

## LOCK SYSTEM, ACCESS CONTROLLER AND KEYPAD

### Field and Background of the Invention

5 The invention generally relates to a lock system and an access controller, particularly but not exclusively, for doors, and also to a keypad suitable for use with such an access controller.

Access controllers have gained popularity as companies and individuals are  
10 swapping the conventional key access with code access which may be in the form of card, PIN or biometric access. Typical access controllers include a memory which stores a database of reference codes and if an access code received matches what is in the memory, this provides access, for example, by unlocking a door lock. It is also common for such access controllers to be  
15 provided with a keypad for a user to input a PIN to open the lock. The keypad usually comprises a number of keys or buttons, each carrying a permanent number from 0 to 9. If the access code is not changed regularly, the buttons on the keypad would experience wear and tear stemming from the frequent physical depression of the buttons by users. As such, the most often used  
20 buttons would appear more distinct than the other buttons after prolonged periods of use, thereby giving hints as to what the access code might be. This compromises security of the access controller.

Further, it is possible to spy or survey physical input motions of a user when entering the code onto the keypad of the access controller and since the numbers appearing on each of the buttons are fixed, it is possible to figure out what the access code might be.

5

To address the above problem(s), it has been proposed to provide a keypad that scrambles the numbers carried by each key/button after each access so that it increases the difficulty of guessing what the access code is.

- 10 It is an object of the present invention to provide an alternative access controller and keypad which provide the public with a useful choice.

### Summary of the Invention

- 15 It is an object of the invention to provide an access controller comprising a memory for storing reference access codes, the reference access codes including a one-time use reference access code; an input interface for allowing a user to input an access code; a processor configured to receive inputs from the input interface and if the input access code matches the one-time use
- 20 reference access code, allow access once and prevents subsequent access based on same input access code.

By having a one-time use reference access code, this provides additional security so that such an access code may be used for personnel needing to gain access on a temporary basis.

- 5     The input interface may comprise a plurality of keys which is configured to display every possible character to form the access code, and the processor may be configured to change the character that is displayed by each key. In this way, the position of each keys are scrambled which makes it difficult for someone to spy on the user to find out the access code.

10

The processor may be configured to change the character after depressing a key on the input interface, and the key may be a "Start" button to initialize the access controller. The input interface may include a plurality of polycarbonate casing, with each casing arranged to cover a corresponding key.

15

The access controller may comprise light elements arranged to form the characters carried by the keys. The processor may be configured to turn at least some of the light elements off if no input is received by the input interface for a predetermined amount of time. This further increases the security level

20     of the access controller.

It is envisaged that the processor may be configured to turn off at least some of the light elements after each access. The access controller may comprise means for acknowledging receipt of an input on the input interface. The

acknowledgement means may include a sound buzzer.

In a second aspect of the invention, there is provided an access controller comprising a memory for storing a plurality of reference access codes, each  
5 reference access code being associated with a different access level which define restrictions as to when the associated reference access codes gain access; an input interface for allowing a user to input an access code; a processor configured to receive inputs from the input interface, and if the input access code matches one of the stored reference access code, determine the  
10 access level of the input access code based on the plurality of reference access codes reference in the memory and if the associated restriction does not apply, allow access and if the associated restriction applies, refuse access.

With the configuration of the second aspect, in addition to an access code or  
15 password, the access controller is able to define another security level through the use of different access levels associated with the reference access codes.

The access levels may be based on date and time. The timer may include an electronic calendar which provides the date and time. The restrictions may be  
20 based on the day of week for example, weekends have a different restriction than weekdays.

The access controller may further comprise more than one reference code for each type of access level, each reference code having an expiry date, and at any one time, there is only one active reference code which gains access. With this configuration, upon expiry of one of the reference codes, another reference  
5 code may become the active one. Preferably, this is preprogrammed by the user before installing the access controller (and thus automatic) and no external intervention is needed.

Preferably, there is a master access level and the reference access codes  
10 associated with the master access level is restriction free. The reference access codes associated with this master access level may then be allocated to administrators of the access controller who then have overriding control.

The input interface may comprise a plurality of keys which is configured to  
15 display every possible character to form the access code, and the processor may be configured to change the character that is displayed by each key. The processor may be configured to change the character if the appropriate setting is programmed beforehand.

20 In a third aspect, there is provided a lock system comprising an access controller and a lock having a lock processor, wherein the access controller includes a memory for storing a reference access code, an input interface for allowing a user to input an access code; and a processor configured to receive inputs from the input interface and if the input access code matches the stored

reference access code, the processor is further configured to send a unique data to the lock processor to open the lock.

With the lock having a lock processor, the lock may be able to have more  
5 security and authentication functions built in by configuring the lock processor accordingly.

The unique data may be a digital sequence such as binary or hexadecimal formal. Of course, other formats are possible.

10

The lock system may further comprise an uninterruptible power supply (UPS).

In a fourth aspect of this invention, there is provided a method of determining access by an access controller, the access controller including a memory for  
15 storing a plurality of stored reference access codes, each reference access code being associated with different access levels which define restrictions as to when the associated reference access codes gain access, the method comprising receiving an input access code;  
comparing the input access code with the plurality of stored reference access  
20 codes and if there is match, checking the associated access level and if the associated restriction does not apply, allow access and if the associated restriction applies, refusing access.

- In a fifth aspect of the invention, there is provided an access controller comprising a memory for storing reference access codes with at least one reference access code having a validity period, an input interface for allowing a user to input an access code; a processor configured to receive inputs from the input interface and if the input access code matches the at least one reference access code and if the input access code is received within the validity period, configured to allow access but if beyond the validity period, configured to prevent access.
- 10 The access controller may further comprise a further reference access code having a different validity period, and upon expiry of the at least one reference access code, this further reference access code takes over as the active reference access code.
- 15 In a sixth aspect of the invention, there is provided a keypad comprising a plurality of buttons, each button comprising a transparent polycarbonate casing encasing Light Emitting Diode arrays for displaying numeric or alphanumeric symbols.
- 20 Instead of allowing access when a valid access code is received, the access controller according to the above mentioned aspects may be configured to prompt for a second access code so that access is allowed when two valid passwords are received.

## Brief Description of the Drawings

An embodiment of the invention will now be described, by way of example, with reference to the drawings in which:

5

Figure 1 is a perspective view of an access controller having a keypad, LCD display and a housing, according to a preferred embodiment of the present invention.

10 Figure 2 shows the keypad and LCD display of Figure 1 more clearly without showing the housing.

Figure 3 is a functional block diagram of a lock system including the access controller of Figure 1, shown as functional blocks, and a lock.

15

## Detailed Description of the Preferred Embodiment.

Figure 1 is a perspective view of an access controller 100 which comprises a front cover 102 and a base 104 cooperating to form a housing to enclose the other components of the access controller 100. In this embodiment, the access controller 100 is arranged to control unlocking of a lock 200 for a user to gain access to a door.

20

The access controller 100 also includes a keypad 106 with a plurality of keys 108 and a LCD display 110 (see Figure 2). Figure 3 is a functional block diagram of a lock system 10 comprising the access controller 100 and an uninterruptible power supply (UPS) 120 which is connected to a mains electrical supply. As it can be appreciated from Figure 3, the access controller 100 also includes a main processor 112, a timer 114, memory 116 and a sound buzzer 118. The access controller 100 also includes a "Reset" button 134 which is intended to reset the access controller 100 when, for example, there is a system hiccup. In this embodiment, activating the reset button 134 does not change preset passwords, dates and times. Further, the access controller 100 includes a communication port 136 for external control of the access controller 100. Most of these will now be described:

a) front cover 102 and base 104

The front cover 102 and base 104 are generally made of plastics material and the front cover 102 includes a transparent portion 102a which is generally rectangular in shape. The size and shape of the transparent portion 102a is adapted to match the LCD display 110 so that the display is visible through the transparent portion 102a. The display 110 is configured to display messages to guide the user. The front cover 102 also includes a plurality of polycarbonate buttons 102b, with the position of each button 102b arranged to correspond to the positions of each key 108 of the keypad 106 when the keypad is arranged within the housing formed by the front cover 102 and the base 104.

Each polycarbonate button 102b is transparent and resiliently depressible so that depressing it sends a signal to the main processor 112 indicating that it has been depressed.

5

b) Keypad 106

The keypad 106 comprises ten character keys 108, and five function keys. Each character key 108 is arranged to display a character such as a numerical value  
10 formed by an array of Light Emitting Diodes (LED). In this embodiment, the numerical value is arranged to display 0-9 with the five function buttons 124,126,128,130,132 displaying "Start", "Next", "Exit", "Cancel" and "Enter" respectively.

15 The keys may display the numerical values in fixed positions or rearranged every time before a password is input.

The "Start" key 124 is an initialization button. This button is pressed before entering any password.

20

The "Next" key 126 is used to bring up the next display on the LCD screen.

The "Exit" key 128 is used to leave the current display on the LCD screen 110 and return to the default display.

The "Cancel" key 130 is used to delete unwanted information in the memory, for example unwanted passwords, dates and/or times.

- 5     The "Enter" key 132 is mainly used to confirm an input password for access. In the settings menu, it is used to store all preset passwords, dates and timings into the system.

c) Main Processor 112

10

The main processor 112 controls the overall functions of the access controller 100. The main processor 112 is configured to receive input signals from the keypad 106, process the input signals and controls what the keys 108, timer 114, sound buzzer 118, LCD screen 110 or the lock 200 should do.

15

Depending on the mode, the main processor 112 is configured to generate a random array of numerical values to be displayed on the keys 108 via the Light Emitting Diode (LED) arrays. This will be further described later.

20

d) Timer 114

The timer 114 has calendar and time functions which feed the date and time information to the processor for display on the LCD screen 110. The timer 114 also includes an internal clock which is used by the processor 112 to keep track

of lapsed time. The timer 114 also plays a part for the main processor 112 to determine whether the password is valid or not. For example, the correct password during a wrong timeframe would indicate an invalid password and thus, the lock does not open.

5

e) Memory 116

The memory 116 stores a table of reference access codes or passwords which are accessible by the main processor 112. When the main processor 112  
10 receives input signals from the keypad 200, which represents an access code, the main processor 112 compares the access code with what is in the table and if a match is found, the access code is valid, and the processor 112 then proceeds with the next action, which may be to unlock the door.

In this embodiment, the memory stores four types of passwords with different  
15 access levels:

- i) Master Password (Top level): The access controller 100 is preprogrammed to store four master passwords which are active one at a time. Each of these master passwords has an activation and  
20 expiration date and when one expires, another new master password automatically becomes effective. There is no time and/or date restriction as to when the master password can be used. When the master password is received, the processor calls up a Settings Menu

on the LCD screen which list of options including allowing the user to open the lock 200.

- 5           ii)     Supervisor Password (2<sup>nd</sup> level): There are also four supervisor passwords stored in the memory 116. Just like the master passwords, each of these passwords has an activation and expiration date and when one expires, another new supervisor password automatically takes over as the active one. However, unlike the master passwords, the supervisor passwords have time restrictions, for example, during  
10           the active period, the passwords may be used only between a stipulated time slot, such as between 8am and 8pm. In this way, the supervisor password provides a different access level or security.
  
- 15           iii)     Staff Password (3<sup>rd</sup> level): The number and functions of the staff passwords are similar to the supervisor passwords. However, there are further restrictions to when the staff passwords may be used, for example, between 9am and 6pm, which means lesser flexibility than supervisor passwords. The purpose is to provide a different access  
20           level.
  
- iv)     One-time Only Password (4<sup>th</sup> level): The access controller 100 is preprogrammed with one such password and as the name implies, it is good for one use, after which it cannot be used again. A user may reprogram the one-time only password using an active master

password. This feature may be useful to enable a user to gain access only once, for example, in the case of external contractors.

It should be envisaged that the various passwords discussed above are  
5 exemplary only and other variations may be used depending on application. For example, the master passwords need not expire if no timing restrictions have been set. There can also be more than one master, supervisor or staff password active at any one time.

10 Having different access levels is particularly useful to assign these passwords to different users depending on their needs without the expense of security.

Further, since the timer 114 is equipped with the calendar function, the access controller 100 may be configured with different timing restrictions based on the  
15 day of the week or date. For example, those days designated as public holidays or weekends may have different timing restrictions depending on the access policy. For example, a password valid on a weekday between 9am and 5pm may be further restricted to be valid only between 9am and 1pm. This may be achieved without external software/hardware since all these may be  
20 preprogrammed using the settings menu, which is only accessible using the Master password.

The memory 116 is configured to record the last nine previously used passwords and data and time details which have been used to access the

access controller. This information may be read off the LCD screen using the Master password, and controlling a few of the function keys 124,126,128,130,132.

5        e) Sound Buzzer 118

The sound buzzer 118 is configured to generate a sound in response to a user's depression of one of the buttons 102b to acknowledge receipt of the input signals. It also gives a long beep after three wrong passwords have been  
10    entered to serve as a warning.

f) LCD Screen 110

The LCD screen 110 is used to display information to the user. For example, by  
15    default, the LCD screen displays the time and date and any other information that is needed to inform the user.

g) UPS 120

20    The access controller 110 also contains an UPS which provides back-up power to the access controller 110 and the lock 200 in case of power failure. This ensures that the access controller 110 and the lock 200 are still operational. In this embodiment, the UPS is able to power the access controller 110 and lock

200 for up to twelve hours but it should be appreciated that the length of time the UPS supports may be changed depending on application.

#### h) Lock 200

5

The lock 200 includes a lock processor 202 and a locking mechanism 204. The lock processor 202 is arranged to control the locking mechanism 204 which in turn locks or unlocks a door. The lock processor 202 is configured to receive a control signal from the main processor 112 and in the absence of such a control  
10 signal, the lock processor 202 does not send a signal to indicate to the locking mechanism 204 to unlock the door. Only when the control signal from the main processor 112 is received, then the lock processor 202 instructs the locking mechanism 204 to open the door.

15 The control signal from the main processor 112 may be a specific sequence of codes, such as binary digits, which are preprogrammed in the main processor 112. Having a specific sequence of codes is advantageous since this makes it more difficult for unauthorized entry.

20 An operation of the access controller 100 and the lock 200 will now be described.

If there is no activity on the keypad for a predetermined amount of time, the main processor 112 puts the access controller in standby mode which means

that the LEDs of the character keys 108 will be turned off. To begin, a user presses the "Start" button 124 and the keypad 106 sends a "start" signal to the main processor 112. The next step depends on which mode is being set up. If the access controller 100 is programmed as "fixed mode", the main processor  
5 112 lights up the array of LEDs with the numerical values displayed in a conventional arrangement each time the "Start" button 124 is pressed.

On the other hand, if the access controller is programmed as "scrambled mode", when the start button 124 is pressed, the main processor 112 scrambles the  
10 positions of each numerical value so that the relative positions of these numbers vary each time.

The user then proceeds to enter his or her password or access code. With each press of the buttons 102b, a corresponding signal is received by the main  
15 processor 112 which acknowledges by controlling the sound buzzer 118 to transmit an audible sound in response to each press.

Upon receipt of the input password, the main processor 112 checks the memory 116 to determine whether the input password matches what is in the memory  
20 table and which security level the password belongs to. If a match is found, this indicates a valid password.

If the password is a one-time use password, with no restrictions, the processor 112 then sends a unique binary sequence to the lock processor 202 and the

lock processor 202 then activates the lock mechanism 204 which unlocks the lock to the door. After this, the password cannot be used to gain entry again.

On the other hand, if the input password is a "Supervisor" or "Staff" password,  
5 the main processor 112 checks the timer to determine whether the time of receiving the input password falls within the restrictions (i.e. outside of the approved day/time) and if yes, the main processor 112 displays a message on the LCD screen 110 to inform the user that entry is refused. If the time of receiving the input password falls outside of the restrictions, then the main  
10 processor 112 similarly sends a code, for example a unique digital sequence to the lock processor 202 to open the door. The digital sequence may be in binary format.

The above describes the operation of what happens when the access controller  
15 100 is set up as a single password access. On the other hand, when the access controller 100 is configured a dual-password access, upon receiving the first input password and if the first input password is valid, the main processor 112 does not send the unique binary sequence but instead proceeds to invite the entry of a second input password by displaying a message on the LCD screen  
20 110. When the second input password is received, a similar procedure as that explained above takes place, and if the second input password is also valid, then the main processor 112 transmits the unique binary sequence to the lock processor 202 to open the lock.

After the door is unlocked, the processor 112 next sets the access controller 100 to the standby mode to conserve power. Likewise, if entry is refused for example because the input password is invalid, the processor 112 denies access and resets to the main screen. Thereafter, the standby mode is

5 activated after a certain elapsed time. To enter a password, the “Start” button is pressed and if the access controller is in “scrambled mode”, the positions of the numerical keys are scrambled randomly before being display on the keys 108.

It should be mentioned that for added security, after a key is pressed and  
10 thereafter there is no further pressing of the keys, the keypad is configured to enter into the standby mode after a certain time has elapsed. The standby mode turns off the LEDs of the keys 108 and backlight of the access controller. The dual-password access is useful in circumstances when there are two parties and either party wants to restrict access to the other party, unless both  
15 parties are present since both passwords must be entered to gain access.

The timer with the in-built electronic calendar is useful since the restrictions need not be limited to the time of a day but it can be extended to different days of the week. For example, a password may be valid from Mondays to Fridays  
20 but not on weekends to limit access to only authorized personnel. Similarly, if an person is employed on a temporary basis the password may be set to expire within a stipulated time period, for example after three months.

It should be appreciated that the lock processor 202 is configured to open the door upon receipt of the unique binary sequence and in the absence of receiving this unique binary sequence, the lock processor 202 does not send a signal to the lock mechanism 204 to unlock the door.

5

With the lock processor 202 and the unique binary sequence, this achieves a higher level of security. It is common for the access controller 100 and the lock 200 to be located at a distance between each other and both are communicatively connected via wires. With the lock processor 202, even if it is possible to gain access to the wires and cut them, it would not be possible to activate the lock mechanism 204 without knowledge of the unique binary sequence, thus resulting in a much more secured lock system. It should be appreciated that unique means that no two main processors (from different access controllers 100) generate the same binary sequence.

15

Having the fixed or scrambled mode, this makes the access controller more flexible since the user may choose which mode he prefers and depending on the security level. The use of the transparent polycarbonate buttons 102b also provides a durable material which reduces the chance of someone guessing what the password might be by checking the wear and tear of the buttons 102b even if the access controller is configured as the fixed mode. In the case of the scrambled mode, the positions of the character keys 108 are varied with each depression of the "Start" button and this provides a continuous and automatical

20

varying of the character keys 108. This reduces the ability of an unauthorized person obtaining the password by surveying a user's actions.

The access controller 100 is a fully integrated device with the ability to re-  
5 configure or re-program the functions through the use of the master password.  
If the processor 112 receives the master password, as mentioned earlier, the processor 112 displays the list of options for the user to choose. The options include opening the lock, changing the passwords of the different levels and storing new ones in the memory, changing the date and time of the timer, and  
10 choosing the modes and access types etc.

With the above features, it can be appreciated that the access controller 100 provides a more secure, reliable and yet flexible controller for the lock 200.  
Together with the lock 200, this forms a lock system which is also more secure  
15 and reduces unauthorized access.

The described embodiment should not be construed as limitative. For example, it is not necessary that there are four passwords stored in the memory 116 for the master, supervisor and staff passwords, and there may be up to the  
20 maximum of four or less. The UPS is preferred since this allows the access controller 100 and the lock 200 to be used even when there is a power failure but it should be appreciated that the UPS is not essential.

In the described embodiment, the sound buzzer 118 is used to provide aural feedback but this may not be necessary. Indeed, it is envisaged that the LCD screen may display a symbol such as an asterisk as an acknowledgement of the pressing of a button 102b. The timer 114 and memory 116 is shown as  
5 separate from the main processor 112 but it is envisaged that they may be incorporated within the main processor 112 as a single integrated circuit.

Instead of setting the access controller 100 to standby mode after each access, the main processor 112 may be configured to turn the character keys 108 off if  
10 no input is received by the keypad 106 for a predetermined amount of time.

Instead of polycarbonate buttons 102b, these buttons may be made with other material.

## CLAIMS

1. A method performed by an access controller having a memory storing reference access codes which includes a one-time use reference access code,  
5 the method comprising
  - (i) receiving an input access code by an input interface;
  - (ii) comparing the input access code to the one-time use reference access code stored in the memory by a processor,
  - (iii) if the input access code matches the one-time use reference access  
10 code stored in the memory, allowing access once and preventing subsequent access based on the same input access code.
2. A method according to claim 1, wherein  
the input interface comprises a plurality of keys configured to display  
15 every possible character to form the access code, and the method comprises changing the character that is displayed by each key.
3. A method according to claim 2, further comprising changing the  
character after a key is pressed on the input interface.  
20
4. A method according to 2 or 3, wherein the input interface includes a plurality of polycarbonate casing, with each casing arranged to cover a corresponding key.

5. A method according to any of claims 2 to 4, wherein the access controller comprises light elements arranged to form the characters carried by the keys.
- 5 6. A method according to claim 5, further comprising turning at least some of the light elements off if no input is received by the input interface for a predetermined amount of time.
7. A method according to claim 5, further comprising turning at least some  
10 of the light elements off after each access.
8. A method according to any preceding claim, further comprising acknowledging receipt of an input on the input interface.
- 15 9. A method according to claim 8, wherein the acknowledgement is performed by a sound buzzer.
10. A method performed by an access controller having a memory for storing a plurality of reference access codes, each reference access code  
20 associated with a different access level which define restrictions as to when the associated reference access codes gain access, the method comprising

- (i) receiving an input access code by an input interface;
  - (ii) comparing the input access code with the plurality of reference access codes stored in the memory by a processor,
  - (iii) if the input access code matches one of the stored reference access code, determining the access level of the input access code based on the plurality of reference access codes stored in the memory, and
  - (iv) if the associated restriction does not apply, allowing access by the access controller and if the associated restriction applies, refusing access by the access controller;
  - (v) wherein the access controller further comprises more than one reference access code for each type of access level, each reference access code having an expiry date, and at any one time, there is only one active reference access code for each type of access level which gains access, and the method further comprises
  - (vi) allowing access only to the active reference access code.
11. A method according to claim 10, wherein the restrictions are based on date and time.
12. A method according to claim 11, wherein the access controller further comprises a timer including an electronic calendar which provides the date and time.

13. A method according to any of claims 10 to 12, wherein upon expiry of one of the reference codes, another reference code becomes the active one.
- 5 14. A method according to any of claims 10 to 13, wherein there is a master access level and the reference access codes associated with the master access level is restriction free.
- 10 15. A method according to any of claims 10 to 14, wherein the input interface comprises a plurality of keys which is configured to display every possible character to form the access code, and the method includes changing the character that is displayed by each key.
- 15 16. A method according to claim 15, further comprising changing the character after depressing a key on the input interface.
17. A method performed by a lock system comprising an access controller having a memory for storing a reference access code, and a lock having a lock processor and a lock mechanism, the method comprising
- 20 (i) receiving an input access code by an input interface;
- (ii) comparing the input access code to the reference access code stored in the memory by a processor of the access controller, and

- (iii) if the input access code matches the stored reference access code stored in the memory, sending a unique data by the processor of the access controller to the lock processor of the lock, and
- (iv) only upon receipt of the unique data, unlocking the lock mechanism by the lock processor.
- 5
18. A method according to claim 17, wherein the unique data is a binary sequence.
- 10 19. A method according to claim 17 or 18, further comprising an uninterruptible power supply (UPS).
20. A method performed by an access controller having a memory for storing reference codes with at least one reference access code having a validity period, the method comprising
- 15 (i) receiving an input access code by an input interface;
- (ii) comparing the input access code to the at least one reference access code stored in the memory by a processor, and
- (iii) if the input access code matches the at least one reference access code and if the input access code is received within the validity period, allowing access;
- 20 (iv) but if beyond the validity period, preventing access,

(v) wherein the memory stores a further reference access code having a different validity period, and upon expiry of the at least one reference access code, this further reference access code takes over as the active reference access code automatically.

5

21. A method according to any of claims 12 to 16, wherein the restrictions are based on the day of the week.
22. A method according to claim 14, wherein weekends have a different  
10 restriction than weekdays.
23. A method according to any of claims 1 to 22, further comprising recording the last nine previously input access codes in the memory.
- 15 24. A method performed by an access controller having a memory for storing a plurality of reference access codes, each reference access code being associated with a different access level which define restrictions as to when the associated reference access codes gain access, the method comprising
- 20 (i) receiving an input access code from a user by an input interface;  
(ii) comparing the input access code to the plurality of reference access codes stored in the memory by a processor, and

- (iii) if a first input access code matches one of the stored reference access code, determining the access level of the first input access code based on the plurality of reference access codes stored in the memory and
- 5 (iv) if the associated restriction does not apply, prompting the user to input a second access code at the input interface, the second input access code having a different access level as the first access code, and
- (v) determining that the second access code matches one of the stored references access code by the processor, and
- 10 (vi) determining the restriction associated with the access level of the second input access code, and
- (vii) if the restriction does not apply, allowing access by the access controller.