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

(11) **EP 1 818 874 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
15.08.2007 Bulletin 2007/33

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

(21) Application number: **06121858.2**

(22) Date of filing: **05.10.2006**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK YU

(30) Priority: **05.10.2005 GB 0520160**

(71) Applicant: **Insafe International Limited**
TN4 9NZ Kent, Tunbridge Wells (GB)

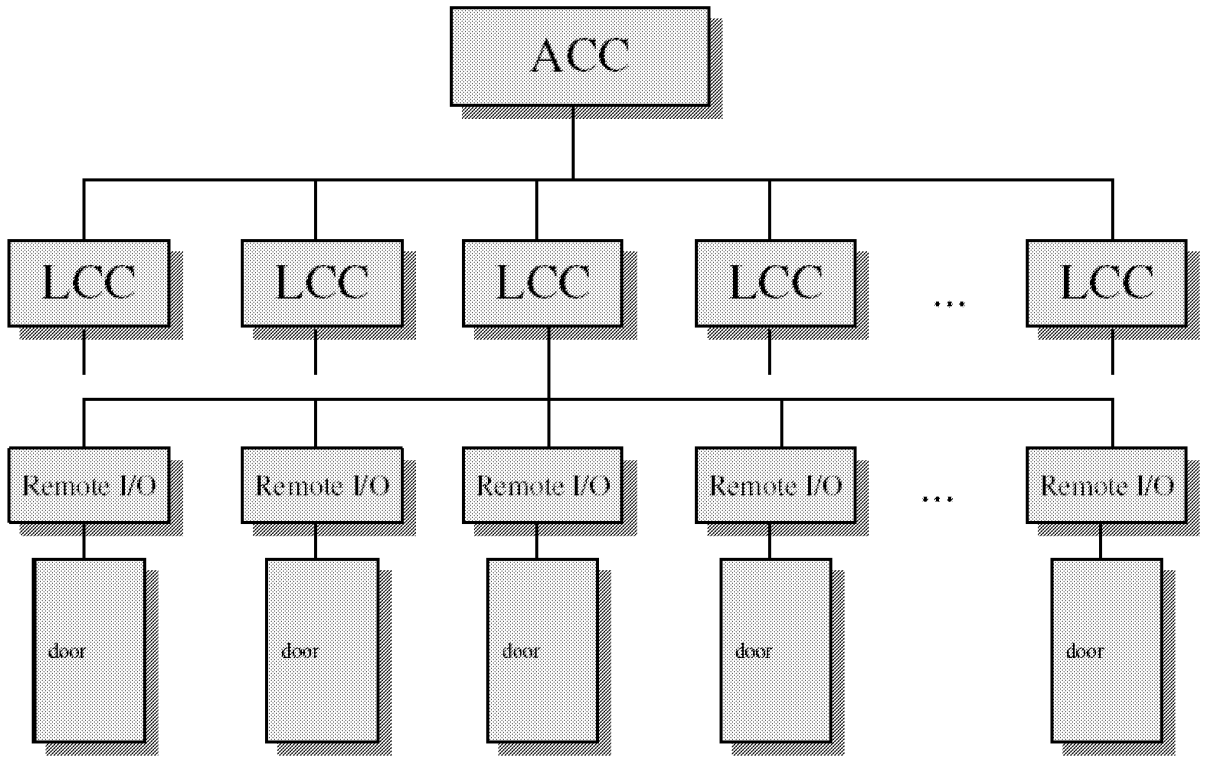
(72) Inventors:
- **Bullock, Alan**
  Tunbridge Wells, Kent TN4 9NZ (GB)
- **Cripps, Michael**
  Tunbridge Wells, Kent TN4 9NZ (GB)
- **Nellen, Stefan**
  Tunbridge Wells, Kent TN4 9NZ (GB)
- **Easterling, Clare**
  Tunbridge Wells, Kent TN4 9NZ (GB)
- **Marsden, Philip**
  Tunbridge Wells, Kent TN4 9NZ (GB)

(74) Representative: **Bailey, David Martin**
Brookes Batchellor LLP,
102-108 Clerkenwell Road
London EC1M 5SA (GB)

(54) **Remote monitoring system for a security lock**

(57) A remote control, monitoring and recording system for a security system to remove control from the site of the door to an off-site location, and to help prevent unauthorised access to a safe or vault.

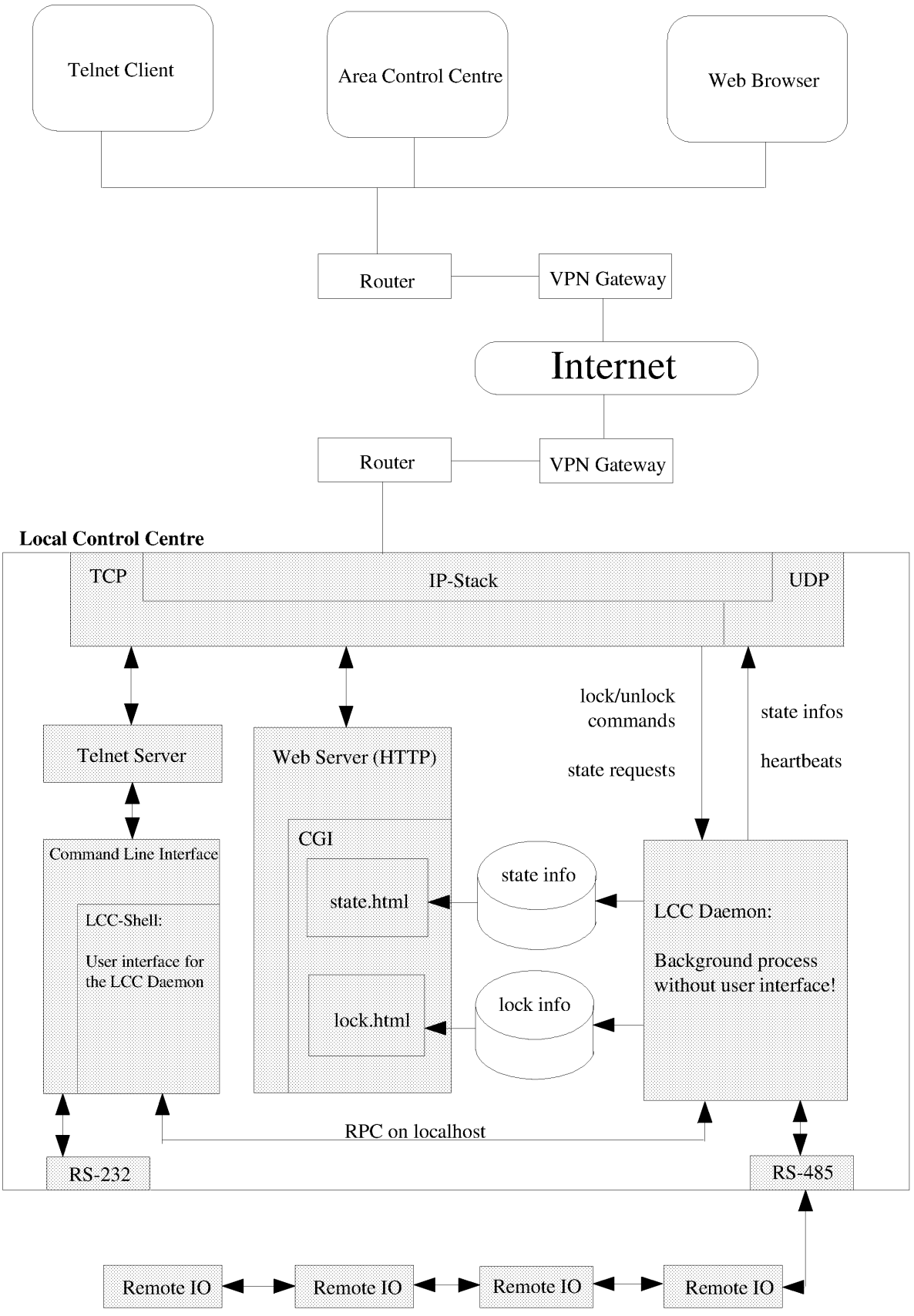
Figure 1a



EP 1 818 874 A1

(Cont. next page)

Figure 1b


Telnet Client
Area Control Centre
Web Browser
Router
VPN Gateway
Internet
Router
VPN Gateway
Local Control Centre
TCP
IP-Stack
UDP
lock/unlock commands
state requests
state infos
heartbeats
Telnet Server
Web Server (HTTP)
CGI
Command Line Interface
LCC-Shell:
User interface for the LCC Daemon
state.html
state info
LCC Daemon:
Background process without user interface!
lock.html
lock info
RPC on localhost
RS-232
RS-485
Remote IO
Remote IO
Remote IO
Remote IO

Description

[0001] The present invention relates to a remote control, monitoring and recording system for electronic locks, and in particular electronic combination locks.

[0002] It is commonly known to provide a number of devices such as keylocks, mechanical combination locks and digital electronic locks for use in securing vault and safe doors.

[0003] Keylocks and mechanical combination locks are considered to be "single user" locks i.e. only a single key or code is available to open the lock and therefore only one person is required to operate it. Such systems are not considered to be particularly secure and require frequent replacement of the lock or changes to the code to prevent unauthorised access. To overcome this problem, two keylocks are typically fitted, such that two people, or one member from each of two groups, are required to open a door which is protected in such a manner. Additionally keylocks can be added to enhance security further. This may result in a number of people having a key or combination code.

[0004] Another problem associated with keylocks and mechanical combination locks is that they are not auditable. That is to say, there is no automatic record or history of lock operation. Therefore, in such systems it is impossible to track who is opening or has opened the lock, at what time the opening occurred and for what length of time the lock remained open. This presents a considerable security risk.

[0005] Digital electronic locks generally have the capacity for handling multiple codes so that a number of different users can each be a code holder, each having their own unique code. Whenever a code is input, the lock is accessed, closed or reset, or the combination is changed an 'event' noting the specific function, time and personal access code used, along with other possibilities, may be recorded in the lock memory. As a result, these events are capable of being audited. However, auditing can only be used to monitor events retrospectively and requires a printer or laptop computer to be physically plugged into the lock to provide a record of the event history. Typically, only the last few hundred events may be recorded. Therefore, when the memory capacity of the lock has been reached, the oldest event will be lost each time a new event is recorded.

[0006] A feature of the aforementioned locking systems is that it is possible for the key or code holders to open the lock(s) even if a breach of security, such as a hold-up or hostage situation, occurs. Under such circumstances, under threats of physical harm the vault or safe can be opened by entry of a slightly different "duress" version of the normal multidigit access code, whereupon a secret alarm signal is transmitted to a remote station, alerting to the forced entry condition. If such a situation occurs, the vault or safe door will still open.

[0007] A problem associated with conventional locking systems is that they are locally controlled and, for convenience, to avoid having to unlock and relock the doors frequently, users often tend to leave the doors open and unmonitored for long periods. An additional problem is that there is no accountability for keys, codes and operation.

[0008] In highly sensitive security environments, it is desirable to be able to monitor the status of combination locks, specifically electronic combination locks, from a remotely located central monitoring station. In order to control access to the lock and to control and restrict entry to the safe or vault, it is desirable to remotely monitor the lock status i.e. whether it is in an open, closed or locked state. It is also desirable to monitor and authorise or prevent access to, and the use of, an input pad, keypad or dial for gaining access to the vault/safe. It is further desirable to control any modification of the lock access codes.

[0009] If an authorised individual with an authorised combination has uncontrolled access to the lock, it is possible for that individual to open the lock, re-set the combination, and close the lock without any control or supervision. Furthermore, it might be possible for the unauthorised operator to change the combination. However, it is desired that the lock is conditioned to allow only a change of the combination when authorisation of any such change is received from the remotely located central Area Control Centre (AAC), prior to any actual alteration taking place. However, it is preferable that the changes to the lock combination are directly implemented from the ACC itself. Through monitoring the operation and status of the lock remote from the site of installation, it is possible to take necessary action when unauthorised persons attempt to breach the lock security. Accordingly, monitoring of the system would allow security personnel located in the ACC to respond appropriately should the monitoring system indicate that the lock is being operated at an unexpected time or under unexpected circumstances.

[0010] The present invention seeks to overcome at least some of these problems and provide a remote control, monitoring and recording system to remove control from the site of the door to an off-site location, creating a break in the chain of operation. Such a break creates an added level or layer of security to help prevent unauthorised access to a safe or vault. All users of the security system including those operating the safe door and those monitoring the system and the operators at the Area Control Centre will have individual codes and will therefore be accountable, and their actions auditable.

[0011] An advantage of the system according to the present invention is that there is no requirement for significant modification of existing lock hardware as standard interfaces can be used. Therefore, the present system can be used in conjunction with existing security arrangements and hardware systems. A further feature of the present system is that control and monitoring of multiple secure doors at a single site can be achieved through a single local control centre (LCC), and that several thou-

sand LCCs can be controlled and monitored by a single ACC. For example, at the present state of technology the described system will have the capacity to control and monitor up to 127 doors per LCC; 4,294,967,296 LCCs per ACC; and therefore 545,460,846,592 doors at the same time. However, in practice a typical system is likely to have a maximum of around 20 doors per LCC and around 200 LCCs per ACC. Since the system utilises modern Internet Protocol (IP) network communication, the control and monitoring of doors around the whole world can be achieved. In the event that connection is lost between an LCC and the ACC the system defaults to "shut-down" mode. If connection is lost whilst the vault is open a timeout will disable all pending authorisations automatically. The LCC will then buffer all events into its internal log files, and after connection is re-established these data will be automatically synchronized.

[0012] In accordance with a first aspect of the invention, there is provided an apparatus for remotely controlling, monitoring and recording access to an electronic lock system, wherein the apparatus comprises:

(i) an electronic lock for a safe or vault door, the electronic lock comprising a lock enable/disable unit, a power supply and ground signal;
(ii) a plurality of electrical conductors;
(iii) at least one remote input/output (I/O) module connectable to the safe or vault door and having a power supply and ground signal;
(iv) a Local Control Centre comprising an embedded computer implementing a monitoring program, a power supply and ground signal; and
(v) an Area Control Centre comprising a computer monitoring system and a connection to said Local Control Centre,

wherein the lock enable/disable unit comprises a driving means, controlled by a microprocessor, and an electronic motor-bolt lock including a redundant power bolt drive, the bolt having an extended first position and a second withdrawn position, movable therebetween by the driving means; and wherein the input/output module is connected to the lock by the plurality of electrical conductors, said plurality of electrical conductors comprising at least three microswitches to monitor the status of the lock and door, and at least two electrical conductors connecting said input/output module to the lock enable/disable unit; the input/output module is further connected to the embedded computer of the Local Control Centre by an isolated differential signalling integrated circuit and the Local Control Centre is linked to the Area Control Centre through either Internet Protocol tunnelling via an intranet or an internet connection.

[0013] According to a second aspect of the invention there is provided an apparatus for remotely controlling, monitoring and recording access to an electronic lock system, wherein the apparatus comprises:

(i) an electronic lock for a safe or vault door, the electronic lock comprising a lock enable/disable unit, a power supply and ground signal;
(ii) a plurality of electrical conductors;
(iii) at least one remote input/output (I/O) module connectable to the safe or vault door and having a power supply and ground signal; and
(iv) an Area Control Centre comprising a computer monitoring system,

wherein the at least one remote I/O module further comprises a microcomputer and network stack and a connection to the Area Control Centre, and in which the lock enable/disable unit comprises a driving means, controlled by a microprocessor, and an electronic motor-bolt lock including a redundant power bolt drive, the bolt having an extended first position and a second withdrawn position, movable therebetween by the driving means; and wherein the input/output module is connected to the lock by the plurality of electrical conductors, said plurality of electrical conductors comprising at least three microswitches to monitor the status of the lock and door, and at least two electrical conductors connecting said input/output module to the lock enable/disable unit; the input/output module is further connected to the embedded computer of the Local Control Centre by an isolated differential signaling integrated circuit and the Local Control Centre is linked to the Area Control Centre through either Internet Protocol tunneling via an intranet or an internet connection.

[0014] This arrangement may be preferable in systems in which only a single door requires remote monitoring as it requires that every vault door has its own Ethernet or network connection.

[0015] Suitably, the Internet Protocol tunnelling via an intranet is over an Ethernet.

[0016] Suitably, the safe or vault door comprises a second input/output module for internal event-logging in the lock.

[0017] Preferably, the apparatus comprises a heartbeat for system monitoring which periodically surveys all connected I/O modules. Preferably, the remote I/O modules automatically switch to a default state in which authorisation is disabled in the event that the system heartbeat fails.

[0018] Suitably, the apparatus comprises a watchdog mechanism. Preferably, the watchdog mechanism comprises a hardware timer that is continually updated and reset whilst the operating system is running normally, and in which the operating system is rebooted and the event logged in response to a system failure in which the operating system is unable to reset the timer. Suitably, the system must be reconfigured before the system hardware and watchdog mechanism can be re-enabled in the event that an attempt is made to disable the watchdog mechanism. Suitably, the LCC hardware comprises an integrated watchdog mechanism.

[0019] In accordance with a third aspect of the inven-

tion, there is provided a method for remotely controlling, monitoring and recording access to an electronic lock system, as described above, wherein the method comprises:

(i) contacting the area control office to request activation of the lock keypad, in which a contact is established by an onsite authorised user;
(ii) identification of the authorised user by an operator at the area control centre;
(iii) enabling of the keypad by the operator for input of an authorised user can input his access code;
(iv) inputting of an authorised user access code;
(v) retracting the boltwork for the door if the access code is correct,
(vi) opening the lock;
(vii) disabling the lock keypad automatically after a predetermined time or by an operator at the ACC;
(viii) sending an alerting signal to the ACC if there is any activity at the door subsequent to stop (vii); and
(ix) sounding an alarm if the doors are left open for too long.

[0020] Preferably, the authorised user is identified by closed circuit television.

[0021] Suitably, the system defaults to a shut-down mode in the event that connection is lost between an LCC and the ACC. Preferably, a timeout will disable all pending automatically authorisations if connection is lost whilst the vault or safe door is open. Preferably, the LCC buffers all events into an internal log files, and upon reconnection these data are automatically synchronized.

[0022] The present invention also provides a safe and a vault door comprising an apparatus as described above.

[0023] The above and other aspects of the present invention will now be illustrated in further detail, by way of example only, with reference to the accompanying drawings in which:

Figure 1a is a system structure overview of an embodiment of the present invention;

Figure 1b is an alternative system structure overview of an embodiment of the present invention;

Figure 2 is a detailed schematic representation of the vault door connections of Figure 1;

Figure 3 is a detailed schematic representation of connections to a remote input/output module of Figure 1;

Figure 4 is a detailed schematic representation of the connections associated with a Local Control Centre of the embodiment of Figure 1;

Figure 5 illustrates an RS485 Bus which links a plurality of remote I/O modules to a Local Control Centre according to the embodiment of Figure 1;

Figure 6 is an information flow diagram from the remote control centre to the electronic lock;

Figure 7 is a logic control flow diagram of the "heartbeat function" between a Local Control Centre and the remote Area Control Centre;

Figure 8 is a logic control flow diagram of the "heartbeat function" between a Local Control Centre and a remote input/output module;

Figure 9 is a logic control flow diagram for the "watchdog mechanism"; and

Figure 10 is a logic control flow diagram between a Local Control Centre and a remote input/output module.

[0024] Referring to Figure 1a, an overview of a security system according to the present invention is illustrated in which the system comprises four levels of security. The first layer, as illustrated in greater detail in Figure 2, comprises a vault door fitted with a digital electronic lock and a series of microswitches for monitoring the door and lock positioning and status. The digital lock has a conventional audit facility which is used to monitor the lock activity. Standard interfaces are used which enable the present system to be implemented alongside existing security systems, and also used in relation to a wide variety different digital electronic lock systems. The microswitches and a Ground Signal link the first layer to the second layer.

[0025] Figure 1b, is an alternative overview of a security system according to the present invention (doors are omitted for clarity) in which the Local Control Centre of Figure 1 (LCC), discussed below in relation to Figure 4, and alternative monitoring and control means in the form of a Telnet Client or internet web browser may be used for management of the security system.

[0026] The second layer as shown in Figure 3, comprises a remote input/output (I/O) module located within the vault or the vault door itself. Each module is connected to a single door and connection is made through six wires linked to the microswitches and two additional wires for enabling/disabling the lock by a relay (from the first layer). Two further wires link the module to a DC power supply. Additionally, in instances where internal event logging of the lock itself is required, a second remote input/output module with a single serial interface is also fitted. All information concerning events and hardware status from the locks and microswitches pass through the dedicated I/O module and is sent to the Local Control Centre of the third security layer.

[0027] Figure 4 illustrates the third layer of security and comprises the Local Control Centre (LCC). The LCC is connected to each I/O module through an isolated differential signaling integrated circuit such as a duplex RS485 bus, and can be linked up to a maximum of 255 doors and I/O modules. However, when online logging is used this figure is cut to 127 because remote serial input modules utilise the other half of the address range. Only one LCC is required for each particular site and this collects all data concerning events occurring at the doors from all connected remote I/O modules.

[0028] Connection of multiple I/O modules to a LCC is through a RS485 Bus and is illustrated in Figure 5. In the RS485 bus each signal uses one twisted-pair (TP) line which comprises two wires twisted around themselves. The RS485 bus is ideally suited for multipoint communications, in which many devices may be connected to a single signal cable, akin to an Ethernet network, and the balanced differential signal transmission of this system is less prone to interference, compared with other similar systems. Such a system has a transfer rate of around 2.5 MB/s system and allows a cable length of up to 1200 meters to be used.

[0029] Most RS485 systems use Master/Slave architecture, in which each slave unit has a unique address and only responds to information packets or telegrams addressed to the particular slave unit. These packets may also include a system heartbeat for system monitoring and are generated by the Master (e.g. LCC), which periodically surveys all connected slave units (e.g. I/O modules). If the system heartbeat fails, the remote I/O modules automatically switch to their default state in which authorisation is disabled.

[0030] As indicated above, the status of each bolt system/lock is monitored by the LCC through a number of microswitches which continually report their status through the system heartbeat. Every vault door is connected to at least one remote I/O module for processing digital inputs and outputs received from microswitches located on the door. The inputs are decoupled and driven by a 24V voltage. The outputs are connected by a Type A relay i.e. not opened as in a standard operation. If online-logging is used, a second remote I/O module is required and is connected to the serial line of the vault door's option box. This enables the remote I/O modules to communicate with the LCC via a double-wired standard bus, such as an ISO 8462 or Electronics Industry Association (EIA) RS485 bus. The LCC is hosted by an embedded ucLinux system, although it will also be recognized that other systems, such as standard UNIX systems and the Microsoft Windows product family could be used. The data collected from the microswitches is then reported to the ACC and subsequently used to update and monitor the LCC status.

[0031] The fourth and final layer of the security system, as seen in the hierarchy of Figure 1, is the Area Control Centre (ACC). This is a centrally manned operations office, located at an independent site, and comprises a computer network linked to all contracting LCCs by an Ethernet link (TCP/IP protocol) to monitor all LCC activity. The system also utilises a standard internet connection as a back-up in case of an Ethernet failure. A local or national security firm will typically operate the ACC, although the described system is also capable of operating on an international scale.

[0032] In Figure 6 the information flow from the operator in a remote central area control centre down to the vault door of the branch and vice versa is shown. In this process, the operator enables (or disables) the lock of the vault door within a graphical user interface (GUI). The GUI then sends this command to the ACC, which then repeats the command to the LCC within its heartbeat telegram (discussed below in relation to Figure 7). Upon receiving this command the LCC updates the output of the remote I/O module to enable or disable authorisation of the lock. The status of the I/O module is then updated and the LCC reads all input and output settings of the I/O module to retrieve the status of the lock bolts and authorisation system. At the same time the online logging of the lock system is read to check for any discrepancies such as incorrect code input or failures etc. This status information is then relayed to the ACC through the system heartbeat and the ACC records are updated, and the information displayed on the GUI for viewing by the operator.

[0033] Figure 7 illustrates the communication principle between the remote Area Control Centre and a Local Control Centre that is locally embedded in the vault or vault door, with communication being conducted using a standard User Datagram Protocol (UDP) over an internet protocol (IP). The internet protocol provides for transmitting blocks of data called datagrams or telegrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long telegrams, if necessary, for transmission through "small packet" networks. The present system provides a heartbeat that is periodically sent from the ACC to constantly update the system status. The heartbeat works by sending out a telegram from the ACC, which is picked up by the various components of the system which then return or echo the heartbeat back to the ACC. All telegrams are packed within a single UDP packet. If this link between ACC and LCC is interrupted either because a response to the heartbeat fails to be received or responded to, or if the operator has forgotten to disable a code authorisation at the on-site door, the LCC will disable the authorisation automatically and will not allow access to the system until the heartbeat monitoring system registers a normal system status.

[0034] Communication between the LCC and remote input/output (I/O) modules is also guarded by the above described heartbeat mechanism, as illustrated in Figure 8.

[0035] In addition to the heartbeat monitoring system, the LCC hardware has an integrated "watchdog mecha-

nism". The watchdog mechanism is a hardware timer that is continually updated and reset as long as the operating system is running normally. If the system fails to do this and hangs, the operating system is no longer able to reset the timer. As a result, the timer will expire which results in an automatic externally initiated reset in which the operating system is rebooted, with the debug information being displayed on a system console at the ACC (Figure 9). The hardware watchdog mechanism is enabled by default. If an attempt is made to disable the watchdog mechanism, the system must be configured before the system hardware and watchdog mechanism can be re-enabled. The hardware watchdog mechanism also serves as an initial safeguard against system hacking.

[0036] Figure 10 illustrates the communication cycle within the LCC link to all connected remote input/output modules.

[0037] In use, before a lock of a vault door can be opened it is necessary for a code input keypad at the site of the door to be activated, since the input pad is disabled by default. To enable the keypad the authorised users must contact an operator at the ACC to request the enabling of the lock input keypad. The operator at the ACC will activate a window on their display screen which will show the particular site details, including the last ~ 0 to 20 events on the door (although the system will record many more events) and the enable/disable buttons. Closed circuit television (CCTV), or other suitable identification means is then used to identify the authorised users and if the operator at the ACC is happy that the users are not under duress, the input pad is enabled. If the operator at the ACC is not happy with the situation at the door, depending upon the circumstance, they have the option to either enable the lock and contact the police (in cases of duress) or not to enable the lock if, for instance, an authorised user is acting suspiciously.

[0038] In a situation where the user incorrectly inputs a code in the keypad, the online-logging reports this event to the LCC. The LCC, in turn, forwards this information to the ACC for event-logging and also for display on the graphical user interface.

[0039] In the event the wires to the remote I/O modules are cut, the remote I/O modules automatically switch to their default state in which authorisation is disabled. The same effect results if the power line is cut.

[0040] As described above, the ACC generates a heartbeat that is transmitted throughout the system. This constantly monitors the system and reports events to the ACC for logging and also the occurrence of any faults in the system.

[0041] As the authorised users enter their codes into the lock an audit signal will be sent from the site to the ACC showing exactly who is entering their code and when the code is entered.

[0042] Once the locks have been opened it will be possible to retract the boltwork of the door. This operation will be reported to and recorded automatically by the monitoring computer at the ACC.

[0043] After a predetermined interval, for example 10 minutes, the lock input keypad will be automatically disabled.

[0044] The constantly monitored system will detect and report any activity at the door to the ACC where it will be recorded and viewed by the operator.

[0045] If doors are left open beyond a pre-determined period, an alarm will sound at the ACC and the relevant indication on the main display will flash. The operator will then be able to contact on-site security regarding the problem.

[0046] By providing an electronic combination lock, in addition to electronic I/O modules, microswitches may be attached to the electronic portion of the lock and subsequently connected to a Local Control Centre. The lock may also be modified to add circuits which provide signals to the Area Control Centre that will be interpreted to indicate the condition or status of the lock at all times. Other microswitches connected to the electrical system of the lock can provide signals to indicate other status conditions for various components of the lock. In addition, a position detector will be installed within the lock housing to monitor and indicate the position of the lock bolt to the LCC/ACC.

Claims

1. An apparatus for remotely controlling, monitoring and recording access to an electronic lock system, wherein the apparatus comprises:

(i) an electronic lock for a safe or vault door, the electronic lock comprising a lock enable/disable unit, a power supply and ground signal;
(ii) a plurality of electrical conductors;
(iii) at least one remote input/output (I/O) module connectable to the safe or vault door and having a power supply and ground signal;
(iv) a Local Control Centre comprising an embedded computer implementing a monitoring program, a power supply and ground signal; and
(v) an Area Control Centre comprising a computer monitoring system and a connection to said Local Control Centre,

wherein the lock enable/disable unit comprises a driving means, controlled by a microprocessor, and an electronic motor-bolt lock including a redundant power bolt drive, the bolt having an extended first position and a second withdrawn position, movable therebetween by the driving means; and wherein the input/output module is connected to the lock by the plurality of electrical conductors, said plurality of electrical conductors comprising at least three microswitches to monitor the status of the lock and door, and at least two electrical conductors connecting said input/output module to the lock enable/dis-

able unit; the input/output module is further connected to the embedded computer of the Local Control Centre by an isolated differential signalling integrated circuit and the Local Control Centre is linked to the Area Control Centre through either Internet Protocol tunnelling via an intranet or an internet connection.

2. An apparatus for remotely controlling, monitoring and recording access to an electronic lock system, wherein the apparatus comprises:

(i) an electronic lock for a safe or vault door, the electronic lock comprising a lock enable/disable unit, a power supply and ground signal;
(ii) a plurality of electrical conductors;
(iii) at least one remote input/output (I/O) module connectable to the safe or vault door and having a power supply and ground signal; and
(iv) an Area Control Centre comprising a computer monitoring system,

wherein the at least one remote IO module further comprises a microcomputer and network stack and a connection to the Area Control Centre, and in which the lock enable/disable unit comprises a driving means, controlled by a microprocessor, and an electronic motor-bolt lock including a redundant power bolt drive, the bolt having an extended first position and a second withdrawn position, movable therebetween by the driving means; and wherein the input/output module is connected to the lock by the plurality of electrical conductors, said plurality of electrical conductors comprising at least three micro switches to monitor the status of the lock and door, and at least two electrical conductors connecting said input/output module to the lock enable/disable unit; the input/output module is further connected to the embedded computer of the Local Control Centre by an isolated differential signalling integrated circuit and the Local Control Centre is linked to the Area Control Centre through either Internet Protocol tunnelling via an intranet or an internet connection.

3. An apparatus as claimed in Claim 1 or Claim 2 further comprising a second input/output module.

4. An apparatus as claimed in any one of claims 1 to 3 wherein the system comprises a heartbeat for system monitoring which periodically surveys all connected I/O modules).

5. An apparatus as claimed in Claim 4 in which the remote I/O modules automatically switch to a default state in which authorization is disabled in the event that the system heartbeat fails.

6. An apparatus as claimed in any one of claims 1 to 5 in which the apparatus further comprises a watchdog mechanism.

7. An apparatus as claimed in Claim 6 in which the watchdog mechanism comprises a hardware timer that is continually updated and reset whilst the operating system is running normally, and in which the operating system is rebooted and the event logged in response to a system failure in which the operating system is unable to reset the timer.

8. An apparatus as claimed in Claim 7 in which the operating system must be reconfigured before the system hardware and watchdog mechanism can be re-enabled in the event that an attempt is made to disable the watchdog mechanism.

9. An apparatus as claimed in any one of claims 6 to 8 in which the LCC hardware comprises an integrated watchdog mechanism.

10. An apparatus as claimed in one of claims 1 to 10 in which the Internet Protocol tunnelling via an intranet is over an Ethernet.

11. A method for remotely controlling, monitoring and recording access to an electronic lock system, wherein the method comprises:

(i) contacting the area control office to request activation of a keypad for operating the lock, in which a contact is established by an onsite authorised user;
(ii) identification of the authorised user by an operator at an area control centre;
(iii) enabling of the keypad by the operator for input of an authorised user access code;
(iv) inputting of an authorised user access code;
(v) retracting the boltwork for the door when a correct authorised access code has been input,
(vi) opening the lock;
(vii) disabling the lock keypad automatically after a predetermined time or in response to an instruction by an operator at the ACC;
(viii) sending an alerting signal to the ACC if there is any activity at the door subsequent to stop (vii); and
(ix) sounding an alarm if the doors are left open for too long.

12. A method as claimed in Claim 11 in which the authorised user is identified by closed circuit television, prior to enablement of the keypad.

13. A method as claimed in Claim 11 or Claim 12 in which the system defaults to a shut-down mode in the event that connection is lost between an LCC and the ACC.

14. A method as claimed in Claim 13 wherein a timeout will disable all pending automatically authorizations if connection is lost whilst the vault or safe door is open.

15. A method as claimed in Claim 14 in which the LCC buffers all events into an internal log files, and upon re-connection these data are automatically synchronized.

16. A safe or a vault door comprising a mechanism as claimed in any one of claims 1 to 10.

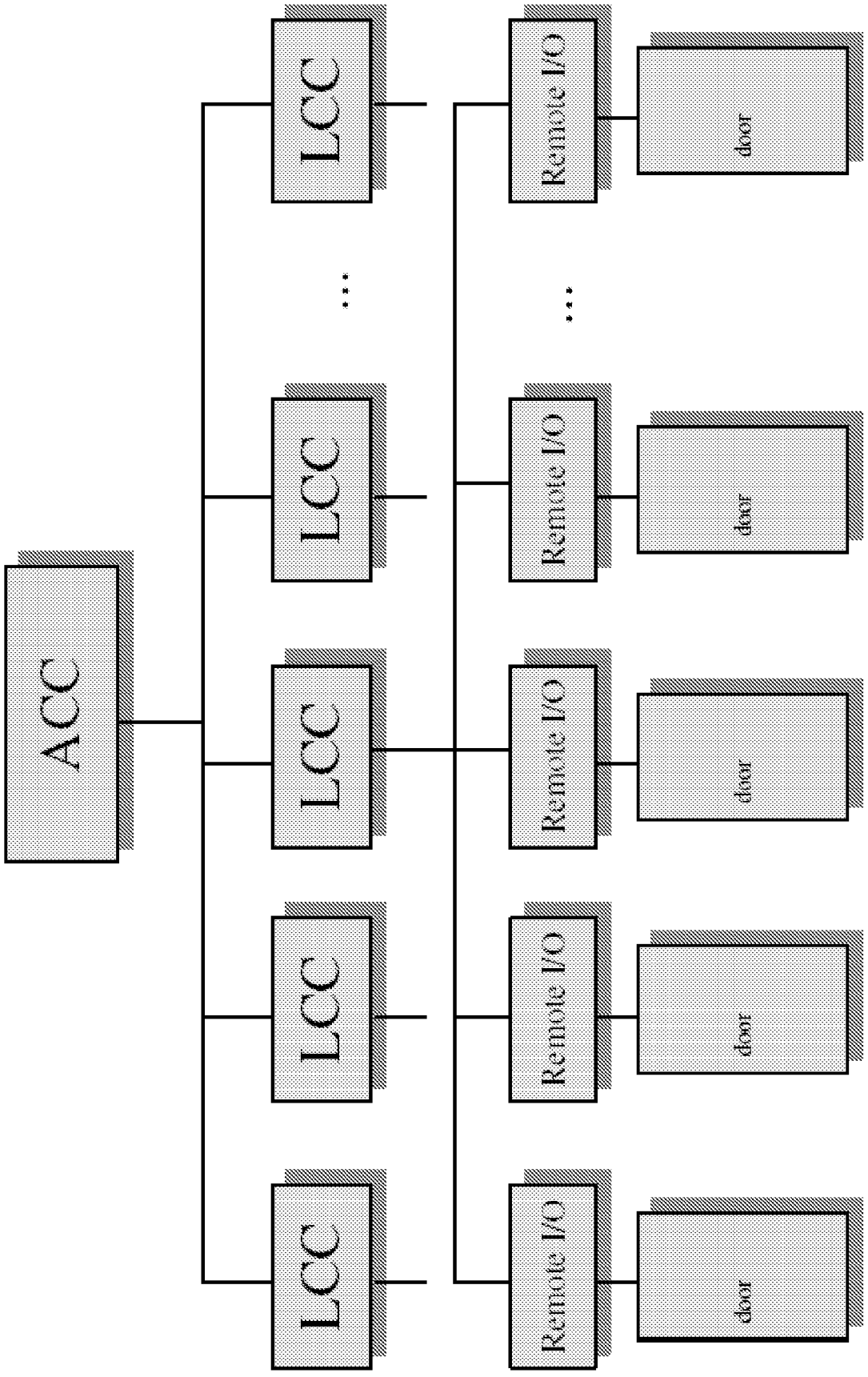

ACC
LCC
LCC
LCC
LCC
LCC
Remote I/O
Remote I/O
Remote I/O
Remote I/O
door
door
door
door

Figure 1a

Figure 1b

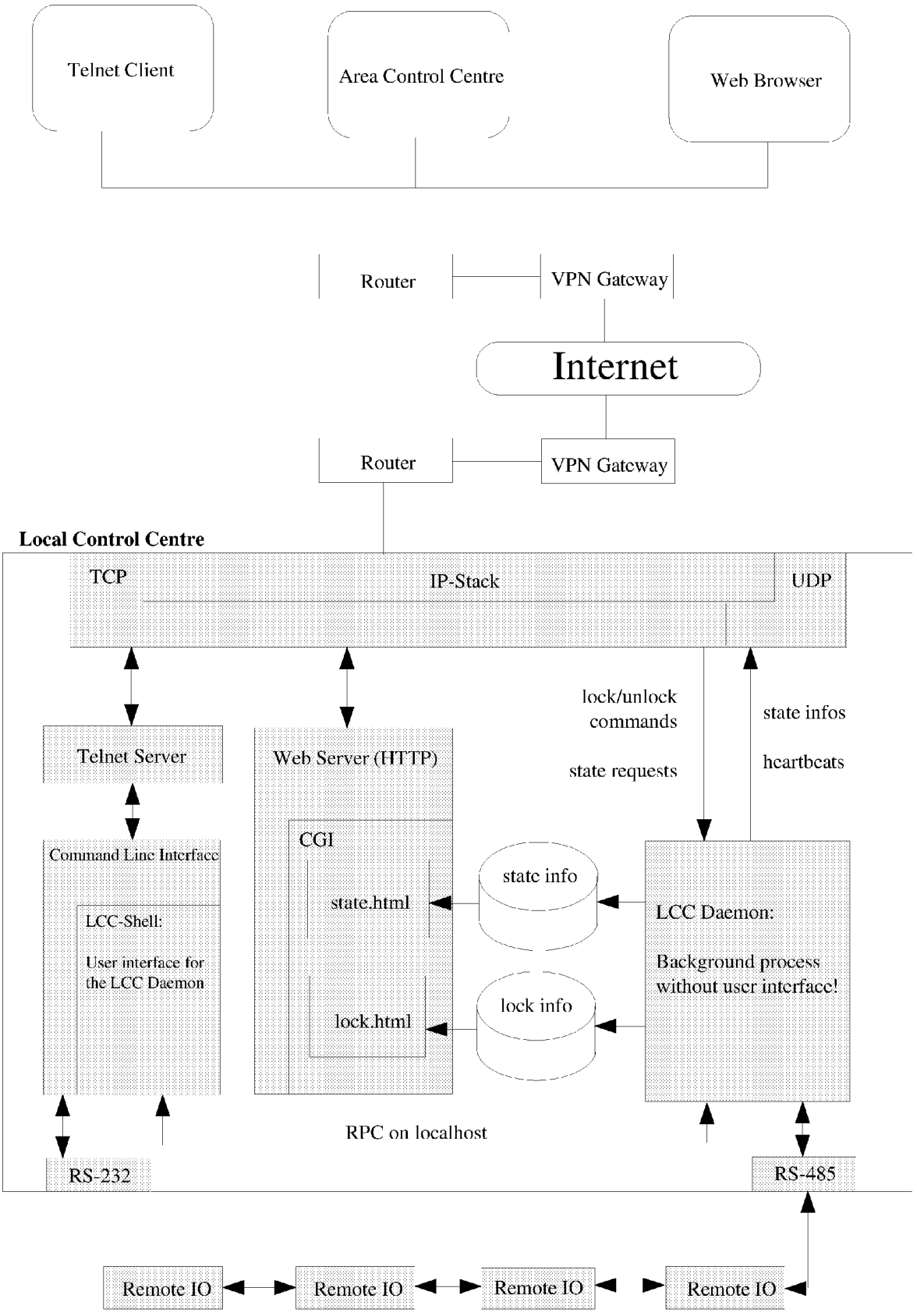

Telnet Client
Area Control Centre
Web Browser
Router
VPN Gateway
Internet
Router
VPN Gateway
Local Control Centre
TCP
IP-Stack
UDP
lock/unlock commands
state requests
state infos
heartbeats
Telnet Server
Web Server (HTTP)
CGI
Command Line Interface
LCC-Shell:
User interface for the LCC Daemon
state.html
lock.html
state info
lock info
LCC Daemon:
Background process without user interface!
RPC on localhost
RS-232
RS-485
Remote IO
Remote IO
Remote IO
Remote IO

Figure 2

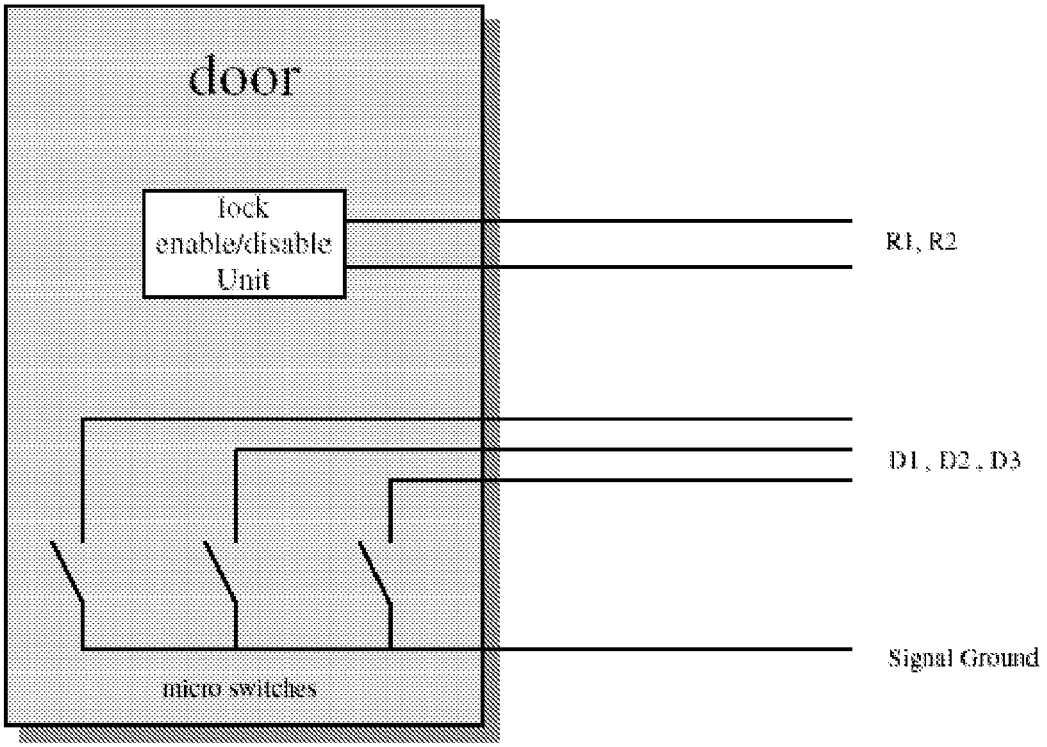


Figure 3

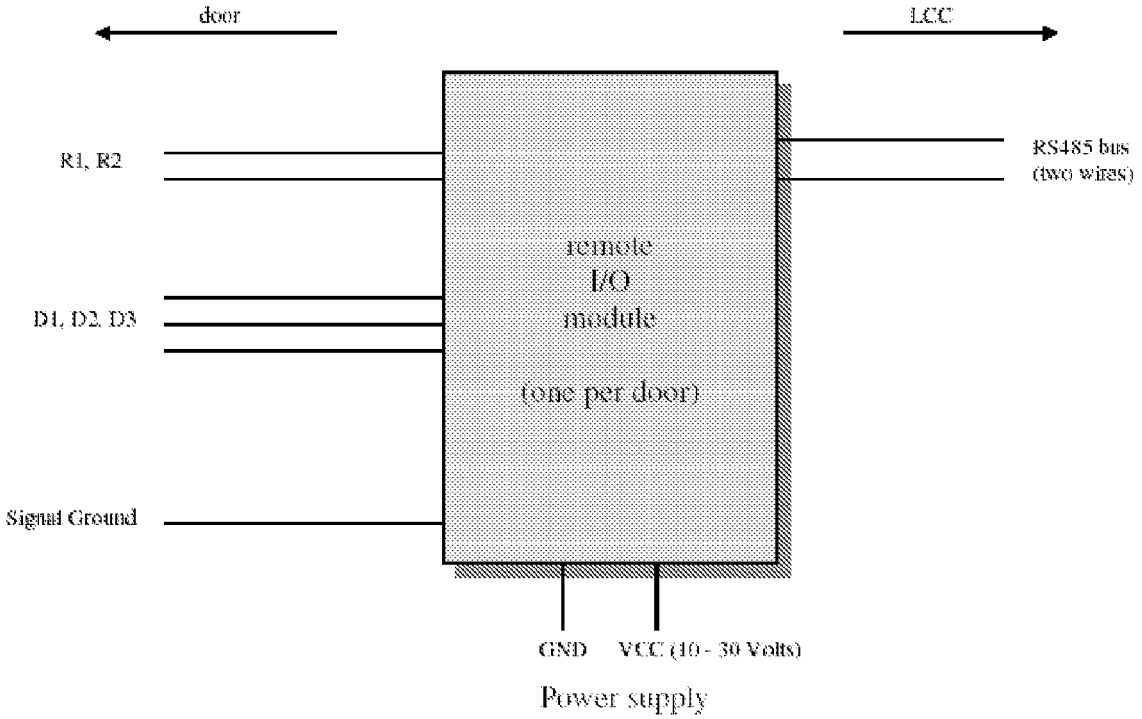


Figure 4

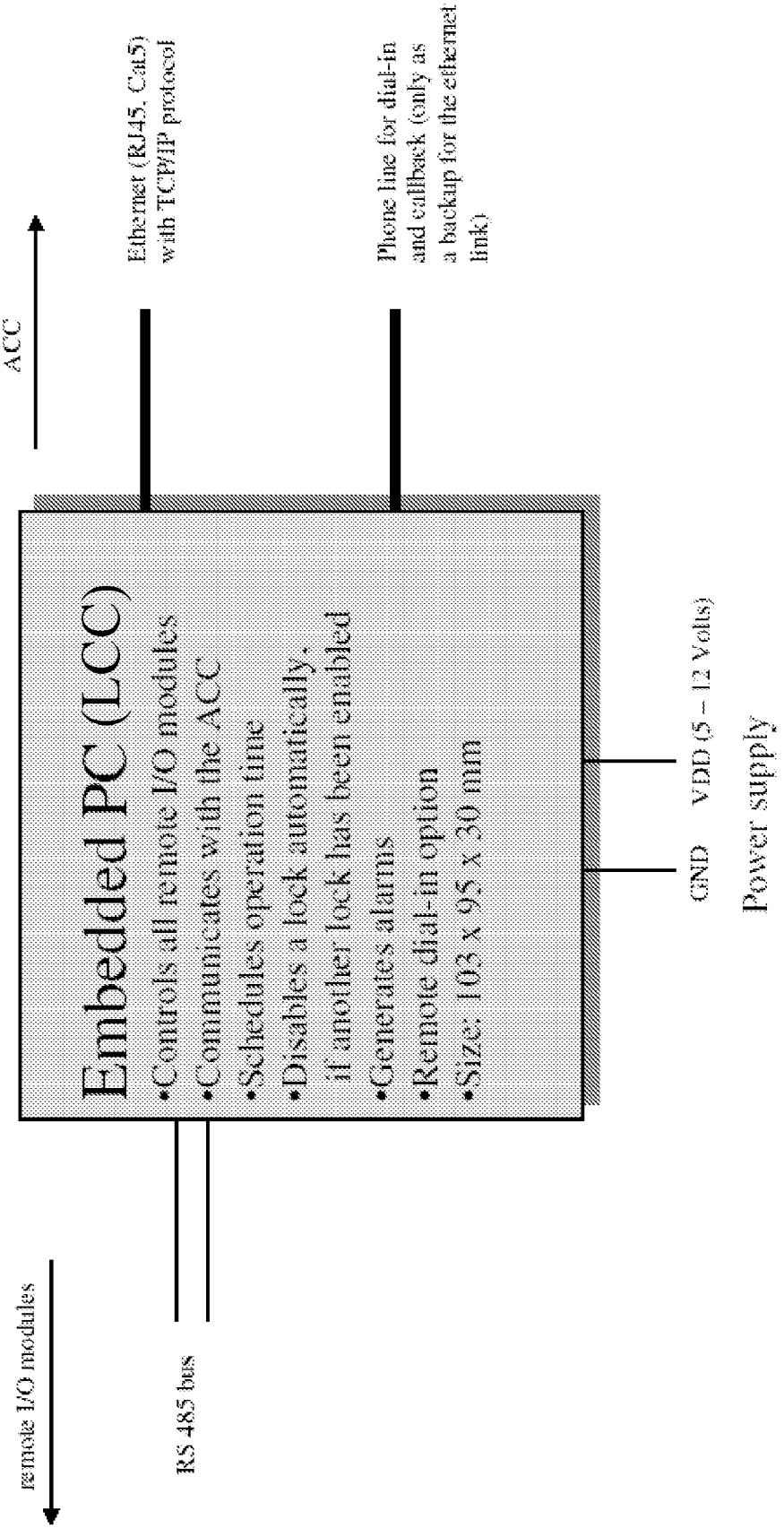

ACC
Ethernet (RJ45, Cat5) with TCP/IP protocol
Phone line for dial-in and callback (only as a backup for the ethernet link)
Embedded PC (LCC)
•Controls all remote I/O modules
•Communicates with the ACC
•Schedules operation time
•Disables a lock automatically, if another lock has been enabled
•Generates alarms
•Remote dial-in option
•Size: 103 x 95 x 30 mm
GND VDD (5 – 12 Volts)
Power supply
RS 485 bus
remote I/O modules

Figure 5

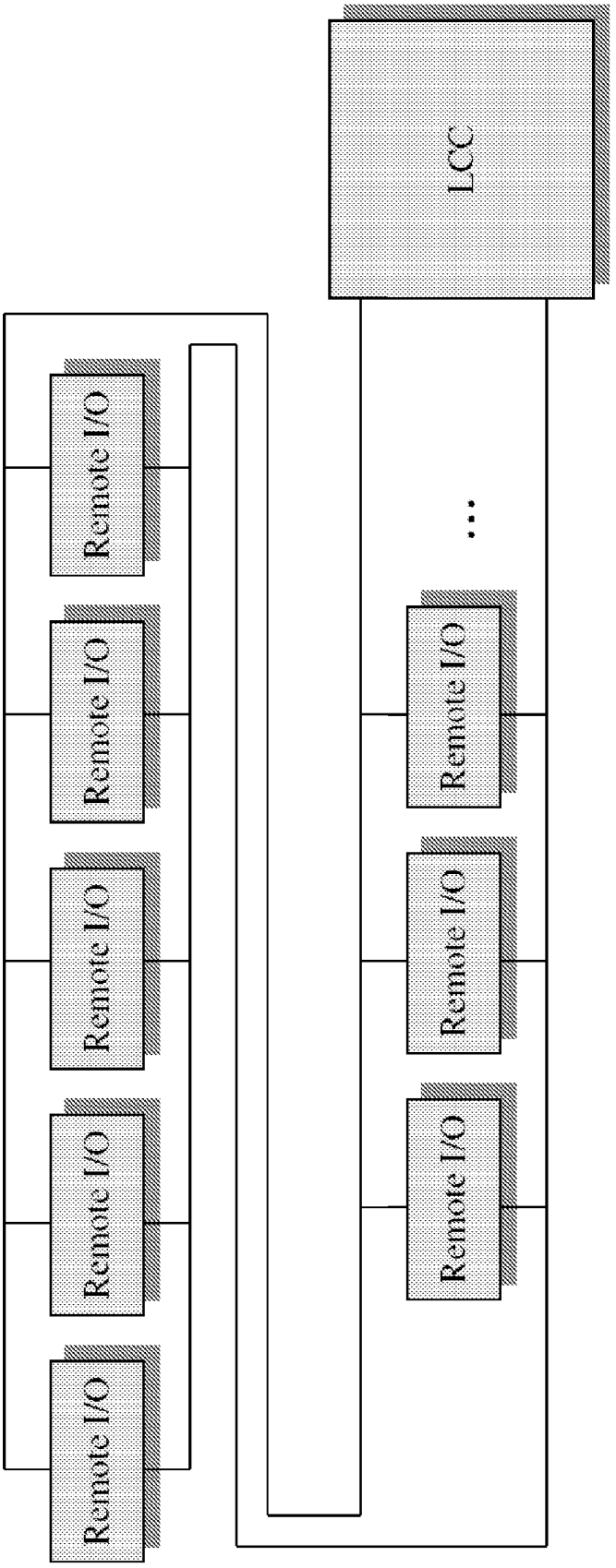

LCC
Remote I/O
Remote I/O
Remote I/O
Remote I/O
Remote I/O
...
Remote I/O
Remote I/O
Remote I/O

Figure 6

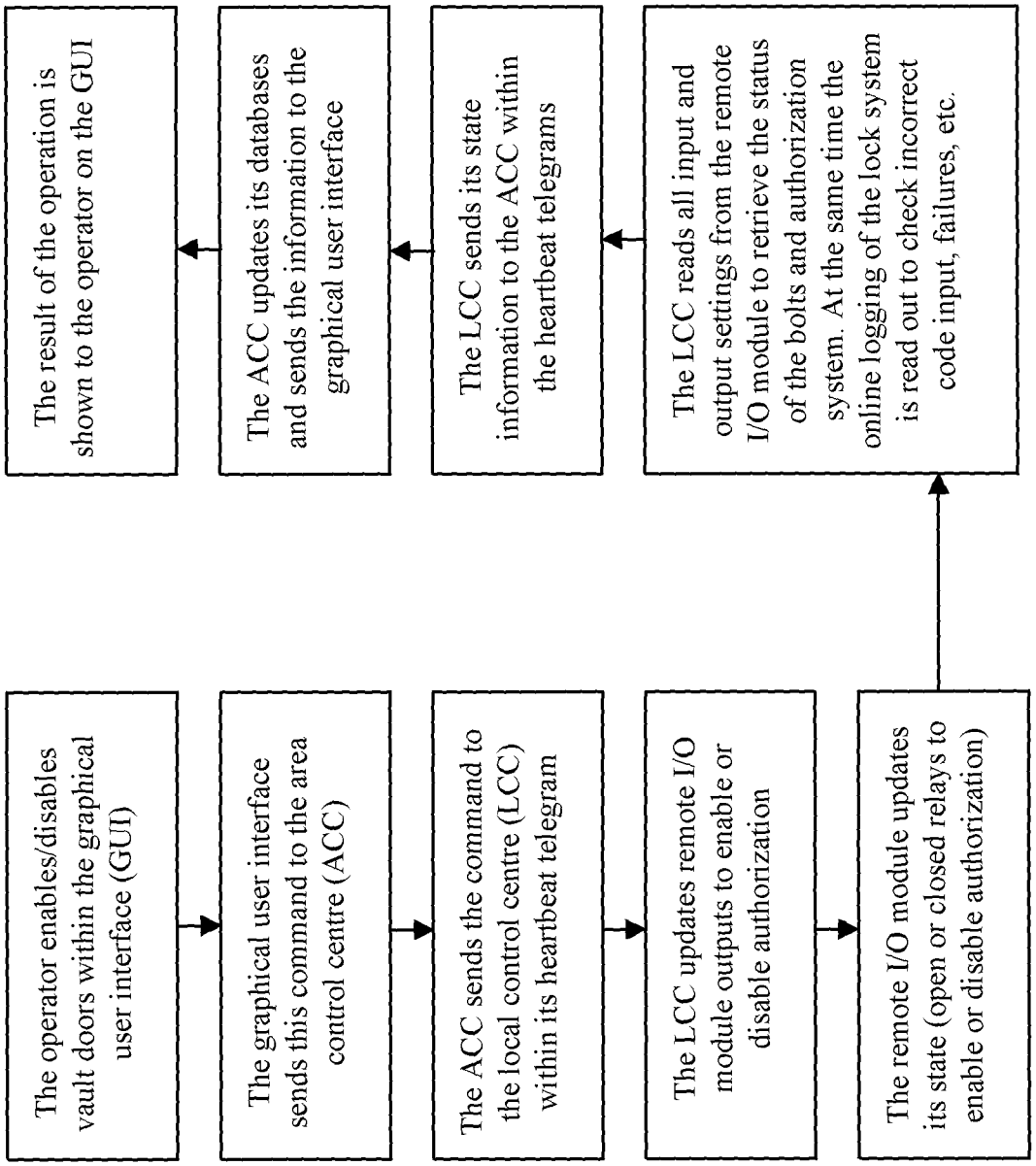
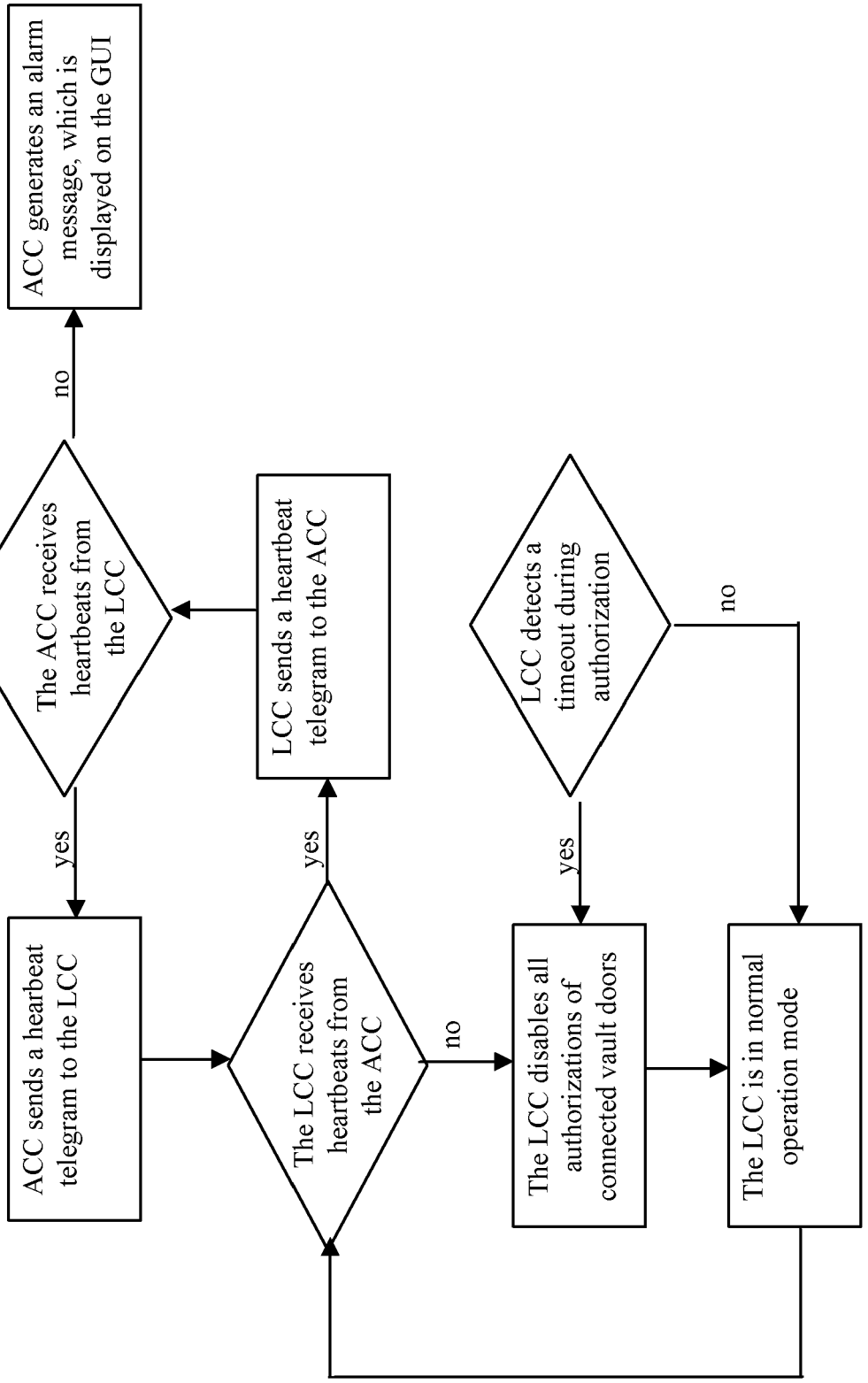

The operator enables/disables vault doors within the graphical user interface (GUI)
The graphical user interface sends this command to the area control centre (ACC)
The ACC sends the command to the local control centre (LCC) within its heartbeat telegram
The LCC updates remote I/O module outputs to enable or disable authorization
The remote I/O module updates its state (open or closed relays to enable or disable authorization)
The LCC reads all input and output settings from the remote I/O module to retrieve the status of the bolts and authorization system. At the same time the online logging of the lock system is read out to check incorrect code input, failures, etc.
The LCC sends its state information to the ACC within the heartbeat telegrams
The ACC updates its databases and sends the information to the graphical user interface
The result of the operation is shown to the operator on the GUI

Figure 7


ACC generates an alarm message, which is displayed on the GUI
no
The ACC receives heartbeats from the LCC
yes
ACC sends a hearbeat telegram to the LCC
LCC sends a heartbeat telegram to the ACC
yes
The LCC receives heartbeats from the ACC
no
The LCC disables all authorizations of connected vault doors
LCC detects a timeout during authorization
yes
no
The LCC is in normal operation mode

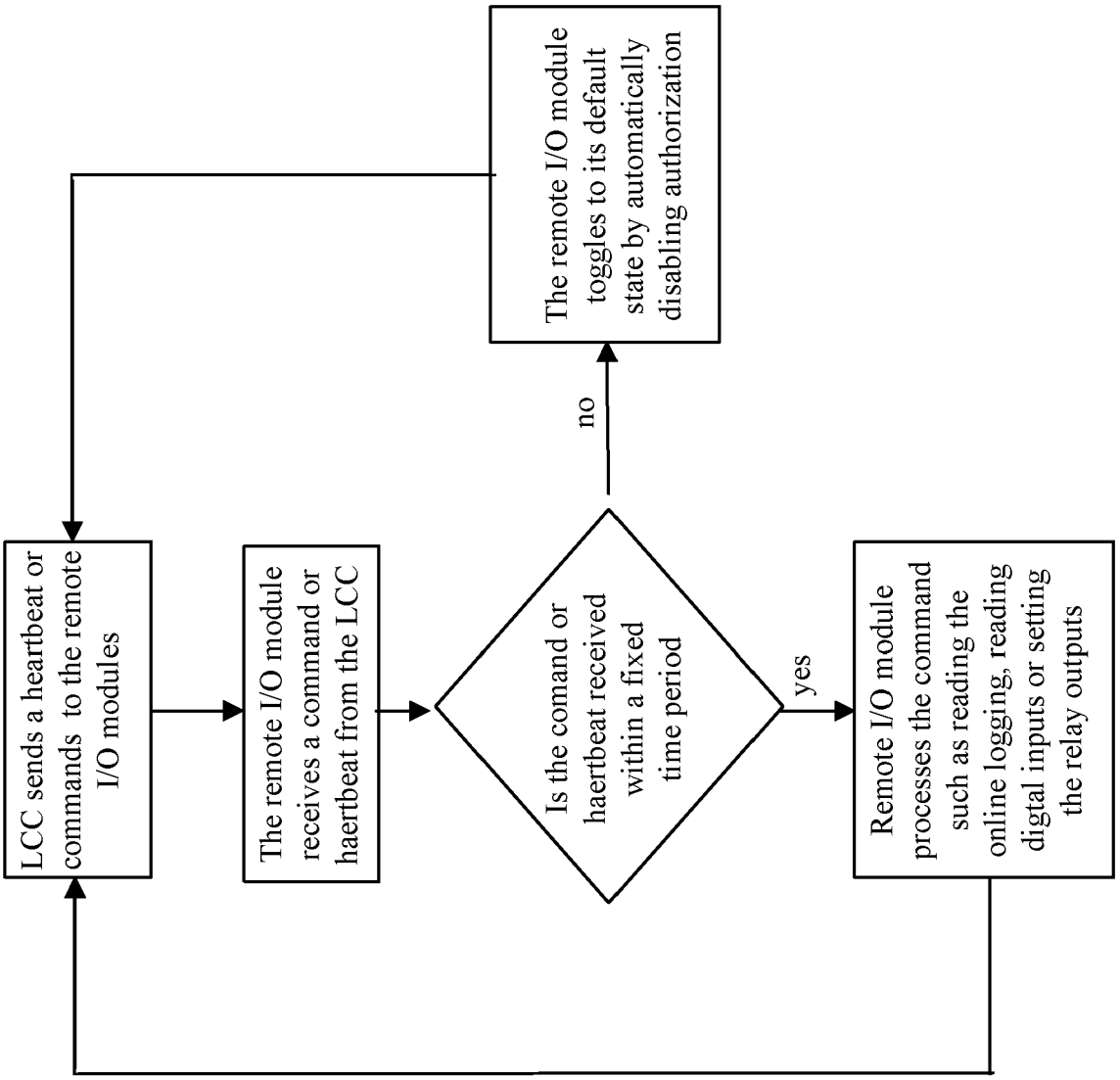

LCC sends a heartbeat or commands to the remote I/O modules
The remote I/O module receives a command or haertbeat from the LCC
Is the comand or haertbeat received within a fixed time period
no
yes
The remote I/O module toggles to its default state by automatically disabling authorization
Remote I/O module processes the command such as reading the online logging, reading digtal inputs or setting the relay outputs

Figure 8

Figure 9

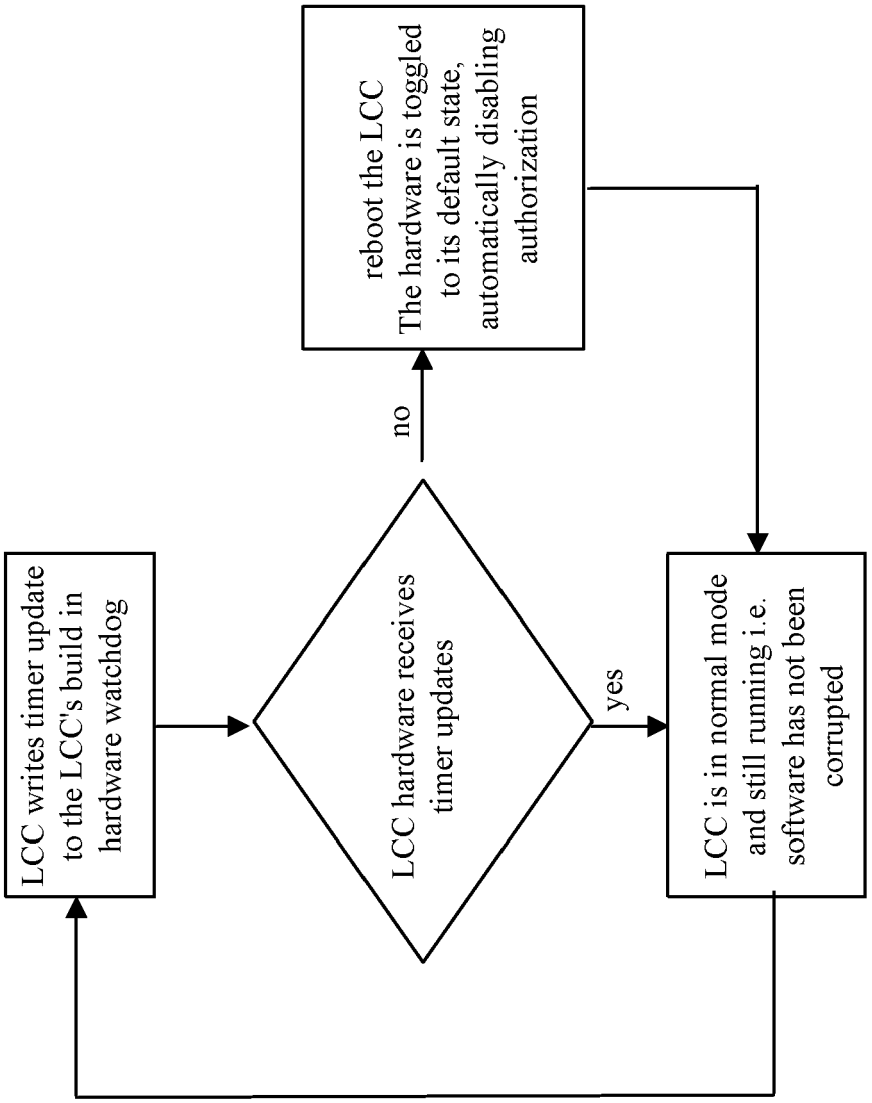
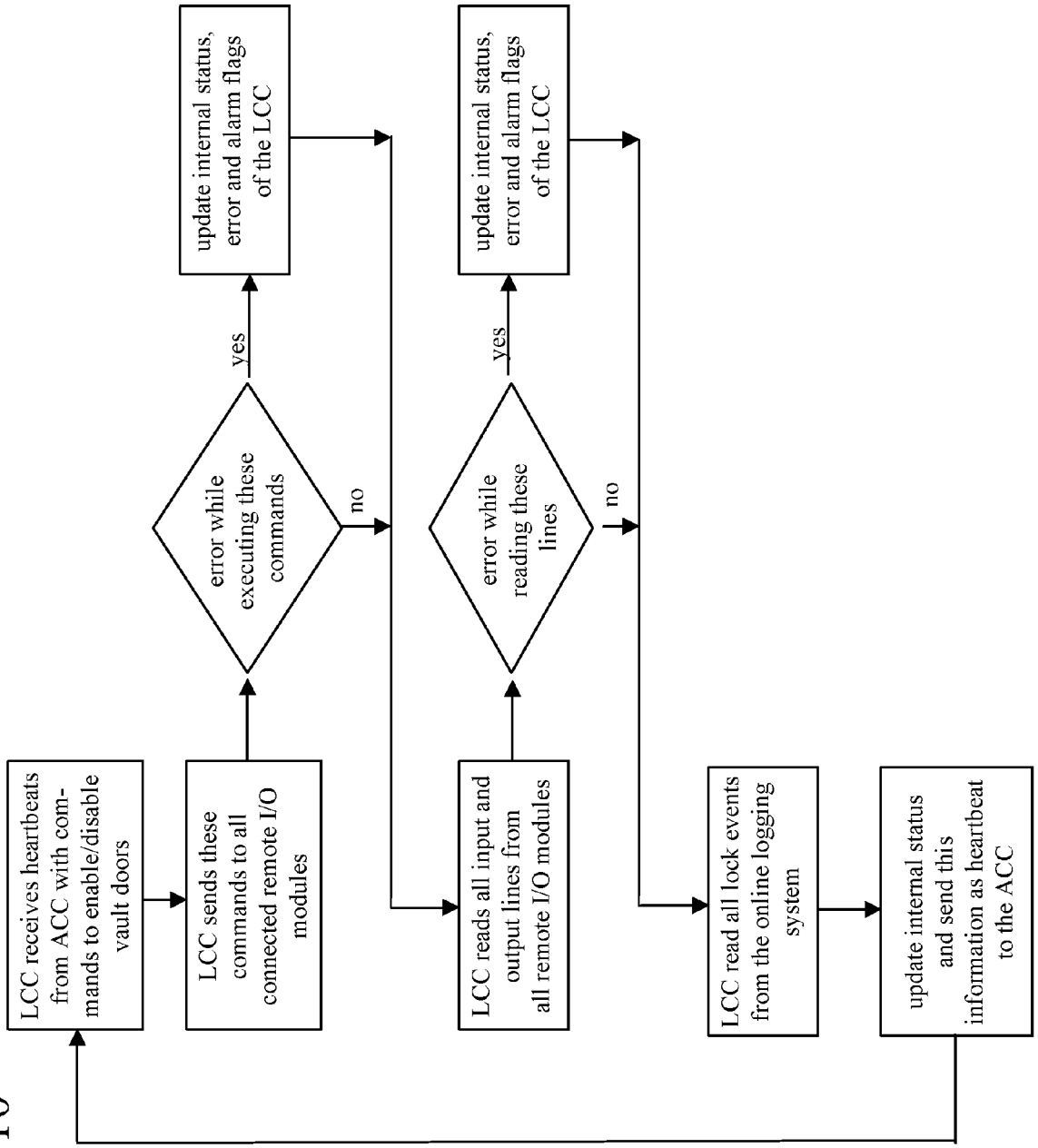

LCC writes timer update to the LCC's build in hardware watchdog
LCC hardware receives timer updates
no
reboot the LCC
The hardware is toggled to its default state, automatically disabling authorization
yes
LCC is in normal mode and still running i.e. software has not been corrupted

Figure 10


LCC receives heartbeats from ACC with commands to enable/disable vault doors
LCC sends these commands to all connected remote I/O modules
error while executing these commands
yes
update internal status, error and alarm flags of the LCC
no
LCC reads all input and output lines from all remote I/O modules
error while reading these lines
yes
update internal status, error and alarm flags of the LCC
no
LCC read all lock events from the online logging system
update internal status and send this information as heartbeat to the ACC

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 12 1858

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	WO 2004/095804 A (DOMINGUEZ CANSINO JUAN MIGUEL [ES]; SARGENT & GREENLEAF [US]) 4 November 2004 (2004-11-04) * abstract * * page 4, line 17 - line 24 * * page 5, line 6 - line 20 * * page 6, line 3 - page 7, line 9 * * page 8, line 21 - page 14, line 20 * * page 19, line 5 - line 10 * * page 34, line 23 - page 36, line 24 * * page 39, line 16 - page 41, line 3 * * figures 1A,1B,2A,2B,3,6 *	1-10,16	INV. G07C9/00
A	DE 195 33 255 A1 (ACKERMANN BERND DIPL ING [DE]; SCHRUFF ALFRED [DE]; JANSER FRANK DIPL) 13 March 1997 (1997-03-13) * abstract * * page 2, line 40 - line 63 * * page 3, line 20 - page 5, line 17 * * figures 1,2 *	1,2,16	
A	TW 235 299 B (NAT CHENG KUNG UNIVERSITY [TW]) 1 July 2005 (2005-07-01) * the whole document *	4,5	TECHNICAL FIELDS SEARCHED (IPC) G07C G07F
P,A	-& US 2005/237926 A1 (CHENG FAN-TIENG [TW] ET AL) 27 October 2005 (2005-10-27) * page 3, paragraph 33 - paragraph 36 * * page 3, paragraph 44 - page 4, paragraph 49 * * page 4, paragraph 53 *	4,5	
A	US 2004/250178 A1 (MUNGUIA PETER R [US] ET AL) 9 December 2004 (2004-12-09) * abstract * * page 1, paragraph 1 - paragraph 2 * * page 1, paragraph 7 - page 2, paragraph 23 *	6-9	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	23 April 2007	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)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 06 12 1858

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	US 2003/169337 A1 (WILSON JEREMY CRAIG [NZ] ET AL) 11 September 2003 (2003-09-11) * abstract * * page 2, paragraph 14 - paragraph 16 * * page 2, paragraph 24 - paragraph 25 * * page 2, paragraph 28 * -----	11,12	
A	US 4 939 352 A (SUNYICH STEVEN L [US]) 3 July 1990 (1990-07-03) * column 3, line 10 - line 31 * * column 6, line 25 - column 9, line 23 * -----	11	
A	GB 1 572 827 A (MCCORQUODALE & CO LTD) 6 August 1980 (1980-08-06) * page 2, line 40 - line 63 * * figure 2 * -----	11	
			TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	23 April 2007	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)

European Patent Office

Application Number
EP 06 12 1858

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims 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 the first ten claims.

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:

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 06 12 1858

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: 1-10,16

Apparatus for remotely monitoring the status of a lock, and safe or vault door comprising such an apparatus.

---

2. claims: 11-15

Method for remotely enabling and disabling the input of an access code into a lock.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 06 12 1858

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.

23-04-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004095804 A	04-11-2004	BR PI0408855 A	04-04-2006
		CA 2520777 A1	04-11-2004
		CN 1871830 A	29-11-2006
		EP 1614272 A1	11-01-2006
		US 2004189439 A1	30-09-2004
DE 19533255 A1	13-03-1997	NONE	
TW 235299 B	01-07-2005	US 2005237926 A1	27-10-2005
US 2005237926 A1	27-10-2005	TW 235299 B	01-07-2005
US 2004250178 A1	09-12-2004	NONE	
US 2003169337 A1	11-09-2003	GB 2394341 A	21-04-2004
US 4939352 A	03-07-1990	NONE	
GB 1572827 A	06-08-1980	NONE	

EPO FORM P0459

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