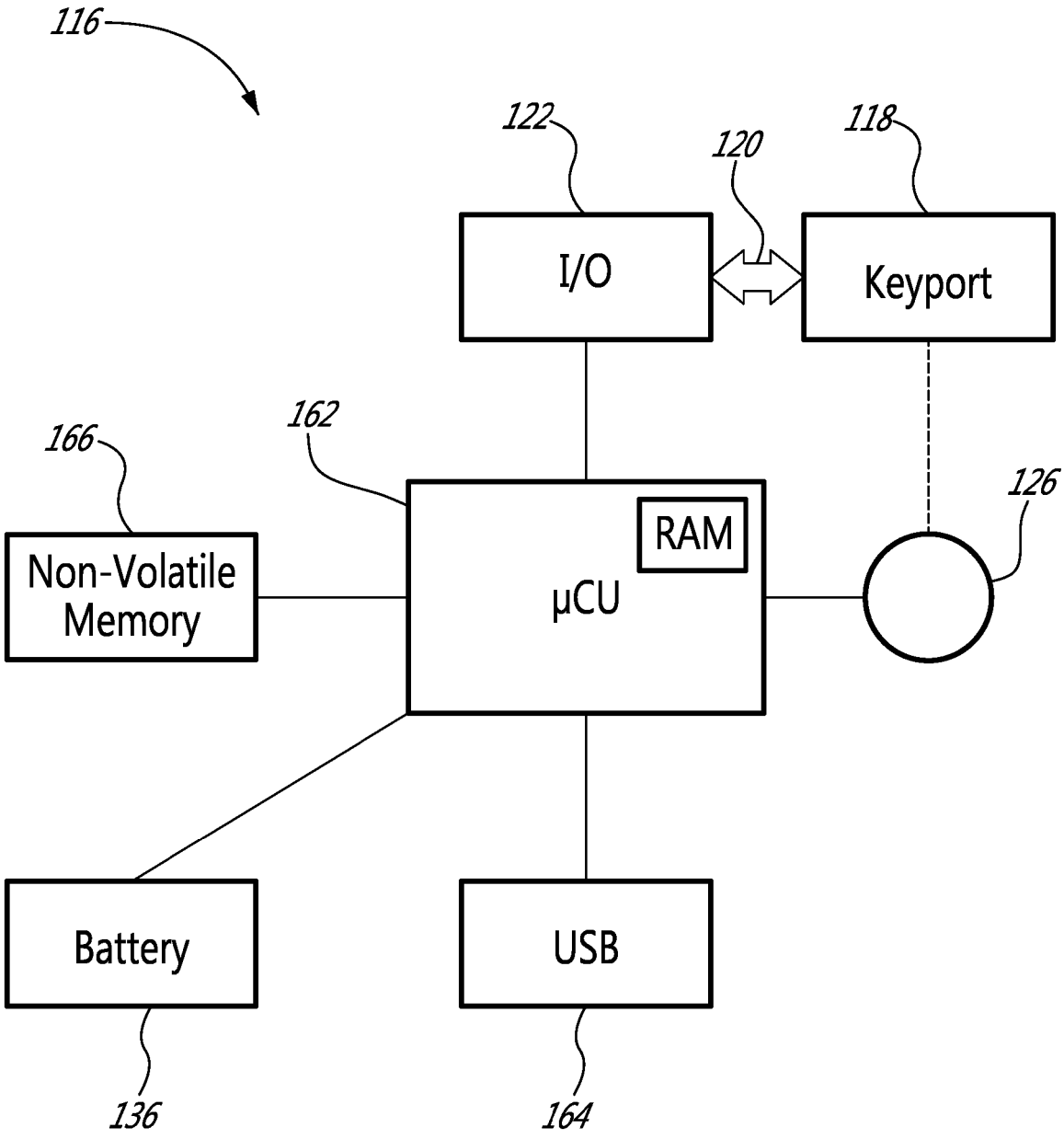
116
122
120
118
I/O
Keyport
162
166
126
RAM
Non-Volatile Memory
µCU
Battery
USB
136
164

Fig. 5B

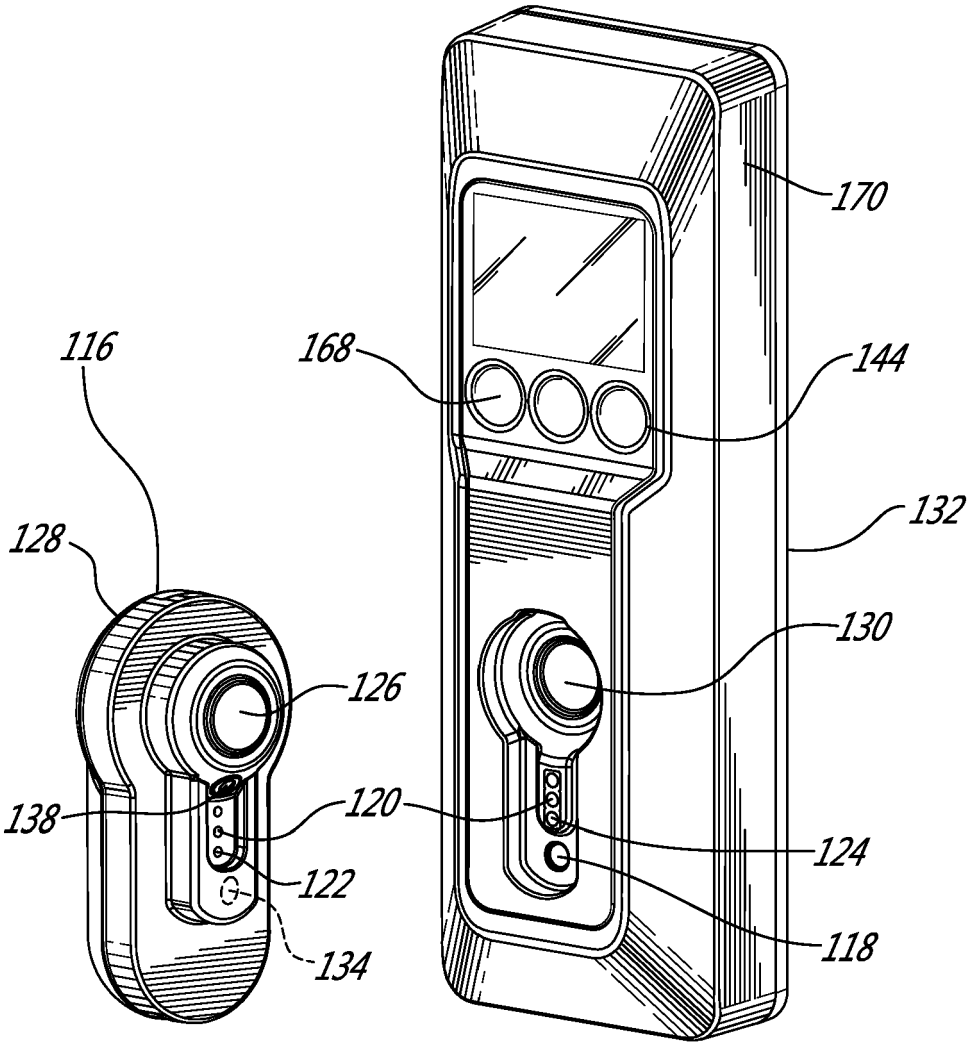

Fig. 5C

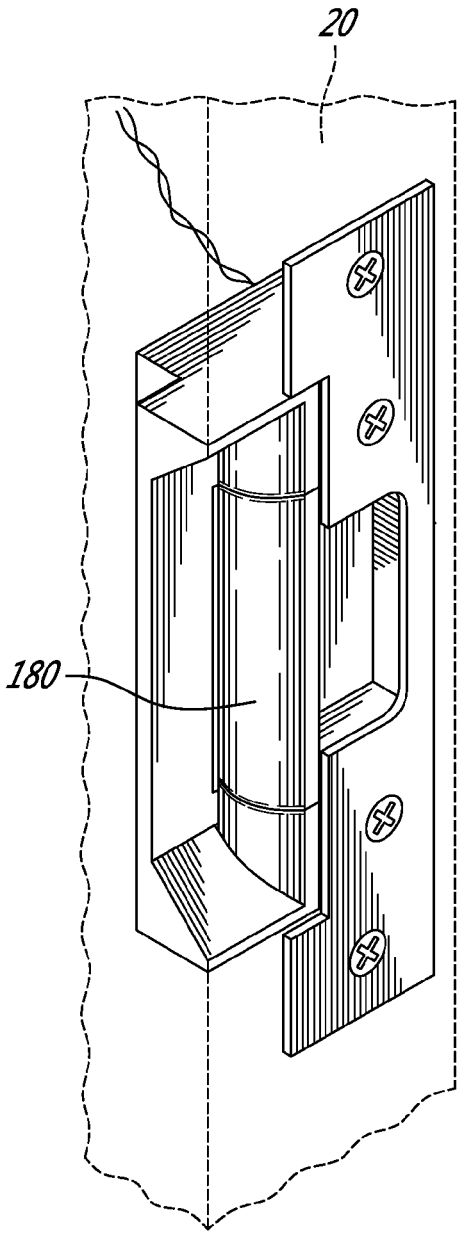

Fig. 6A

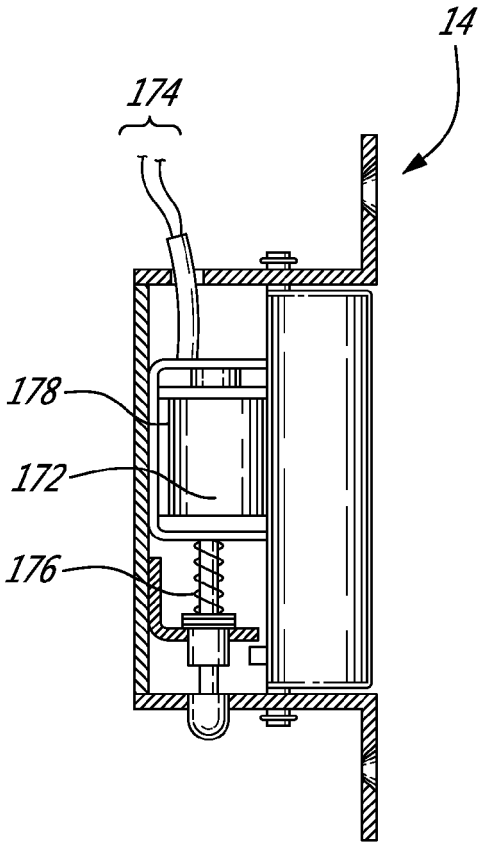

Fig. 6B

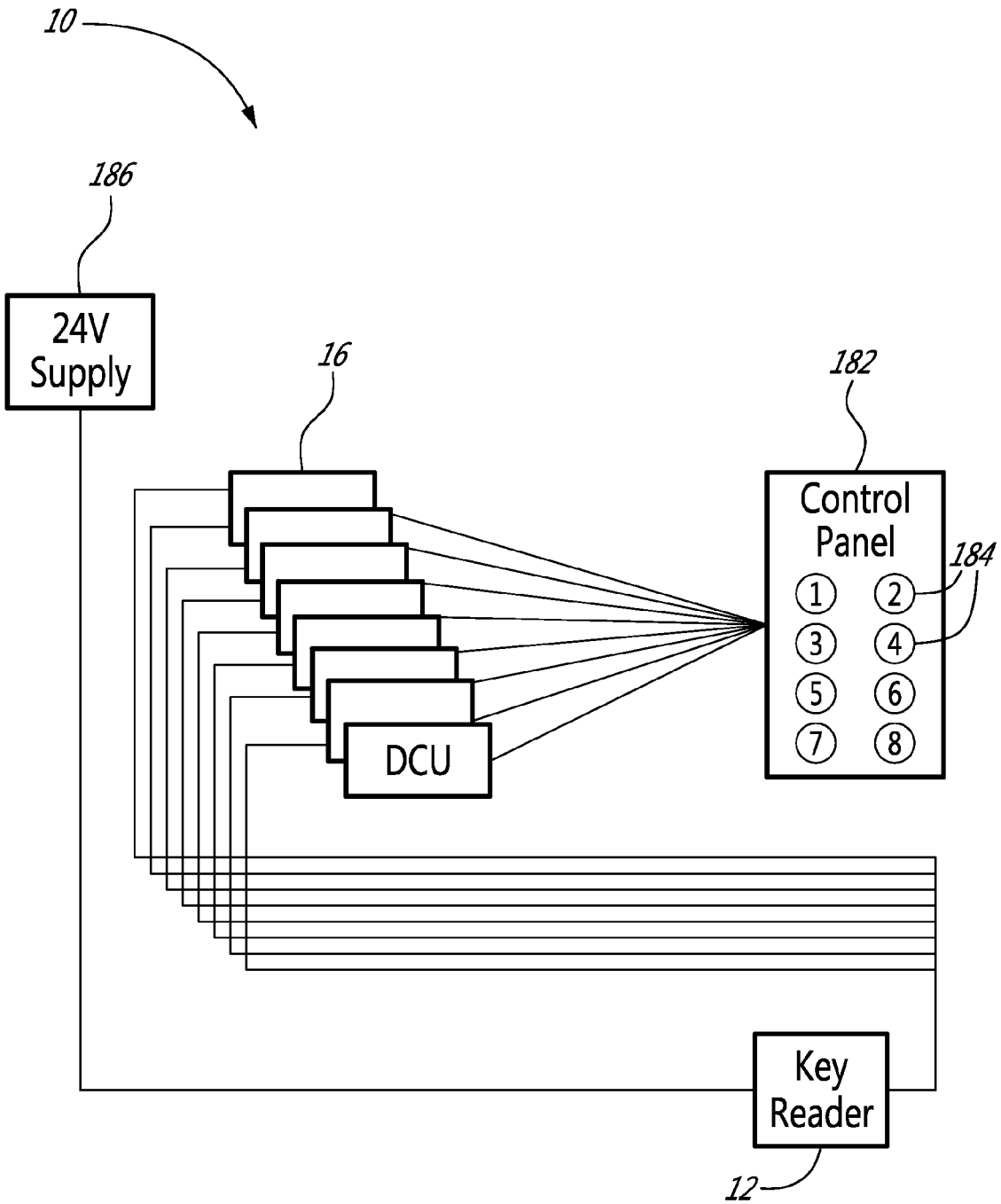
10
186
24V Supply
16
182
Control Panel
184
1
2
3
4
5
6
7
8
DCU
Key Reader
12

Fig. 7

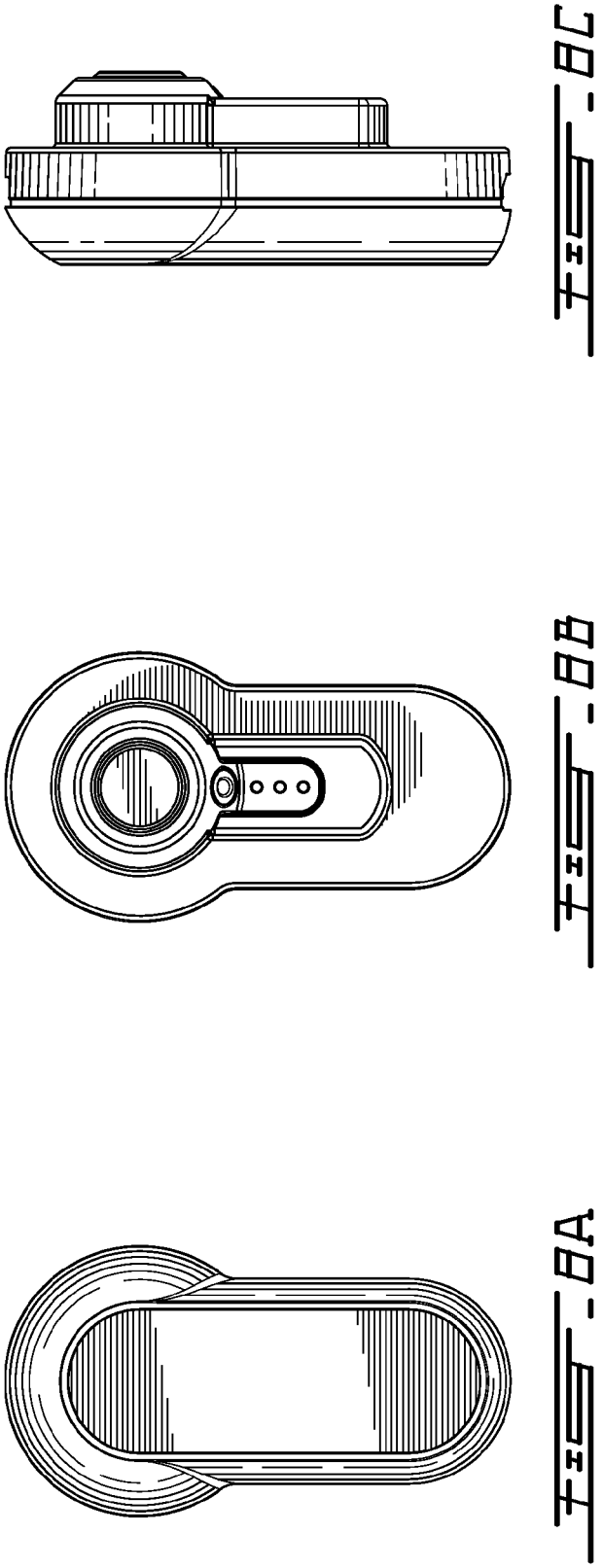
FIG-8A
FIG-8B
FIG-8C
FIG-8D
FIG-8E

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 14 16 5305

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 5 606 615 A (LAPOINTE BRIAN K [US] ET AL) 25 February 1997 (1997-02-25) * abstract * * column 1, line 5 - line 9 * * column 2, line 36 - column 3, line 2 * * column 3, line 28 - line 31 * * column 4, line 45 - column 8, line 54 * * column 10, line 8 - line 67 * * figures 1-3 * -----	1-5	INV. G07C9/00
Y	GB 2 395 978 A (NCR INT INC [US]) 9 June 2004 (2004-06-09) * page 3, line 1 - page 4, line 2 * * page 5, line 20 - page 10, line 18 * * page 11, line 7 - line 12 * * figure 1 * -----	1-5	
Y	EP 0 104 767 A2 (FIGGIE INT INC [US]) 4 April 1984 (1984-04-04) * page 2, line 19 - page 3, line 23 * * page 4, line 26 - page 7, line 34 * * page 11, line 1 - line 11 * * page 12, line 36 - page 13, line 12 * * page 25, line 21 - page 27, line 12 * * page 33, line 19 - page 41, line 12 * -----	1-5	TECHNICAL FIELDS SEARCHED (IPC) G07C E05B
A	WO 00/77330 A1 (BEST ON LINE SECURITY SYSTEMS [US]; WENKMAN GREGORY J [US]; WENKMAN WI) 21 December 2000 (2000-12-21) * page 7, line 10 - page 9, line 2 * * page 10, line 30 - page 12, line 5 * * figures 1,2 * -----	1,3	

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
The Hague	24 September 2014	Van der Haegen, D

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)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Application Number
EP 14 16 5305

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing claims for which payment was due.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☒ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

1-5

☐ The present supplementary European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims (Rule 164 (1) EPC).

Europäisches Patentamt
European Patent Office
Office européen des brevets

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 14 16 5305

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-5

   Electronic door access control apparatus preventing tampering by using an encrypted binding.

   ---

2. claims: 6, 7

   Method for preventing tampering by switching a normally closed relay.

   ---

3. claims: 8-10

   Electronic door access control system storing a time stamp and a door identifier in a key used for accessing a door.

   ---

4. claims: 11-15

   Electronic door access control system making use of a charge pump to obtain a voltage required for actuating a latch.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 14 16 5305

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.

24-09-2014

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5606615 A	25-02-1997	NONE	
GB 2395978 A	09-06-2004	GB 2395978 A	09-06-2004
		US 2004134980 A1	15-07-2004
EP 0104767 A2	04-04-1984	DE 3381363 D1	26-04-1990
		EP 0104767 A2	04-04-1984
		JP S59109676 A	25-06-1984
WO 0077330 A1	21-12-2000	AU 5331500 A	02-01-2001
		WO 0077330 A1	21-12-2000

EPO FORM P0459

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