

(43) International Publication Date
23 September 2010 (23.09.2010)(10) International Publication Number
WO 2010/106474 A1

(51) International Patent Classification:

E05B 47/00 (2006.01) *G07C 9/00* (2006.01)
E05B 47/06 (2006.01)

(21) International Application Number:

PCT/IB2010/051067

(22) International Filing Date:

12 March 2010 (12.03.2010)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2009901185 19 March 2009 (19.03.2009) AU

(71) Applicant (for all designated States except US): **HONEYWELL INTERNATIONAL INC.** [US/US]; 101 Columbia Road, AB-2B, Morristown, New Jersey 07962 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BHANDARI, Nee-lendra** [IN/IN]; BB/76/3RD/30 Govt. Hospital Campus, Barmer, RAJASTHAN 344001 (IN). **ROY, Sanjay** [IN/IN]; C/o Shelston Ip, Level 21 60 Margaret Street, Sydney, New South Wales 2000 (AU). **REDDY, Chandrakantha** [IN/IN]; S/o C. Lakshmi Reddy, Reddy's

Street, Velgode Kurnool District, Andhra Pradesh 518533 (IN).

(74) Agent: **ANURADHA, Moulee**; SHELSTON IP, Level 21, 60 Margaret Street, Sydney, NSW 2000 (AU).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR MANAGING ACCESS CONTROL DEVICES

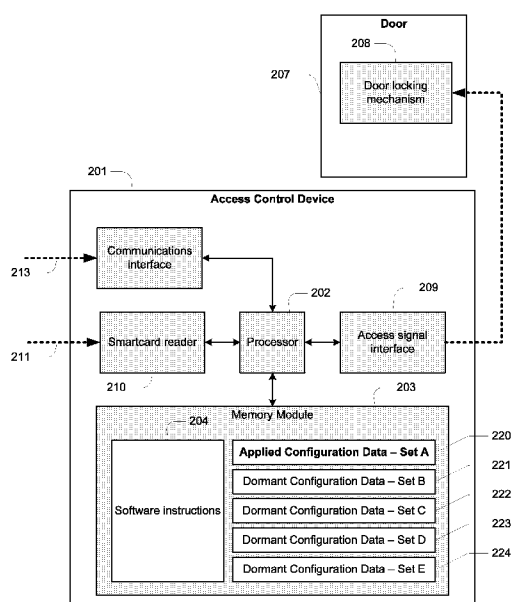


FIG. 2

(57) Abstract: Described herein are systems and methods for managing access control devices. In overview, an access control device is configured to function on the basis of an applied set of configuration data. For example, the manner in which the device processes an access request is dependent on the configuration data. A device according to an embodiment of the present invention is configured to locally maintain plurality of uniquely applicable sets of configuration data. Each set, when applied, causes the device to function in accordance with a respective mode of operation. The device is configured to change which set of configuration data is applied in response to a predetermined command, thereby allowing the device to shift between modes of operation relatively quickly and without the need to download additional configuration data. In some cases, the modes of operation correspond to threat levels, and the use of such access control devices allows a change in threat level to be applied across an access control environment quickly and with minimal bandwidth requirements.



Published:

— *with international search report (Art. 21(3))*

- 1 -

SYSTEMS AND METHODS FOR MANAGING ACCESS CONTROL DEVICES

FIELD OF THE INVENTION

[0001] The present invention relates to access control, and more particularly to systems and methods for managing access control devices. In particular, some embodiments include access control devices themselves, and/or software operable on access control devices or other devices.

[0002] Embodiments of the invention have been particularly developed for allowing the efficient implementation of a threat level across an access control environment. Although the invention is described hereinafter with particular reference to such applications, it will be appreciated that the invention is applicable in broader contexts.

BACKGROUND

[0003] Any discussion of the prior art throughout the specification should in no way be considered as an admission that such prior art is widely known or forms part of common general knowledge in the field.

[0004] It is known to use a large number of access control devices in an access control environment. Before each individual access control device is able to function as part of the access control environment, those individual devices need to be commissioned and configured. Commissioning refers to a process whereby the devices are initialized to operate within a common access control environment. Configuration refers to a process whereby configuration data is downloaded to the individual devices, thereby to allow those devices to function appropriately. For example, configuration data affects how a device will respond to an access request from a user.

[0005] From time-to-time, there may be a desire to modify configuration data on some or all of the access control devices within an access control environment and, in this regard, there are various known approaches for transferring new configuration data to those devices. For example, it is often possible to transfer such configuration data from a central server to the individual devices via a network, such as a TCP/IP network. Other approaches include the use of portable computers and the like.

- 2 -

[0006] Transferring configuration data can be a time and resource intensive task, and this can lead to complications in situations where there is a desire to make a change across an entire access control environment on an expeditious basis.

[0007] It follows that there is a need in the art for improved systems and methods for managing access control devices.

SUMMARY

[0008] It is an object of the present invention to overcome or ameliorate at least one of the disadvantages of the prior art, or to provide a useful alternative.

[0009] One embodiment provides an access control device including: a processor for allowing the execution of software instructions, including software instructions for processing data indicative of access requests on the basis of an applied set of configuration data and selectively allowing or denying the respective requests; a memory module coupled to the processor, the memory module storing data indicative of the software instructions and configuration data, wherein the configuration data stored by the device includes a plurality of uniquely applicable sets of configuration data, wherein each set, when applied, causes the device to function in accordance with a respective mode of operation; and a communications interface that is configured for receiving data indicative of a command to change modes of operation, wherein in response to the command the software instructions cause the device to cease applying a current set of configuration data and commence applying a different set of configuration data identified by the command.

[0010] One embodiment provides a method performable by an access control device, the method including: applying a first set of configuration data stored locally at the access control device, the first set of configuration data, when applied, causing the device to function in a first mode of operation; whilst functioning in the first mode of operation, processing data indicative of access requests on the basis of the first set of configuration data; receiving data indicative of a command to change to a second mode of operation; in response to the command, ceasing application of the first set of configuration data and commencing application of a second set of configuration data, wherein the second set of configuration data is also stored locally at the access control device, the second set of configuration data, when applied, causing the device to

- 3 -

function in the second mode of operation; and whilst functioning in the second mode of operation, processing data indicative of access requests on the basis of the second set of configuration data.

[0011] One embodiment provides access control system including: a plurality of access control devices as described herein; and a central server in communication with the plurality of access control devices via a network, wherein the central server is configured to provide to the plurality of devices data indicative of a command to change modes of operation, wherein in response to the command, the devices each cease applying a current set of configuration data and commence applying a different set of configuration data identified by the command.

[0012] One embodiment provides a method for controlling an access control environment, wherein the access control environment includes a plurality of access control devices as described herein, the method including providing to the devices data indicative of a command to change modes of operation, wherein in response to the command the software instructions cause the device to cease applying a current set of configuration data and commence applying a different set of configuration data identified by the command, wherein the different set of configuration data is locally stored at the devices.

[0013] One embodiment provides a hardware component configured device configured to perform a method as described herein.

[0014] One embodiment provides a computer program product configured device configured to perform a method as described herein.

[0015] One embodiment provides a carrier medium carrying computer executable code that, when executed on one or more processors, cause the performance of a method as described herein.

[0016] Reference throughout this specification to “one embodiment” or “an embodiment” or “some embodiments” means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases “in one embodiment” or “in an embodiment” or “in some embodiments” in various places

- 4 -

throughout this specification are not necessarily all referring to the same embodiment, but may. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner, as would be apparent to one of ordinary skill in the art from this disclosure, in one or more embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

[0018] FIG. 1 schematically illustrates an access control environment according to one embodiment.

[0019] FIG. 2 schematically illustrates an access control device according to one embodiment.

[0020] FIG. 3A schematically illustrates an access control environment according to one embodiment.

[0021] FIG. 3B schematically illustrates an access control environment according to one embodiment.

[0022] FIG. 4 illustrates a method according to one embodiment.

DETAILED DESCRIPTION

[0023] Described herein are systems and methods for managing access control devices. In overview, an access control device is configured to function on the basis of an applied set of configuration data. For example, the manner in which the device processes an access request is dependent on the configuration data. A device according to an embodiment of the present invention is configured to locally maintain a plurality of uniquely applicable sets of configuration data. Each set, when applied, causes the device to function in accordance with a respective mode of operation. The device is configured to change which set of configuration data is applied in response to a predetermined command, thereby allowing the device to shift between modes of operation relatively quickly and without the need to download additional configuration data. In some cases, the modes of operation correspond to threat levels, and the use of such access control

- 5 -

devices allows a change in threat level to be applied across an access control environment quickly and with minimal bandwidth requirements.

[0024] Although examples considered herein are focused on access control devices, in other embodiments implementation occurs in respect of other devices, such as other devices in a broader security system (e.g. control systems configured for intrusion detection and/or video surveillance).

ACCESS CONTROL ENVIRONMENT

[0025] FIG. 1 schematically illustrates an access control environment 101 according to one embodiment. Environment 101 includes connected access control devices 102 to 104 and disconnected access control devices 105 to 107. The primary point of difference between the connected access control devices and the disconnected access control devices is that the former are connected to a network 108 (such as a TCP/IP or other network), whilst the latter are not. All of the access control devices have been commissioned for operation within environment 101, and provided configuration data to allow such operation.

[0026] An administration server 110 is also connected to network 108, and the connected access control devices are able to communicate with this administration server over the network. In this manner, server 110 is able to communicate with connected devices 105 to 107.

[0027] Although server 110 is schematically illustrated as a single component, in some cases it is defined by a plurality of distributed networked components.

[0028] For the sake of the present disclosure, it is assumed that each of access control devices 102 to 107 include similar hardware and software components, and each that device is configured to progress between a connected state and a disconnected state depending on whether or not a connection to network 108 and central server is available. However, in other embodiments a variety of different access control devices are used. For example, in some embodiments the access control devices are designed, from a hardware perspective, to allow/deny control to a variety of different locations or functionalities.

- 6 -

[0029] In the context of the present disclosure, the term “access control device” refers generally to any device having an access control functionality. That is, any device with which a user interacts to gain access to a physical region or virtual functionality. Common examples include devices that control locking mechanisms on doors or other barriers. An access control device includes either or both of hardware and software components.

ACCESS CONTROL DEVICE

[0030] FIG. 2 illustrates an exemplary access control device 201 according to one embodiment. Device 201 is configured for integration into an access control environment such as environment 101 of FIG. 1. Device 201 includes a processor 202 coupled to a memory module 203. Memory module 203 carries software instructions 204 which, when executed on processor 202, allow device 201 to perform various methods and functionalities described herein, which in themselves also provide embodiments of the present invention.

[0031] In the present example, device 201 is configured for selectively granting access through a door 207 having a locking mechanism 208. When in a locked state, this mechanism prevents access through the door, and when in an unlocked state, permits access through the door. To this end, processor 201 is coupled to an access signal interface 209 which selectively provides to locking mechanism 208 signals for unlocking and/or locking the door (in some cases the door retunes to a default locked state automatically, without need for an explicit “lock” signal). Whether or not the locked state is default depends on the configuration data applied at a particular point in time, although for the present example it is considered that the locked state is default, and unlocking of the door requires allowance of an access request.

[0032] A user wishing to gain access through door 207 makes an access request via device 201. For the sake of this example, this access request is initiated when the user presents (indicated by arrow 211) an access card to a card reader 210, which is also coupled to processor 201. Upon presentation of the access card, processor 202 performs an authentication/authorization process, influenced by configuration data, to determine whether or not access should be granted (i.e. the access request allowed). In the event that the authentication/authorization process is successful, interface 209 provides to

- 7 -

mechanism 208 a signal thereby to progress mechanism 208 to the unlocked state for a predefined period of time, typically the order of a few seconds, before returning to the locked state. If the authentication process is unsuccessful, mechanism 208 remains in the locked state, and access is denied.

[0033] The nature of card reader 210 varies between embodiments depending on the nature of access card that is used in a given access control environment. In the embodiment of FIG. 2, access cards are in the form of smartcards, and reader 210 is a smartcard reader. However, in other embodiments alternate components are provided for the same purpose, including the likes of magnetic card readers, proximity readers, biometric readers, keypads, and so on. In some cases multiple readers are present, such as a smartcard reader in combination with a biometric reader (for instance an iris scanner).

[0034] Device 201 additionally includes a communications interface 212, such as a wired or wireless Ethernet networking interface, or the like. This allows device 201 to communicate with remote components, such as a central server (at least when the device operates in a connected state). In this regard, device 201 is configured to receive a control signal 213 from a central server, or other networked component.

CONFIGURATION DATA

[0035] An access control device operates on the basis of configuration data. That is, the manner in which the device operates is dependent on the configuration data applied at a given point in time. For example, software instructions 204 include software instructions for processing data indicative of access requests, and this processing is performed on the basis of an applied set of configuration data. A given access request might be allowed based on one applied set of configuration data, but denied were another set of configuration data to be applied. This configuration data also influences other functionalities of the access control device.

[0036] Typically, an access control device maintains only a single set of configuration data. In known situations, such configuration data is downloaded during an initial configuration of a device, and updated configuration data is downloaded to the device over time as required. However, in accordance with the present embodiments, multiple sets of configuration data are downloaded to a device, with one being applied and the

- 8 -

others remaining dormant in memory. This allows for a change in device configuration without a need to download new configuration data; the applied set is simply interchanged for one of the dormant sets.

[0037] A set of configuration data includes a plurality of aspects of data, optionally including one or more of the aspects of data outlined below:

- Settings directly relevant to the processing of access requests, such as authentication/authorization settings and/or other access permission settings. Specific examples include visitor access card rules (for example some sets of configuration data block authorization for visitor access cards), supervisor requirements (for example some sets of configuration data require a supervisor present before access is granted), minimum occupancy requirements (for example requiring a minimum number of authorized persons to enter/exit/remain with a zone at any given point in time).
- Hardware settings, such as whether a locked/unlocked state is default.
- Scheduling settings. These include, for example, scheduling matters, such as where a device adopts a certain default locked/unlocked state during one time period, and another default locked/unlocked state during a different time period. Scheduling settings may also affect settings directly relevant to the processing of access requests, for example by causing these to be varied over time.
- Special functions. For example, configuration data in some cases causes a device to provide a signal to a surveillance system when predefined criteria are met.

[0038] In the case of device 201, memory module 203 stores configuration data including a plurality of uniquely applicable sets of configuration data. In this sense, the term “plurality” refers to “two or more”. That is, there may be two sets of configuration data, or more than two sets of configuration data.

[0039] In the context of FIG. 2, there are several sets of configuration data: configuration data set 220 and configuration data sets 221 to 224. For the sake of the example, set 220 is identified as the “active” configuration data (that which is applied) and sets 221 to 224 as “dormant” (that which is not applied).

- 9 -

[0040] Sets of configuration data are “uniquely applicable” in the sense that only one set is able to be applied at any given time, with other stored sets remaining dormant in memory. Although FIG. 2 illustrates only a small number of sets of dormant configuration data, there may be other sets of dormant configuration data stored in memory module 203 or elsewhere in device 201.

[0041] Each set of configuration data, when applied, causes the device to function in accordance with a respective mode of operation. In terms of the language presently used, the configuration data includes an n^{th} set of configuration data that, when applied, causes the device to function in an n^{th} mode of operation. For example:

- A first set of configuration data that, when applied, causes the device to function in a first mode of operation.
- A second set of configuration data that, when applied causes the device to function in a second mode of operation.

[0042] Communications interface 212 is configured for receiving data indicative of a command to change modes of operation. In response to such a command, software instructions 104 cause device 201 to cease applying a current set of configuration data and commence applying a different set of configuration data identified by the command. For example, when the device is functioning in a first mode of operation, the communications interface is configured for receiving data indicative of a command to change to a second mode of operation, and in response to the command the software instructions cause the device to cease applying the first set of configuration data and commence applying the second set of configuration data. In the context of FIG. 2, such a command causes a specified one of sets 221 to 224 to become active, and set 220 to become dormant in memory.

[0043] The nature of “data indicative of a command to change modes of operation” varies between embodiments. In some cases this data references a mode of operation to be adopted, in other cases it references a set of configuration data to be applied, and in other cases it refers to a threat level (or other criteria) to be applied. The data is in some embodiments transmitted over the network to connected access control devices as a TCP/IP signal or the like.

APPLICATION TO THREAT LEVELS

[0044] Embodiments are described below by reference to a situation where each set of configuration data corresponds to a respective “threat level”. The term “threat level” is used to describe a high-level security assessment. For example, the US Department of Homeland Security implements a “threat level” system via their Homeland Security Advisory System. This system uses the following criteria:

- Severe (red): severe risk.
- High (orange): high risk.
- Elevated (yellow): significant risk.
- Guarded (blue): general risk.
- Low (green): low risk.

[0045] In general terms, the Homeland Security Advisory System is a color-coded terrorism threat advisory scale. The different levels trigger specific actions by federal agencies and state and local governments, and they affect the level of security at some airports and other public facilities. In this regard, there is often a link between the System and the manner in which access control environments should be implemented. For example, an escalation in threat levels might have a practical consequence in that greater access control scrutiny is applied in, say, regions of an airport. For example, a particular class of employee may be able to access a particular area under one threat level, but not under another.

[0046] Different threat level systems are used in other jurisdictions and/or for other purposes, including UK Threat Levels, and Vigipirate in France. The present disclosure should not be limited to any such system in isolation, and the use of the term “threat level” is descriptive only, relating to the general concept of a tiered system whereby security or other concerns are categorized at a high-level and in an objective manner.

[0047] In the present embodiments, a set of configuration data is defined for each threat level, and the resulting sets of configuration data downloaded to the individual access control devices. At any given time, one set of configuration data is applied

- 11 -

(preferably corresponding to the current threat level) and the other sets remain dormant in memory.

[0048] In general terms, an access control device according to the present embodiment stores in memory:

- A first set of configuration data, when applied, causes the software instructions process data indicative of access requests in accordance with a first threat level.
- An n^{th} set of configuration data, when applied, causes the software instructions process data indicative of access requests in accordance with an n^{th} threat level.

[0049] Such an embodiment is schematically illustrated in FIG. 3A and FIG. 3B. A threat level advisory service 301 provides data indicative of a threat level, or change in a threat level. This data is provided to the central server 302 of an access control system. In some embodiments the data is provided by an automated electronic process (for example an automated notification), whilst in other cases the data is initially provided electronically via a notification (for example through a news agency, email, or the like), and subsequently manually entered into the central server.

[0050] When the central server receives data indicative of a change in threat level, it provides a signal to all connected access control devices 303 with which it compatibly interacts. In the illustrated example, there are “n” access control devices 303, and each maintains configuration data for at least three threat levels, being set 304A for “threat level A”, set 304B for “threat level B”, and set 304C for “threat level C”.

[0051] In the context of FIG. 3A, set 304A (corresponding to threat level A) is applied. For the sake of a simple example, it is assumed that threat level advisory service 301 provides to server 302 data indicative of a change to threat level B. As such, server 302 provides to each of devices 303 an instruction to apply set 304B, and those devices apply that set as shown in FIG. 3B.

[0052] It is not necessary that configuration data sets be identical among devices. For example, data set 304A might differ between devices, for example where those devices behave differently for a given threat level. For example, one device might control access to an area that is restricted to certain personnel during a given threat level, whilst another device might control access to an area that is restricted to other certain personnel during

- 12 -

that same threat level. This is optionally managed via system wide configuration, as described below.

SYSTEM WIDE CONFIGURATION

[0053] From an implementation perspective, one embodiment provides a threat level configuration module 310, being a software-based component allowing a user to define configuration data corresponding to threat levels. This module is, as illustrated, operable on central server 302. However, in another embodiment it is operable on a machine in communication with server 302. In some embodiments the module executes on a processor of server 302, although a user interface is presented on a remote terminal via a browser-based implementation or the like.

[0054] For the sake of the present examples, it is considered that module 310 provides a user interface for allowing a user to select between a plurality of threat levels, and adjust various parameters for each of those threat levels. For example, a user is able to select a GUI object corresponding to a particular threat level, and via that object access various menus and options for allowing modification of parameters for that threat level. The threat levels are optionally provided with default parameters.

[0055] In overview, module 310 allows a user to set up configuration data for a plurality of threat levels on a system-wide level. That is, rather than manually defining individual sets of configuration data for each individual access control device, module 310 provides an interface for defining the meaning of threat levels on a system wide basis, and from that automatically defines the actual sets of configuration data for the individual devices.

[0056] FIG. 4 illustrates a method for configuring threat levels in an access control environment according to one embodiment. This method is described in terms of a configuration module method, which is indicative of processes performed by the configuration module, and a user method, which is indicative of actions undertaken by a human user.

[0057] At step 401 the configuration module presents an initial user interface, which allows a user to select between one of a plurality of threat levels. These may be pre-defined, or available for user creation. A user selects a threat level at step 402, and the

- 13 -

configuration module presents a modification interface for that threat level at step 403. For example, the modification interface provides various prompts, menus and/or fields for allowing the user to modify various parameters for a threat level. The presently considered parameters are:

- Name and description. For example, these could optionally correspond to names and descriptions for an existing threat level system, such as the Homeland Security Advisory System.
- Behavior parameters. These define how a given access control device should behave under a given threat level. For example, this may include settings such as allow/block visitor cards, supervision requirements, minimum occupancy requirements, default door states (locked/unlocked), authentication needs, authorization settings, camera recording settings, and so on.
- Access right parameters. These define which cardholders/categories of cardholders have access to a given door (i.e. can traverse a given access control device) for the relevant threat level.

[0058] The user decides which parameter to modify at step 404, and optionally modifies name and description at 405 (leading to a name/description update at 406), behavior parameters at 407 (leading to a behavior parameter update at 408), or access right parameters at 409 (leading to a access right parameter update at 410). Whichever of these is selected, the method progresses to decision 411, where the user decides whether or not to modify other parameters, based on which the method either loops to step 404, or progresses to decision 412. At decision 412, the user decides whether configuration is complete, and either selects another threat level at 402, or provides and indication (explicit or implicit) that configuration is complete.

[0059] Following step 413, the configuration module defines configuration data for download to the individual control devices at step 414. This is downloaded to the devices at step 415, using one of the various known methodologies for downloading configuration data to access control devices. For example, this may include network transfer, download to portable media for provision to disconnected devices, and so on.

- 14 -

[0060] Once the configuration data is downloaded, the devices initially adopt a specified default threat level. It will be appreciated that a simple command is all that is required to progress the devices to a different threat level.

APPLYING THREAT LEVEL CHANGES TO DISCONNECTED DEVICES

[0061] As noted above, an access control environment often includes disconnected devices, being access control devices that are not connected to the central server via a network. The above disclosure deals with a situation where threat level changes are communicated via a command provided via the network. It will be appreciated that other approaches are required to communicate such a command to disconnected devices. Some exemplary approaches for achieving that goal are discussed below.

[0062] A relatively rudimentary approach is to simply manually deliver the command to disconnected devices, for example by presenting a smartcard or other carrier substrate (e.g. USB device) to the individual devices, or by connecting a portable computational platform (e.g. notebook computer, PDA, smartphone or the like) and uploading the command directly.

[0063] A more advanced (and less resource intensive) approach is to use ordinary user interactions to propagate a command. In the context of the present example, smartcards are used for the purpose of providing access requests. In overview, timestamped threat level information is maintained on smartcards, and devices are configured to read from each smartcard timestamped data indicative of a threat level. Subject to a predetermined authentication/authorization procedure (and other predefined constraints) the device selectively either:

- Adopts the set of configuration data for that threat level. This only occurs where the read data has a more recent timestamp as compared with the threat level being applied by the device. In some cases there are additional constraints for security purposes, one of which might be to prevent reduction in threat level by various classes of user.
- Writes to the smartcard updated timestamped data indicative of a threat level. This occurs where the device has newer threat level information than the smartcard. In

- 15 -

this manner, connected devices begin updating smartcards as soon as a threat level change command is received from a central server and processed.

- Takes no action.

[0064] It will be appreciated that such an approach is particularly effective for propagating threat level changes throughout an access control environment having disconnected devices, in a relatively unobtrusive and resource conscious manner.

[0065] In some cases threat levels cause devices to make additional modifications to smartcards. For example, various categories of user may have their cards cancelled, so that they can not be used in future.

CONCLUSIONS AND INTERPRETATION

[0066] It will be appreciated that the above disclosure provides various systems and methods for managing access control devices, these methods and systems providing distinct advantages and technical contributions over what was previously known in the art. For example, the storage of multiple sets of configuration data locally at individual devices allows substantial modification to device configuration/operation to be effected quickly and efficiently by way of a simple command signal. This is especially significant in respect of disconnected readers, noting that the simple nature of the command signal allows it to be effected by data carried by a conventional access card (in spite of inherent information storage constraints of such access cards) for convenient delivery to disconnected access control devices.

[0067] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing," "computing," "calculating," "determining", analyzing" or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities into other data similarly represented as physical quantities.

[0068] In a similar manner, the term "processor" may refer to any device or portion of a device that processes electronic data, e.g., from registers and/or memory to transform that electronic data into other electronic data that, e.g., may be stored in registers and/or

- 16 -

memory. A "computer" or a "computing machine" or a "computing platform" may include one or more processors.

[0069] The methodologies described herein are, in one embodiment, performable by one or more processors that accept computer-readable (also called machine-readable) code containing a set of instructions that when executed by one or more of the processors carry out at least one of the methods described herein. Any processor capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken are included. Thus, one example is a typical processing system that includes one or more processors. Each processor may include one or more of a CPU, a graphics processing unit, and a programmable DSP unit. The processing system further may include a memory subsystem including main RAM and/or a static RAM, and/or ROM. A bus subsystem may be included for communicating between the components. The processing system further may be a distributed processing system with processors coupled by a network. If the processing system requires a display, such a display may be included, e.g., an liquid crystal display (LCD) or a cathode ray tube (CRT) display. If manual data entry is required, the processing system also includes an input device such as one or more of an alphanumeric input unit such as a keyboard, a pointing control device such as a mouse, and so forth. The term memory unit as used herein, if clear from the context and unless explicitly stated otherwise, also encompasses a storage system such as a disk drive unit. The processing system in some configurations may include a sound output device, and a network interface device. The memory subsystem thus includes a computer-readable carrier medium that carries computer-readable code (e.g., software) including a set of instructions to cause performing, when executed by one or more processors, one of more of the methods described herein. Note that when the method includes several elements, e.g., several steps, no ordering of such elements is implied, unless specifically stated. The software may reside in the hard disk, or may also reside, completely or at least partially, within the RAM and/or within the processor during execution thereof by the computer system. Thus, the memory and the processor also constitute computer-readable carrier medium carrying computer-readable code.

[0070] Furthermore, a computer-readable carrier medium may form, or be included in a computer program product.

- 17 -

[0071] In alternative embodiments, the one or more processors operate as a standalone device or may be connected, e.g., networked to other processor(s), in a networked deployment, the one or more processors may operate in the capacity of a server or a user machine in server-user network environment, or as a peer machine in a peer-to-peer or distributed network environment. The one or more processors may form a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine.

[0072] Note that while some diagrams only show a single processor and a single memory that carries the computer-readable code, those in the art will understand that many of the components described above are included, but not explicitly shown or described in order not to obscure the inventive aspect. For example, while only a single machine is illustrated, the term “machine” or “device” shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

[0073] At least one embodiment of various methods described herein is in the form of a computer-readable carrier medium carrying a set of instructions, e.g., a computer program that are for execution on one or more processors, e.g., one or more processors that are part of building management system. Thus, as will be appreciated by those skilled in the art, embodiments of the present invention may be embodied as a method, an apparatus such as a special purpose apparatus, an apparatus such as a data processing system, or a computer-readable carrier medium, e.g., a computer program product. The computer-readable carrier medium carries computer readable code including a set of instructions that when executed on one or more processors cause the a processor or processors to implement a method. Accordingly, aspects of the present invention may take the form of a method, an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. Furthermore, the present invention may take the form of carrier medium (e.g., a computer program product on a computer-readable storage medium) carrying computer-readable program code embodied in the medium.

- 18 -

[0074] The software may further be transmitted or received over a network via a network interface device. While the carrier medium is shown in an exemplary embodiment to be a single medium, the term "carrier medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "carrier medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by one or more of the processors and that cause the one or more processors to perform any one or more of the methodologies of the present invention. A carrier medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical, magnetic disks, and magneto-optical disks. Volatile media includes dynamic memory, such as main memory. Transmission media includes coaxial cables, copper wire and fiber optics, including the wires that comprise a bus subsystem. Transmission media also may also take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications. For example, the term "carrier medium" shall accordingly be taken to include, but not be limited to, solid-state memories, a computer product embodied in optical and magnetic media, a medium bearing a propagated signal detectable by at least one processor of one or more processors and representing a set of instructions that when executed implement a method, a carrier wave bearing a propagated signal detectable by at least one processor of the one or more processors and representing the set of instructions a propagated signal and representing the set of instructions, and a transmission medium in a network bearing a propagated signal detectable by at least one processor of the one or more processors and representing the set of instructions.

[0075] It will be understood that the steps of methods discussed are performed in one embodiment by an appropriate processor (or processors) of a processing (i.e., computer) system executing instructions (computer-readable code) stored in storage. It will also be understood that the invention is not limited to any particular implementation or programming technique and that the invention may be implemented using any appropriate techniques for implementing the functionality described herein. The invention is not limited to any particular programming language or operating system.

- 19 -

[0076] Similarly it should be appreciated that in the above description of exemplary embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims following the Detailed Description are hereby expressly incorporated into this Detailed Description, with each claim standing on its own as a separate embodiment of this invention.

[0077] Furthermore, while some embodiments described herein include some but not other features included in other embodiments, combinations of features of different embodiments are meant to be within the scope of the invention, and form different embodiments, as would be understood by those in the art. For example, in the following claims, any of the claimed embodiments can be used in any combination.

[0078] Furthermore, some of the embodiments are described herein as a method or combination of elements of a method that can be implemented by a processor of a computer system or by other means of carrying out the function. Thus, a processor with the necessary instructions for carrying out such a method or element of a method forms a means for carrying out the method or element of a method. Furthermore, an element described herein of an apparatus embodiment is an example of a means for carrying out the function performed by the element for the purpose of carrying out the invention.

[0079] In the description provided herein, numerous specific details are set forth. However, it is understood that embodiments of the invention may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description.

[0080] As used herein, unless otherwise specified the use of the ordinal adjectives "first", "second", "third", etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that

- 20 -

the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

[0081] In the claims below and the description herein, any one of the terms comprising, comprised of or which comprises is an open term that means including at least the elements/features that follow, but not excluding others. Thus, the term comprising, when used in the claims, should not be interpreted as being limitative to the means or elements or steps listed thereafter. For example, the scope of the expression a device comprising A and B should not be limited to devices consisting only of elements A and B. Any one of the terms including or which includes or that includes as used herein is also an open term that also means including at least the elements/features that follow the term, but not excluding others. Thus, including is synonymous with and means comprising.

[0082] Similarly, it is to be noticed that the term coupled, when used in the claims, should not be interpreted as being limitative to direct connections only. The terms "coupled" and "connected," along with their derivatives, may be used. It should be understood that these terms are not intended as synonyms for each other. Thus, the scope of the expression a device A coupled to a device B should not be limited to devices or systems wherein an output of device A is directly connected to an input of device B. It means that there exists a path between an output of A and an input of B which may be a path including other devices or means. "Coupled" may mean that two or more elements are either in direct physical or electrical contact, or that two or more elements are not in direct contact with each other but yet still co-operate or interact with each other.

[0083] Thus, while there has been described what are believed to be the preferred embodiments of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the spirit of the invention, and it is intended to claim all such changes and modifications as fall within the scope of the invention. For example, any formulas given above are merely representative of procedures that may be used. Functionality may be added or deleted from the block diagrams and operations may be interchanged among functional blocks. Steps may be added or deleted to methods described within the scope of the present invention.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. An access control device including:

a processor for allowing the execution of software instructions, including software instructions for processing data indicative of access requests on the basis of an applied set of configuration data and selectively allowing or denying the respective requests;

a memory module coupled to the processor, the memory module storing data indicative of the software instructions and configuration data, wherein the configuration data stored by the device includes a plurality of uniquely applicable sets of configuration data, wherein each set, when applied, causes the device to function in accordance with a respective mode of operation; and

a communications interface that is configured for receiving data indicative of a command to change modes of operation, wherein in response to the command the software instructions cause the device to cease applying a current one of the sets of configuration data and commence applying a different one of the sets of configuration data identified by the command.

2. An access control device access according to claim 1 wherein the plurality of sets of configuration data include:

a first set of configuration data that, when applied, causes the device to function in a first mode of operation; and

a second set of configuration data that, when applied causes the device to function in a second mode of operation;

such that when the device is functioning in the first mode of operation, the communications interface is configured for receiving data indicative of a command to change to the second mode of operation, and in response to the command the software instructions cause the device to cease applying the first set of configuration data and commence applying the second set of configuration data.

- 22 -

3. An access control device access according to claim 1 wherein the configuration data includes an n^{th} set of configuration data that, when applied, causes the device to function in an n^{th} mode of operation.
4. An access control device access according to claim 1 wherein each set of configuration data corresponds to a respective threat level.
5. An access control device according to claim 4 wherein:
 - a first set of configuration data, when applied, causes the software instructions process data indicative of access requests in accordance with a first threat level; and
 - a second set of configuration data, when applied, causes the software instructions process data indicative of access requests in accordance with a second threat level.
6. An access control device access according to claim 1 wherein each set of configuration data describes respective authentication/authorisation settings.
7. An access control device access according to claim 1 wherein each set of configuration data describes respective access permission settings.
8. An access control device access according to claim 1 wherein each set of configuration data describes settings in relation to one or more of the following:
 - visitor access card rules;
 - supervisor requirements;
 - minimum occupancy requirements;
 - default access control states;
 - other access related rules and
 - surveillance settings.
9. An access control device access according to claim 1 including an input for interacting with an access control token, wherein the access control token maintains timestamped data indicative of a mode of operation and wherein, in response to the data indicative of a mode of operation, the device selectively adopts that mode of operation.

- 23 -

10. An access control device access according to claim 1 including an input for interacting with an access control token, wherein the access control token maintains timestamped data indicative of a mode of operation and wherein, in response to the data indicative of a mode of operation, the device selectively writes to the access control token updated timestamped data indicative of a mode of operation, the updated data being indicative of the current mode of operation of the device.

11. A method performable by an access control device, the method including:

applying a first set of configuration data stored locally at the access control device, the first set of configuration data, when applied, causing the device to function in a first mode of operation;

whilst functioning in the first mode of operation, processing data indicative of access requests on the basis of the first set of configuration data;

receiving data indicative of a command to change to a second mode of operation;

in response to the command, ceasing application of the first set of configuration data and commencing application of a second set of configuration data, wherein the second set of configuration data is also stored locally at the access control device, the second set of configuration data, when applied, causing the device to function in the second mode of operation; and

whilst functioning in the second mode of operation, processing data indicative of access requests on the basis of the second set of configuration data.

12. A method according to claim 11 wherein the device additionally stores an n^{th} set of configuration data that, when applied, causes the device to function in an n^{th} mode of operation.

13. A method according to claim 11 wherein each set of configuration data corresponds to a respective threat level.

14. A method according to claim 13 wherein:

when the first set of configuration data is applied, processing data indicative of access requests is performed in accordance with a first threat level; and

- 24 -

when the second set of configuration data is applied, processing data indicative of access requests is performed in accordance with the second threat level.

15. A method according to claim 11 wherein each set of configuration data describes respective authentication/authorisation settings.

16. A method according to claim 11 wherein each set of configuration data describes respective access permission settings.

17. A method according to claim 11 wherein each set of configuration data describes settings in relation to one or more of the following:

- visitor access card rules;
- supervisor requirements;
- minimum occupancy requirements;
- default access control states;
- other access related rules; and
- surveillance settings.

18. A method according to claim 11 including the steps of:

- reading an access control token, wherein the access control token maintains timestamped data indicative of a mode of operation;
- processing the data indicative of a mode of operation; and
- selectively adopting that mode of operation.

19. A method according to claim 11 including the step of:

- reading an access control token, wherein the access control token maintains timestamped data indicative of a mode of operation;
- processing the data indicative of a mode of operation; and
- selectively writing to the access control token updated timestamped data indicative of a mode of operation,

the updated data being indicative of the current mode of operation of the device.

- 25 -

20. A method according to claim 11 wherein the method is performable on the basis of software instructions stored on a memory module of the access control device by execution of those instructions on a processor of the access control device:

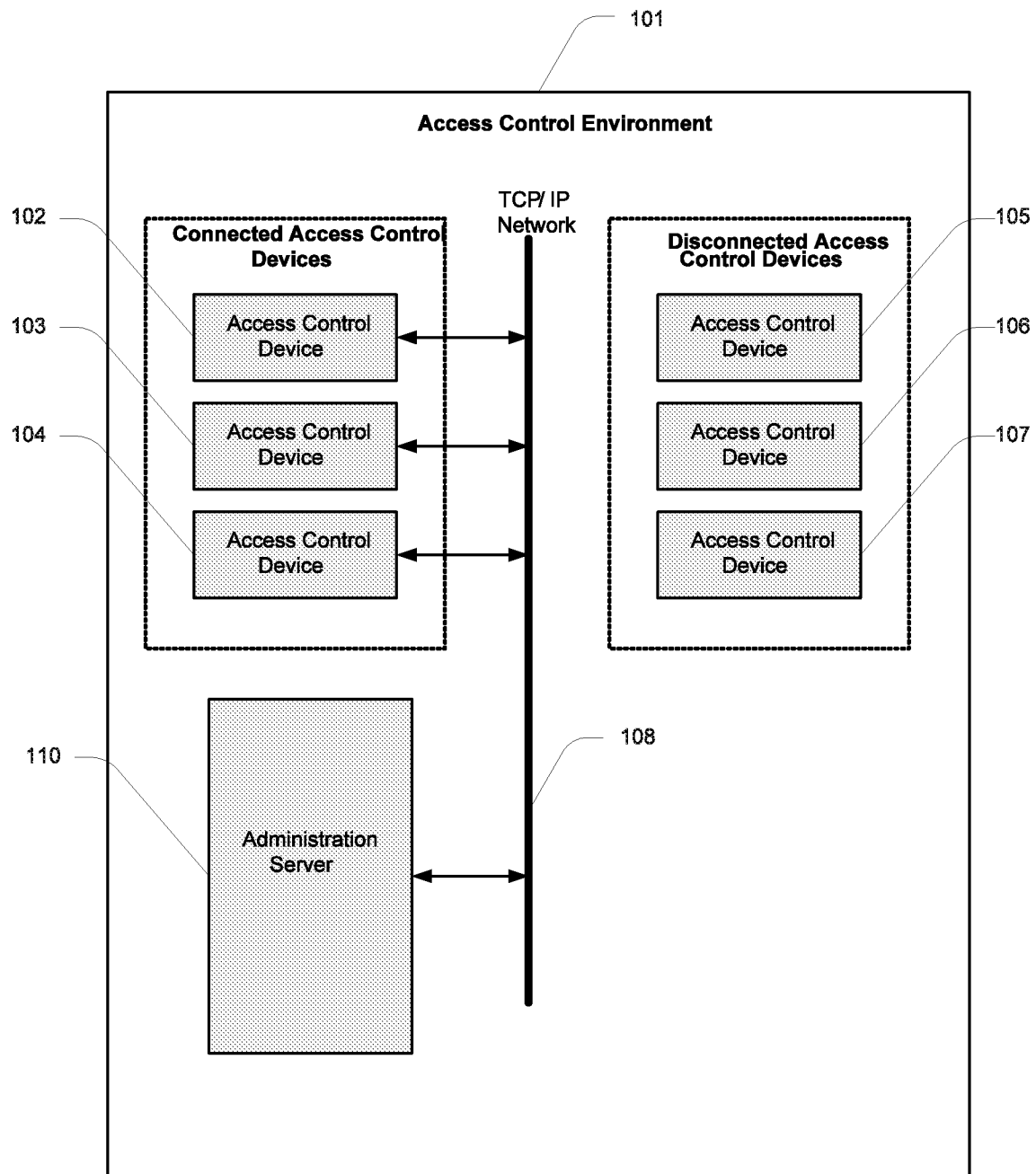
21. An access control system including:

a plurality of access control devices according to claim 1; and

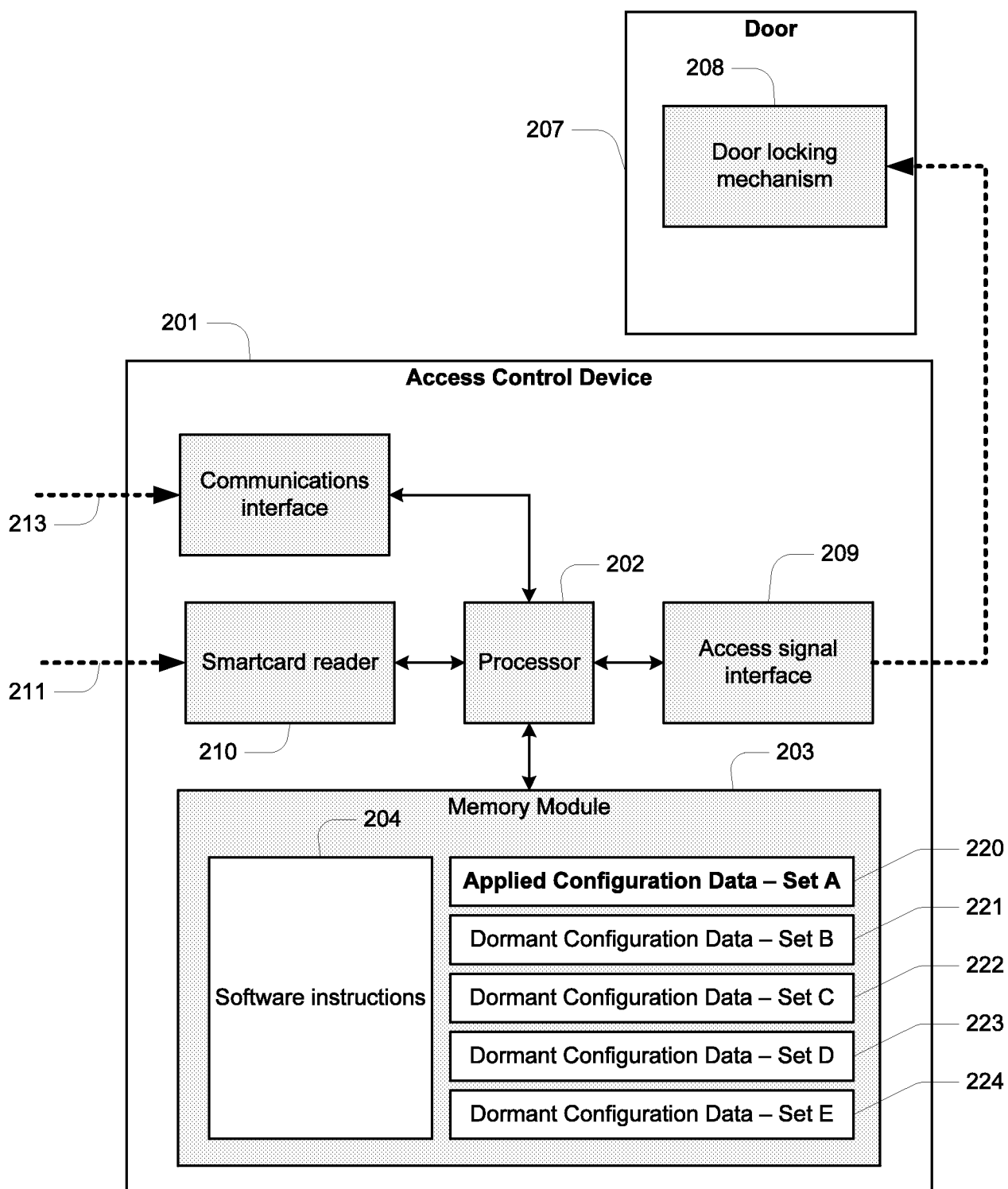
a central server in communication with the plurality of access control devices via a network, wherein the central server is configured to provide to the plurality of devices data indicative of a command to change modes of operation, wherein in response to the command, the devices each cease applying a current set of configuration data and commence applying a different set of configuration data identified by the command.

22. A method for controlling an access control environment, wherein the access control environment includes a plurality of access control devices according to claim 1, the method including providing to the devices data indicative of a command to change modes of operation, wherein in response to the command the software instructions cause the device to cease applying a current set of configuration data and commence applying a different set of configuration data identified by the command, wherein the different set of configuration data is locally stored at the devices.

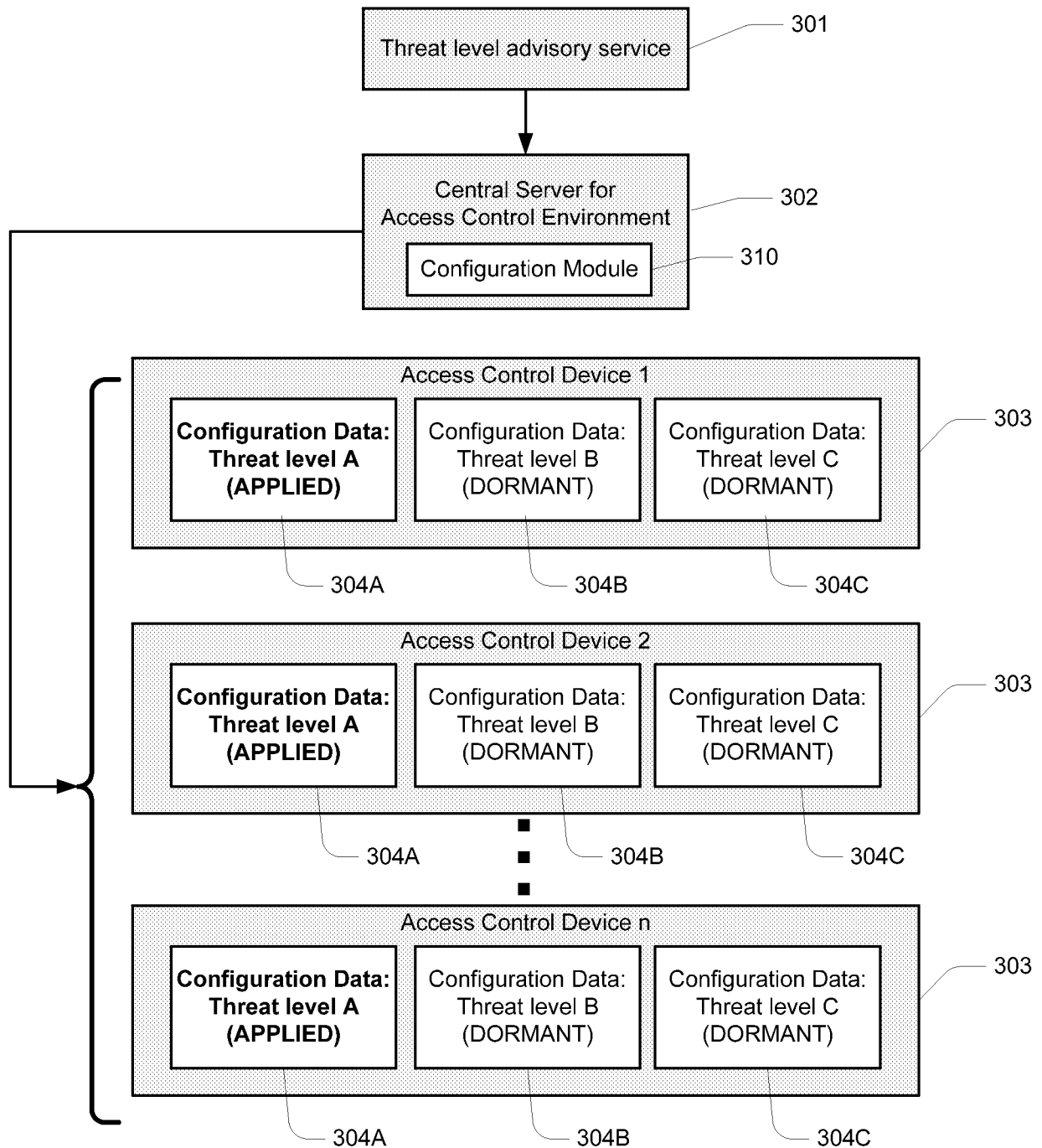
1/5

**FIG. 1**

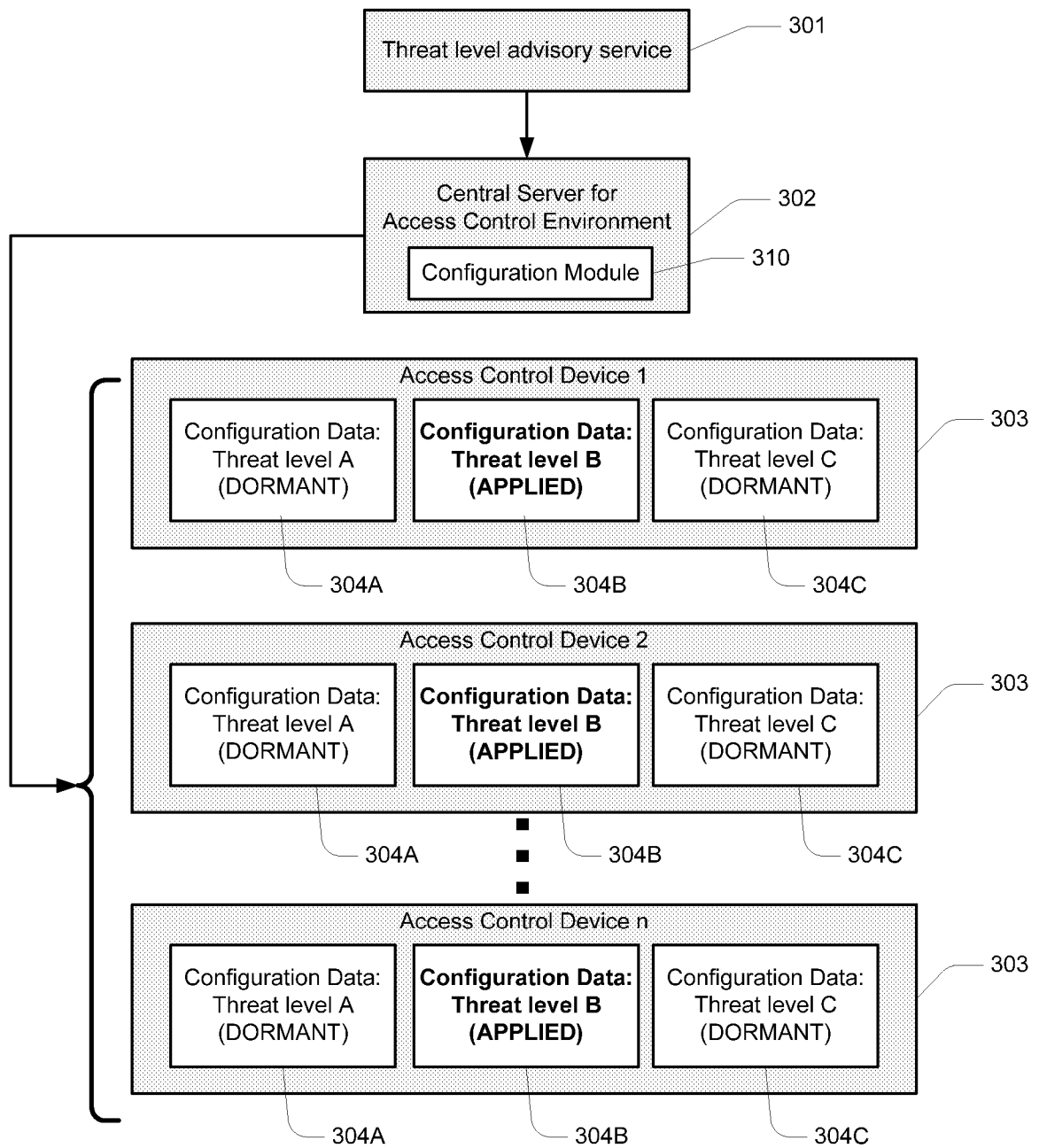
2/5

**FIG. 2**

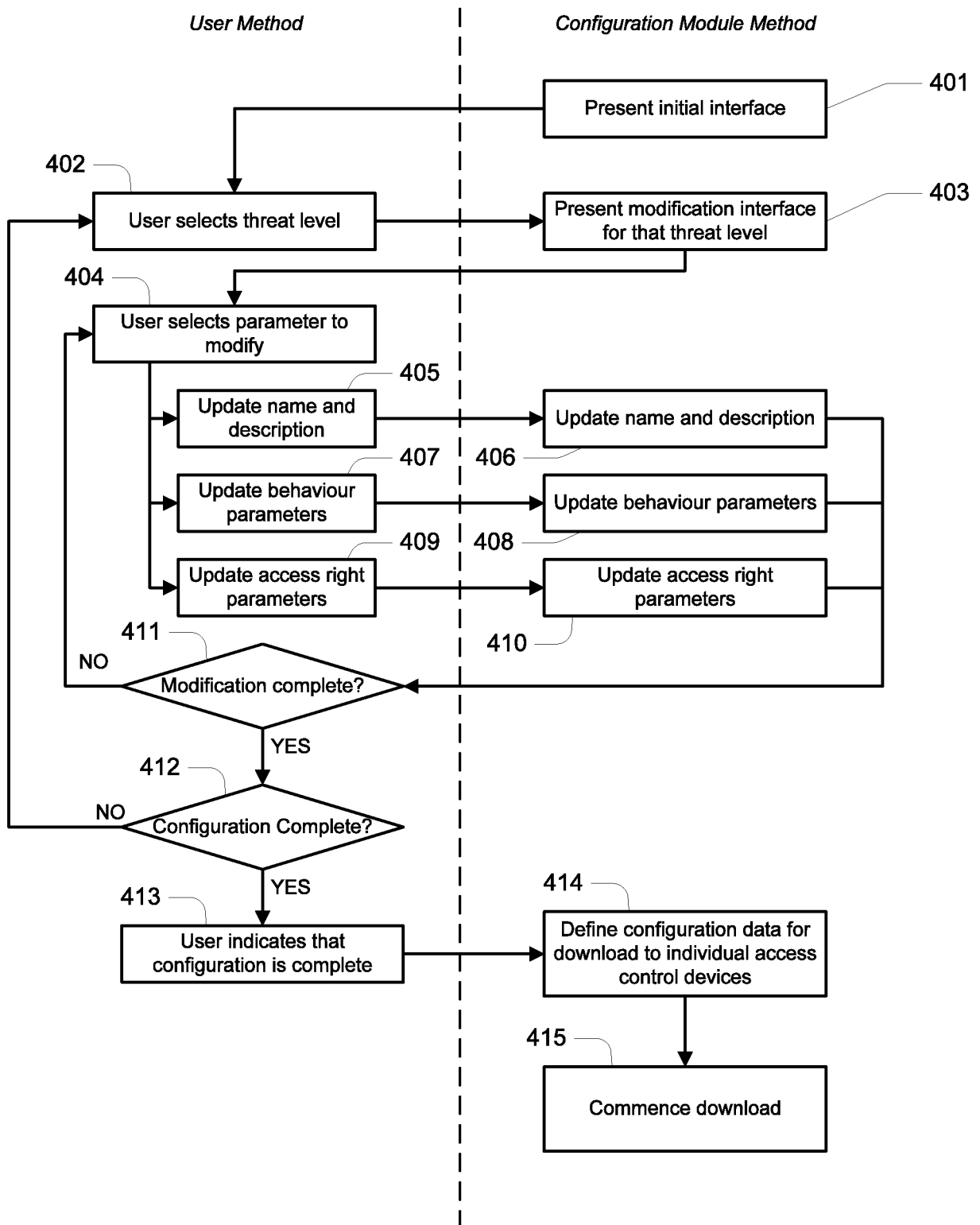
3/5

**FIG. 3A**

4/5

**FIG. 3B**

5/5

**FIG. 4**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB2010/051067

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

E05B 47/00 (2006.01)

E05B 47/06 (2006.01)

G07C 9/00 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, keywords (access, entry, exit, control, restriction, permission, authorization, security, rule, policy, configuration, card reader, electronic lock, operation mode, programmable, keyless, multiple) and the like terms, USPTO database, Google, Patenscope, esp@cenet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6318137 B1 (CHAUM) 20 November 2001 Abstract, col. 6 line 60-col. 8 line 26, col. 12 lines 6-44, col. 14 lines 28-64	1-22
A	US 2007/0132550 A1 (AVRAHAM et al.) 14 June 2007 Abstract, fig. 2, pars.[0011, 0013, 0016, 0019, 0049]	1-22
A	WO 2004/092514 A1 (TCAM TECHNOLOGY PTE. LTD.) 28 October 2004 Abstract, page 2 lines 14-24, page 5 lines 1-9, page 9 lines 20-29, fig. 1	1-22
A	US 2008/0313556 A1 (ZHANG et al.) 18 December 2008 Abstract, pars. [0004, 0007, 0016]	1-22



Further documents are listed in the continuation of Box C



See patent family annex

* "A"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E"	earlier application or patent but published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means	"&"	document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
24 May 2010

Date of mailing of the international search report

28 MAY 2010

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustalia.gov.au
Facsimile No. +61 2 6283 7999

Authorized officer

YING LI

AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : (02) 6283 2802

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/IB2010/051067

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member	
US	6318137	AU 41999/00 WO 0060197	EP 1165911 US 2003205070
US	2007132550	NONE	
WO	2004092514	NONE	
US	2008313556	CA 2634780	CN 101329781 EP 2003620
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.			
END OF ANNEX			