(12) UK Patent Application (19) GB (11) 2 434 239 (13) A

(43) Date of A Publication 18.07.2007

(21) Application No: 0600553.2

(22) Date of Filing: 12.01.2006

(71) Applicant(s):
Motorola Inc
(Incorporated in USA - Delaware)
1303 East Algonquin Road, Schaumburg,
Illinois 60196, United States of America

(72) Inventor(s):
Kenneth Jahn Lavrsen
Torben Truelsen

(74) Agent and/or Address for Service:
Optimus
Grove House, Lutyens Close,
Chineham Court, BASINGSTOKE,
Hampshire, RG24 8AG, United Kingdom

(51) INT CL:
G08B 13/08 (2006.01) ***G01S 13/87*** (2006.01)
G08B 13/24 (2006.01)

(52) UK CL (Edition X):
G4N NPL NPPXA1 NSBA NSBB

(56) Documents Cited:
GB 2279170 A **JP 2003303379 A**
US 6577238 B1 **US 20040150521 A1**

(58) Field of Search:
UK CL (Edition X) **G4N**
INT CL **G01S, G08B**
Other: **online: WPI, EPODOC**

(54) Abstract Title: **Security system with RFID tag reader**

(57) A security system monitors a number of entry point(s) each having an entry mechanism to gain access to an enclosed space 100. An RFID (radio frequency identification) tag 140 is located on a number of the entry mechanisms 110, 120, 130 to be monitored. A tag reader 115 is located within the space 100, such that when an entry mechanism 110, 120, 130 is in a closed state a tag 140 located thereon is located within a detection range of the tag reader 115. Conversely, when the entry mechanism 110, 120, 130 is in an open state the tag is located outside the range of the tag reader 115 and an alarm condition may be triggered. The tag reader 115 may be configured to communicate data via a wireless network.

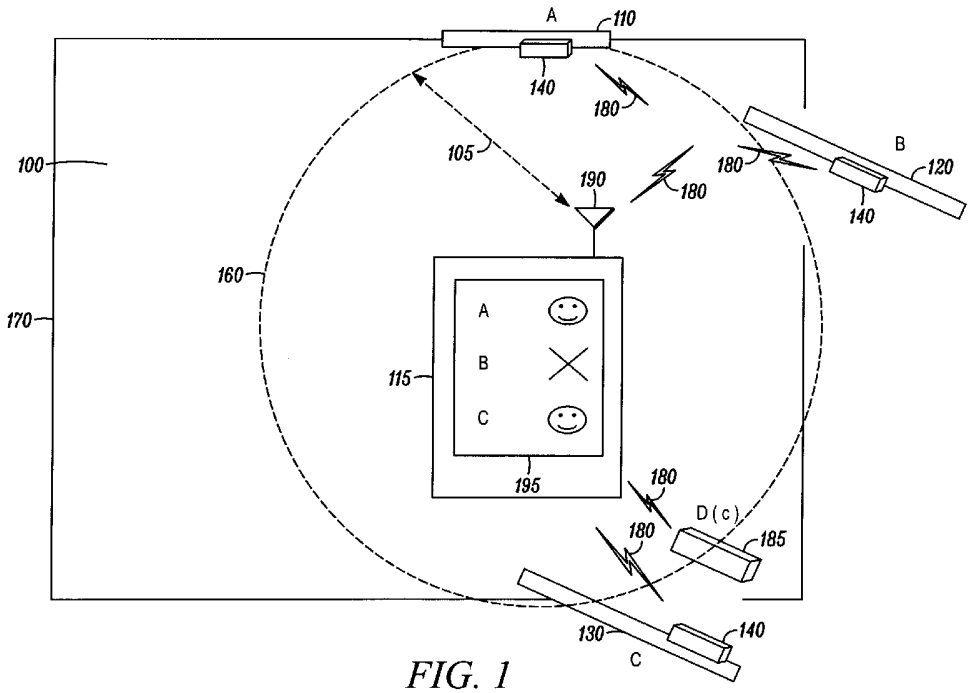

FIG. 1

GB 2 434 239 A

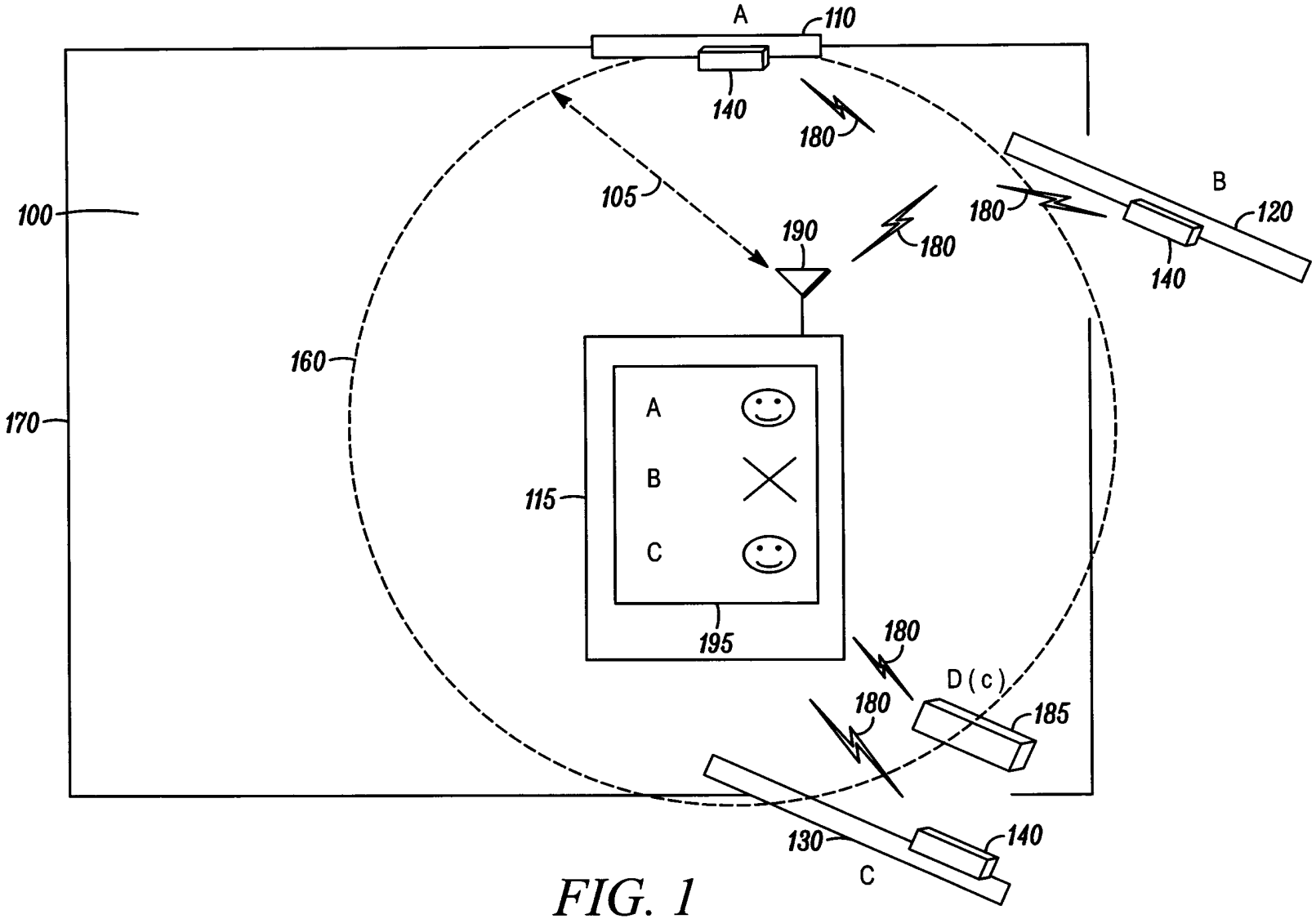
A
110
140
180
105
100
190
180
B
180
120
140
160
170
A
B
C
115
195
180
D(c)
180
185
130
140
C

FIG. 1

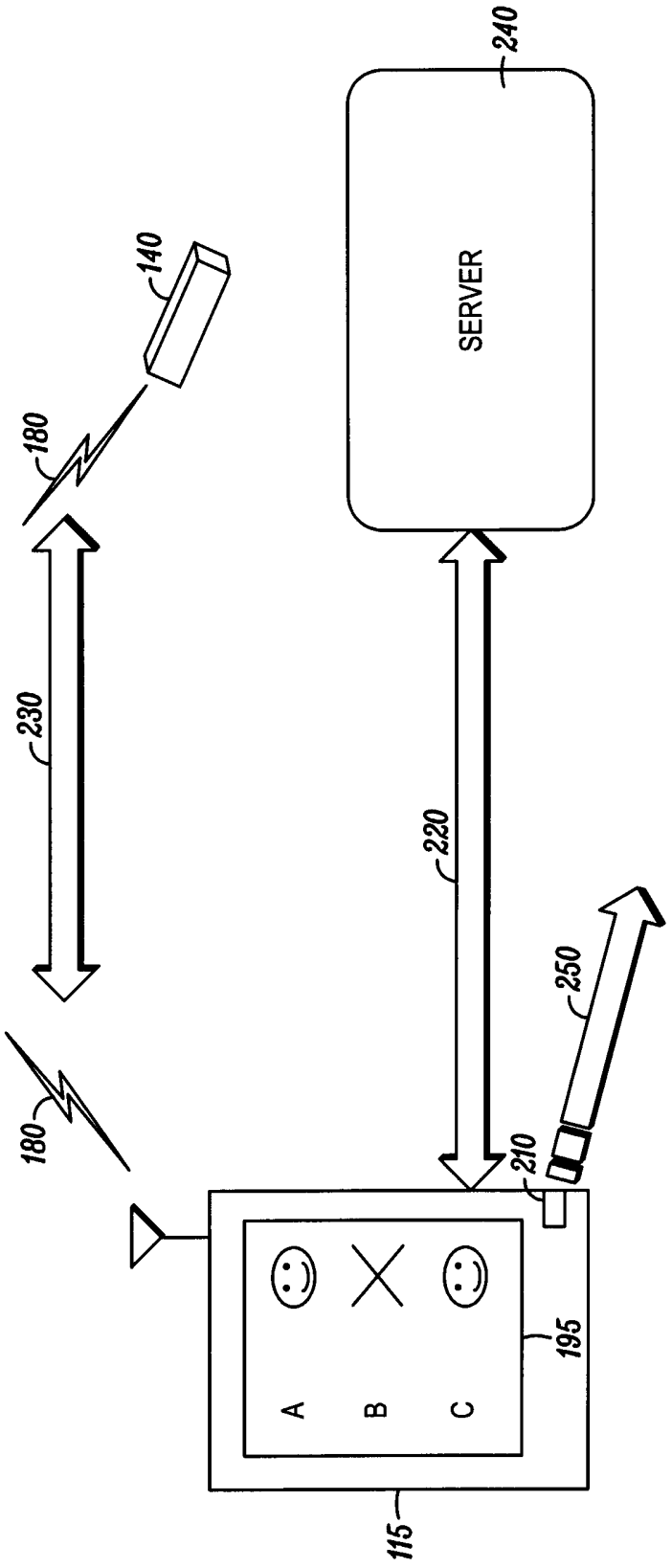

FIG. 2

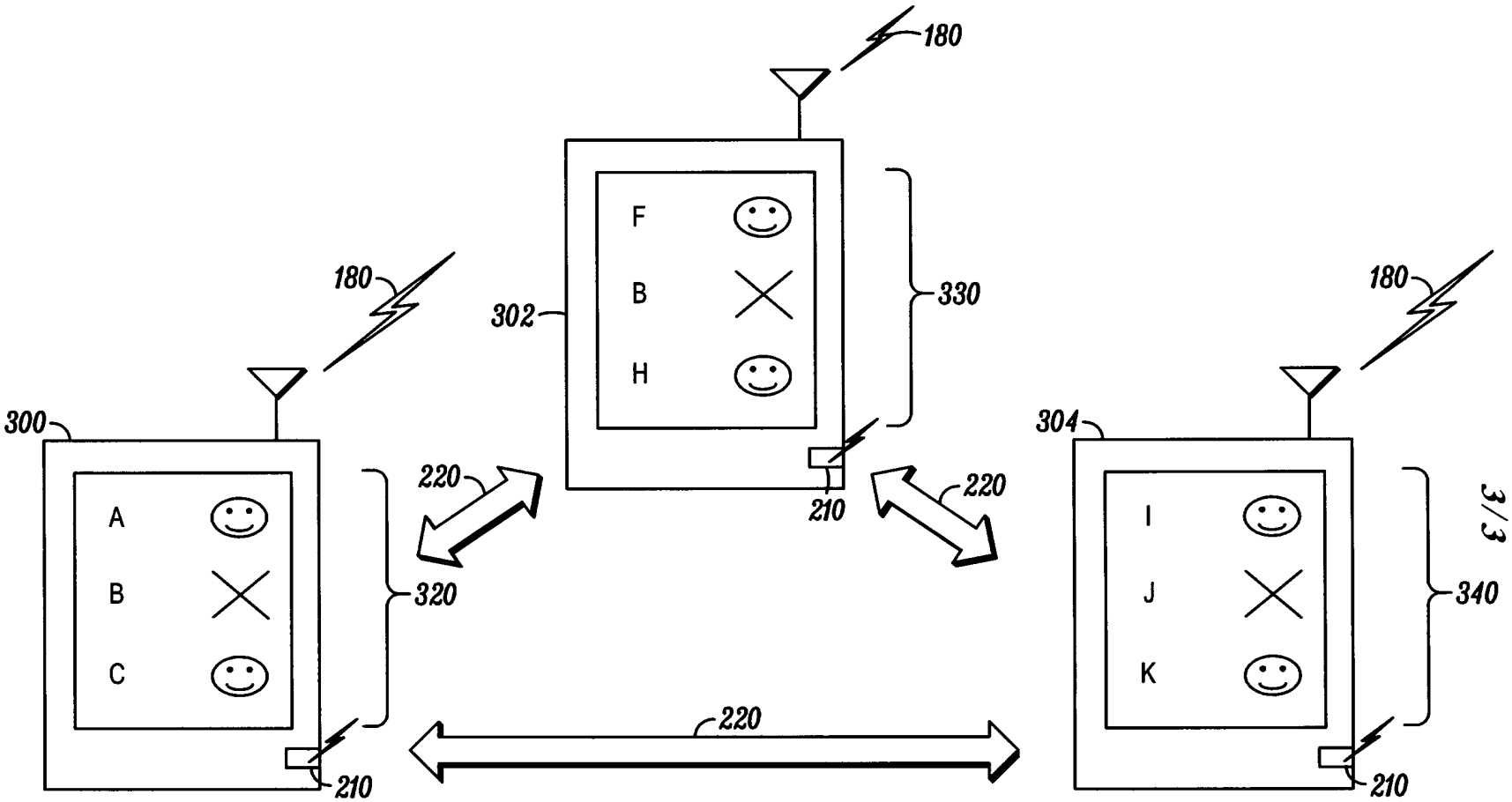
180
180
180
302
330
F
B
H
300
304
220
220
220
320
340
A
B
C
I
J
K
210
210
210
3/3

FIG. 3

SECURITY SYSTEM AND RFID TAG-READER THEREFOR

Field of the Invention

Embodiments of the present invention relate to a security system for monitoring access points to a protected, physically-enclosed space. The invention is applicable, but not limited to, monitoring of access points to living accommodation or working spaces, such as a building or an individual room, or to other spaces such as a control cabinet or a safe.

Background of the Invention

Security systems that are designed to protect against unauthorised ingress into a building, a room, a car or other enclosed space, are well described in the literature. An intrusion detection system designed for protecting a building or room typically employs a number of normally closed (N/C) or normally open (N/O) mechanical switches, or electromagnetic proximity switches. The switches are typically mounted directly to entry points, such as the frame of a door or a window, such that opening of the door or the window causes the switch to change state (i.e. close or open).

The individual switches are typically wired to a central control system or unit that monitors the state (i.e. open/closed) of each of the switches. The monitoring operation is often performed by measuring a resistance, a voltage or a current of a circuit.

This approach to security systems is well established, but far from fool-proof. Despite these drawbacks, such a system is still commonly in use, and has also been applied to the monitoring and protection of control cabinets in large radio systems. Some limitations of this type of security system include the following.

i) A mechanical switch is relatively easy to tamper with.

ii) The switch may simply fail, or worse, fail over time, resulting in random false alarms.

iii) A mechanical switch is costly. The costs include connectors at the switch and controller side, wires to and from the main controller, and of course, the cost of the switch itself.

iv) An alarm is triggered irrespective of the reason that the door or window is opened, and no matter who accessed the room or building.

v) If legitimate access is required, for example to service equipment via one of the protected entry points to the protected space, then the whole security system must typically be deactivated at the control unit.

Other more costly systems available on the market employ the concept of "zones" in order to break up a large system into smaller specific areas, each of which can be monitored individually, and some form of access cards or access keys are required to enter each zone. For such systems, card readers or key readers are also required and must be wired to the control unit for each zone. Accordingly, as stated above, these systems are even more costly. Moreover, they are complex to use and to install and also difficult to maintain.

Thus, a need exists for a flexible security system, capable of monitoring entry points to physically enclosed spaces such as, for example, a room, a building, or a control cabinet, whilst alleviating the problems associated with existing solutions.

Summary of the Invention

In accordance with a first aspect of the present invention, there is provided a security system, as claimed in Claim 1.

In accordance with a second aspect of the present invention, there is provided a RFID tag-reader device, as claimed in Claim 12.

In accordance with a third aspect of the present invention, there is provided a radio system base station cabinet, as claimed in Claim 18.

Further aspects and advantageous features of embodiments of the present invention are as described in the appended Claims.

Brief Description of the Drawings

Exemplary embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

FIG. 1 shows a schematic plan view of a cabinet, access to which is controlled by a security system according to one embodiment of the present invention.

FIG. 2 shows a schematic representation of communication between a RFID tag-reader, a RFID tag, and a central controller.

FIG. 3 illustrates a network of three RFID tag-readers communicating with each other.

Description of Embodiments of the Invention

Embodiments of the present invention will be described in terms of a security system for controlling access to a radio system control cabinet. However, it will be appreciated that the inventive concept may be embodied in any security system for controlling access to any physical space.

In the context of the present invention, the term 'radio frequency identifier (RFID)' used hereinafter is intended to encompass other technologies than strictly a 'radio frequency' based device. In this regard, RFID should be interpreted as encompassing any device that contains an identification code that is capable of being read over a short distance by means of radio communication, such as via optical communication or audio communication.

A security system is described for monitoring points of entry to a substantially physically enclosed space, each entry point having an entry mechanism with a defined closed and open state, physical motion of the entry mechanism being required to gain access to the space.

Advantageously, a RFID (radio frequency identification) tag is located on each entry mechanism to be monitored, with a corresponding tag-reader being located within the space such that, when the entry mechanism is in the closed state, the tag located on it is within the detection range of the tag-reader. When, however, the aforementioned entry mechanism is in the open state, said tag is, advantageously, outside the detection range of the tag-reader.

This beneficial arrangement of RFID tag and tag-reader is such that the act of opening the entry point to which the tag is attached, causes the tag to move outside the detection range of its associated tag-reader. This provides immediate information as to the actual state of the entry point, and thus provides the basis of a sophisticated intrusion detection system.

The tag-reader may be arranged to scan periodically, say at a pre-defined rate, for the presence of a corresponding tag. Thus, and advantageously, the rate at which the space is scanned by the tag-reader can be made inversely proportional to the expected time required to open the entry point to which the tag is attached. This matching of the sensor (RFID tag) sample rate to the dynamic characteristics of the entry point mechanism, saves electrical power, which is of great benefit in a battery powered system, but also reduces the computational load on, and thus the cost of, the tag-reader. In one embodiment, this is achieved by optimising the amount of data per period collected from the sensor or RFID tag.

In one embodiment, it is envisaged that when a tag goes out of range of a corresponding tag-reader, the tag-reader communicates this information to a further control system via a further communication interface of the tag-reader. Thus, the tag-reader is advantageously constructed with a communications interface that allows it to transmit data or information to a further control system or management system. This 'further' system may then process the data, thereby reducing the processing load on the tag-reader device.

In one embodiment of the present invention, when a tag goes out of range of the corresponding tag-reader, the tag-reader triggers an alarm via a further communication interface of the tag-reader. This advantageous capability allows a tag-reader to generate an alarm locally, whether the alarm is acoustic, optical, or otherwise. Thus, this embodiment reduces the dependence on the communications network for signalling a missing tag or other event.

In a yet further advantage of this embodiment, an access tag, capable of storing information readable by one or more tag-readers of the system, is provided for the purpose of modifying the behaviour of the tag-reader(s). This special class of tag, the 'access tag', carries a security code and/or other digital information readable by a tag-reader. This special class of tag may be carried, or worn, by someone wishing to access a space protected by the security system of the present invention. Use of access tags enhances the capabilities of security system, by allowing the behaviour of one or more tag-readers, and thus the behaviour of the entire

security system, to be modified in a predictable and defined way, as and when required.

In a yet further advantageous embodiment, an access tag contains a code which, when read by a tag-reader, disables one or more entry point monitoring functions of that reader. Thus, it is possible to create digital access rights to the space for whatever purpose may be necessary.

In an advantageous feature of one embodiment of the present invention each tag-reader contains a list of access, or security codes, and corresponding access rights. These codes are associated with specific tag-reader behaviours. An access code read from an access tag is compared with this list, and if a matching code is found, the behaviour associated with that code is adopted by the tag-reader. The list of access codes may also be stored on a remote server, to which the tag-reader has access via a communications interface, and be read from the server by the tag-reader when required.

A range of access codes, corresponding to a range of access rights or authorities, may easily be implemented, thus further extending and enhancing the capabilities of the security system.

Advantageously, the access-tag is continuously scanned by the tag-reader, the behaviour of the tag-reader being modified only during the time that the access-tag can be detected by the reader, the original behaviour being re-adopted once the access-tag can no longer be detected.

A RFID tag-reader, modified for use in the security system of one embodiment of the present invention is described. The tag-reader comprises, advantageously, a computing device capable of storing and executing at least one user-defined software program(s). The behaviours of the tag-reader are defined in the program(s), at least one of which can be modified as and when required, thus allowing the functionality or performance of tag-reader's to be updated via a firmware update if necessary.

In one embodiment of the present invention, the tag-reader comprises at least one communications interface capable of exchanging data with a further tag-reader or other remote computing device. This communication capability allows data to be shared within a network of tag-readers, as well as allowing configuration and reconfiguration of the tag-readers. This communication capability also allows updates and modifications to be carried out remotely.

Advantageously, the communication interface is a wireless interface, allowing all similarly equipped tag-readers to build an ad-hoc network and exchange data.

This networking capability allows redundancy to be built into the security system, by having, for example, two or three tag-readers monitoring one RFID-tag, whereby they can exchange information about the state of the tag.

In one embodiment of the present invention, the tag-reader is advantageously capable of accessing standard wireless communications networks and of transmitting data

in standard wireless network formats, such as short message service (SMS) messages or e-mail. This enables the tag-reader to directly and securely contact a specific person or persons via e-mail or SMS, as and when required.

In a further embodiment, the detection range of the tag-reader is programmable. This allows the RFID-tag and tag-reader to be quickly positioned in roughly the correct position within the space, and subsequently adjusted via a range feature menu, such that the opening of the entry point mechanism causes the tag-reader to lose communication with the RFID-tag once this range has been exceeded.

A radio system base station cabinet is described that incorporates the security system described in embodiments of the present invention. The cabinet comprises an RFID tag attached to an inside surface of at least one cabinet door, the corresponding tag-reader being located within the cabinet. Loss of contact with the RFID tag by the tag-reader causes the tag-reader to trigger an alarm or a data communication. A substantially simultaneous detection of a valid access-tag, or access code, causes the tag-reader behaviour to be modified accordingly.

The radio system cabinet can thus be monitored for unauthorised access or ingress, whilst at the same time, the same security system components and the same basic technologies can be used to provide only authorised persons with access to the cabinet, without triggering an alarm. This substantially reduces the complexity and cost of the system.

In an advantageous embodiment, the tag-reader communicates two alarm states "intrusion" and "service. Loss of contact with the RFID tag causes the state "intrusion" to be communicated. Any subsequent detection of an access-tag, say with valid access code, causes the alarm state to be changed from "intrusion" to "service". The associating of specific information, e.g. in this case "service", with an access tag, allows the tag-reader to communicate the action being undertaken by the authorised user, and not simply to inhibit a trigger of the intrusion alarm.

In this manner, the aforementioned problems associated with security systems have been alleviated whilst simultaneously alleviating the problems associated with the prior-art, are substantially resolved.

This has been achieved in one embodiment by the provision of a RFID tag-reader with a specified or adjustable detection range. A RFID tag is mounted to an entry point of the space to be monitored, and an access tag carrying a digital access code readable by the tag-reader, is used to modify the behaviour of the tag reader.

The teachings of the current invention are applicable to security systems for any physically enclosed space with entry points, to which access is occasionally required, examples of which are: a building, a room, a car, or a control cabinet as described herein.

Moreover, the above advantages are only exemplary. These or other advantages may be realized, and not all

advantages need be achieved by all embodiments of the inventions.

In FIG. 1 there is shown a space 100 in plan view, enclosed by a physical barrier (e.g. a container) 170 with entry points 110, 120, 130. This space could be a room within a building or house to which access is to be limited. In this case, the space 100 is a control cabinet for a large radio system, the entry points 110, 120, 130 being three doors allowing access to the cabinet. The cabinet is shown in plan view, as though a "picture" was taken from the ceiling looking down into the cabinet. The doors 110, 120, 130, shown in FIG. 1 swing open outwards, but could open inwards, or slide open in other embodiments.

In FIG. 1, doors 120 and 130 are shown in the open state, while door 110 is shown in the closed state. Each door 110, 120, 130 has affixed to it a RFID tag 140 shown transmitting a signal 180, the signals being monitored by a tag-reader 115 also located within the space. In one embodiment of the present invention, it is envisaged that the signals 180 that are transmitted from the RFID tags 140 may comprise standard radio signals that would be found in such a tag/tag reader arrangement, as known to those skilled in the art.

In one embodiment of the present invention, the RFID tags 140 store a serial number that identifies itself on a microchip that is attached to an antenna (the microchip and the antenna together are called an RFID transponder or an RFID tag). The RFID system consists of a number of RFID tags 140, made up of a microchip with an antenna,

and an interrogator or tag reader 115 with an antenna. The tag reader 115 sends out electromagnetic waves. The RFID tag antenna is tuned to receive these waves. Thus, a passive RFID tag 140 draws power from a magnetic field created by the tag reader 115 and uses it to power the microchip's circuits. The microchip then modulates the waves that the RFID tag 140 sends back to the tag reader 115 and the reader converts the new waves into a suitable format, such as digital data that can then be passed, for example, to a computer or processing unit that can make use of the information.

In one embodiment of the present invention, the RFID tags 140 may store other information, such as a version of the RFID tag or a set that the RFID tag belongs to.

The three door mounted tags 140 are labelled 'A', 'B' and 'C'. A further tag 'D'(c) 185, not fixed to any structure within the space, is also shown at entry point 130. Tag 'D'(c) is, in this case, an access tag, which is also shown transmitting a signal 180. The subscript (c) in FIG. 1 is employed simply as a means of indicating that access tag 'D', is in some way related to or linked with RFID-tag 'C' mounted to entry point 130.

The tag-reader 115 is shown having a display 195, and an antenna 190. Any further communication ports are omitted here for clarity purposes only. The dotted line 160, shown as a circle, with a radius 105 centred on the antenna of tag reader 115 in this example, illustrates schematically (in two dimensions) the detection range of the radio system of the tag-reader.

In one embodiment of the present invention, the communication between one or more tags 120, 130, 140 and the tag reader 115 comprises a radio communication link between, for example, a passive tag and a tag reader as is well known in the art.

The detection space of the tag-reader is, of course, a 3-dimensional space, defined by the characteristics of the antenna 190 and the strength of the magnetic field generated by the tag-reader 115. It is envisaged in other embodiments, that a tag-reader with a far more directional antenna could be used, in order to monitor a very specific space.

In the example of FIG. 1, the characteristics of the detection space of the tag-reader have been taken into account when locating it within the cabinet 100, resulting in a detection space defined by the circle 160.

The tag-reader 115 is shown wirelessly scanning 180 the space 100, at say, some pre-defined rate, e.g. once per second, checking for the presence of the three RFID tags 140. In the example in FIG. 1, doors 120 and 130 are open, and thus tags 'B' and 'C' are no longer within the detection space 160 of tag-reader 115. The tag-reader has thus, at some point in the past, lost contact with tags 'B' and 'C' due to the doors 120, 130 being opened. Tag 'A' is still within the detection space of the tag reader, and is being detected at each scan.

On the display of the tag-reader 115 there are shown icons corresponding to each of the entry point tags 'A', 'B', 'C', the tags being represented by letters on the

display. The icons corresponding to tag 'A' (smileys) indicate that this tag has been, or, more accurately, is being detected. Tag 'B' is clearly out of range of the tag reader i.e. outside the circle 160. The cross against tag 'B' indicates that this tag is out of range. In other implementations the cross may indicate that a tag is for some other reason not being detected.

Tag 'C' is clearly also out of range of the tag reader i.e. outside the circle 160. However, access tag D(c), is within the detection range circle 160, and this tag acts as a proxy for tag 'C', which is therefore indicated as a 'smiley' on display 195. Tag 'D'(c) contains an access code readable by the tag reader 115, the access code being able to function in a number of ways.

The access code may mimic tag 'C', i.e. be a clone of tag 'C', thus confusing the system into thinking that tag 'C' is still being detected. Alternatively, tag 'D' may contain an access code which, when decoded, instructs the reader to override the detection feature for tag 'C' at entry point 130.

In the example in FIG. 1, the former case is implemented, i.e. the reader interprets the signals as tag 'C' being in range, as it is still being detected, because tag 'D' is a clone of tag 'C'. In some embodiments, the latter case is more practically useful. In this case, the tag-reader would lose contact with tag 'C', and then shortly afterwards detect tag 'D', or perhaps simultaneously detect 'D' and 'C'. In either case, the access code read from tag 'D' causes the tag-reader to inhibit any alarm triggered by losing contact with tag 'C'. In one

embodiment the tag-reader displays a further icon to indicate that an override had occurred. The tag-reader may, if equipped with the necessary communication interface, take some further action, such as contacting a control centre or sending an SMS or e-mail, say to a predefined recipient.

Egress from the cabinet 100 of FIG. 1, for a service technician for example, would simply be the reverse of ingress. Here, we assume that a service technician with access rights granted by tag 'D', had entered the cabinet in order to service some piece of equipment, and was now again leaving the cabinet.

Tag 'C' may, when door 130 is again closed, move back into the detection space of the tag-reader 115 and be detected, and tag 'D' could move outside the detection space i.e. leave the cabinet with the service technician. Thus, the system provides automatic detection of multiple active states.

The access code programmed into access tag 'D' could, of course, contain much more information about the tag holder, and access rights that he/she has. These access rights could be communicated via the tag-reader 115 to a computer (not shown) of the security system, which would then modify the system access rights accordingly.

FIG. 2 shows schematically a tag-reader 115, with a first RFID radio interface 180, a second communication interface 210, and a display 195. In this case, the second communication interface 210 may be a further wireless interface, such as Blue-Tooth™ or WiFi™. The

tag-reader 115 is shown communicating with a remote device 240, and an associated RFID tag 140. The display 195 of the tag-reader 115 is showing the same information as the tag-reader 115 of FIG. 1, e.g. that tag 'B' can no longer be detected.

In one embodiment remote device 240 may be a remote computer, a server of some kind, or a further communication unit, such as a mobile phone or personal digital assistant (PDA). In the example of FIG. 2, the remote device 240 is a server providing computing resources to the security system.

The tag-reader 115 of FIG. 2 is shown transmitting 220 and 230 the current state of the security system to the server and, simultaneously transmitting 250 an SMS message to a registered user (not shown) of the security system. The tag-reader 115 may inform theses devices/units of the loss of contact with tag 'B'. This feature may be programmable by the user, and may be used to communicate any events that the user feels is important enough to warrant an e-mail or SMS message.

The schematic of FIG. 3 illustrates three tag-reader devices 300, 302, 304 with multiple communication interfaces 180, 210 all communicating with each other. A specific feature of the current invention is the ability of the tag-reader devices to form networks and to take part in peer-to-peer communications 220 on these networks. Tag-reader devices 300, 302 and 304 respectively include displays 320, 330 and 340, wherein each display shows the same information as the tag-reader

115 of FIG. 1, e.g. that tag 'B' can no longer be detected.

Each tag-reader device 300, 302, 304 may be able to locate other tag-readers via one or more of its wireless interfaces 180, 210, thereby creating a network, over which system security data, for example, can be shared between the tag-reader devices 300, 302, 304. In the example of FIG. 3, the tag-readers 300, 302, 304 have detected each other and have formed an ad-hoc network for sharing data with each other.

In one embodiment the network may also be used to allow one reader to access functionality available on a different reader. For example, tag-reader 300 may not have built in SMS capability, but may want to send an SMS. Thus, this tag-reader 300 may then query tag-readers 302 and/or 304 to determine if they offer such a service. If the queried tag-readers 302 and/or 304 do offer such as service, tag-reader 300 may request that the SMS be sent by one of them. Such a system also allows multiple tag-readers to monitor the same tag or tags to provide redundancy in detection, and/or a means of detecting reader errors. If, for example, three tag-readers monitored a tag 140, and one tag-reader declared the tag to be missing whilst the other two still detected the tag 140, then this would be a sign that the tag-reader that indicated a missing tag 140 was faulty.

Embodiments of the present invention are described in terms of a tag-reader with display and multiple communication interfaces. However, it will be appreciated by a skilled artisan, that the inventive

concept herein described may be embodied in any type of tag-reader capable of reading RFID tags.

It will be appreciated that any suitable distribution of functionality between different functional units or signal processing elements such as RFID tags, tag-readers, signal processing units, etc. may be used without detracting from the inventive concept herein described. Hence, references to specific functional devices or elements are only to be seen as references to suitable means for providing the described functionality, rather than indicative of a strict logical or physical structure or organization.

Aspects of the invention may be implemented in any suitable form including hardware, software, firmware or any combination of these. The elements and components of an embodiment of the invention may be physically, functionally and logically implemented in any suitable way. Indeed, the functionality of a tag-reader may, for example, be implemented in a single unit or IC, in a plurality of units or ICs or as part of other functional units.

In particular, it is envisaged that the aforementioned inventive concept can be applied by a semiconductor manufacturer to any RFID system. It is further envisaged that, for example, a semiconductor manufacturer may employ the inventive concept in a design of a RFID tag-reader and RFID-tag based security system, for protecting a control cabinet for a radio system.

Although the present invention has been described in connection with some embodiments, it is not intended to be limited to the specific form set forth herein. Rather, the scope of the present invention is limited only by the accompanying claims. Additionally, although a feature may appear to be described in connection with particular embodiments, one skilled in the art would recognize that various features of the described embodiments may be combined in accordance with the invention. In the claims, the term 'comprising' does not exclude the presence of other elements or steps.

Furthermore, although individual features may be included in different claims, these may possibly be advantageously combined, and the inclusion in different claims does not imply that a combination of features is not feasible and/or advantageous. Also, the inclusion of a feature in one category of claims does not imply a limitation to this category, but rather indicates that the feature is equally applicable to other claim categories, as appropriate.

Furthermore, the order of features in the claims does not imply any specific order in which the features must be performed and in particular the order of individual steps in a method claim does not imply that the steps must be performed in this order. Rather, the steps may be performed in any suitable order. In addition, singular references do not exclude a plurality. Thus, references to "a", "an", "first", "second" etc. do not preclude a plurality.

Thus, a security system comprising an RFID tag reader with a defined and/or selectable detection range, one or more RFID tags for detecting motion of an entry point mechanism, and a further access tag for use therewith, has been described, where the aforementioned disadvantages with prior art arrangements have been substantially alleviated.

Claims

1. A security system for monitoring a number of entry point(s) (110, 120, 130) having an entry mechanism to gain access to an enclosed space (100), characterised in that, a RFID (radio frequency identification) tag (140) is located on a number of entry mechanisms (110, 120, 130) to be monitored, a tag-reader (115) is located within the enclosed space (100) such that, when an entry mechanism (110, 120, 130) is in a closed state (110), the tag located thereon is further located within a detection range (160) of the tag-reader (115), and wherein when an entry mechanism is in an open state (140), the tag (140) located thereon is further located outside the detection range (160) of the tag-reader (115).

2. The security system of claim 1, further characterised in that the tag-reader (115) is arranged to scan periodically for the presence of a corresponding tag (140).

3. The security system according of Claim 1 or Claim 2 further characterised in that, when a tag (140) is located outside the detection range (160) of the tag-reader (115), the tag-reader (115) communicates (220) this to a control system (240) via a further communication interface (210) of the tag-reader (115).

4. The security system of Claim 1 or Claim 2 further characterised in that when a tag (140) is located outside the detection range (160) of the tag-reader (115), the tag-reader triggers an alarm condition.

5. The security system of any of the preceding Claims further characterised in that the tag-reader (115) modifies its behaviour in response to an access tag (140).

6. The security system of Claim 5, further characterised in that the access tag (140) contains a security code, which, when read by the tag-reader (115), disables the entry point monitoring function of that tag-reader (115).

7. The security system of Claim 5, further characterised in that the tag-reader (115) contains a list of security codes and corresponding access rights associated with specific tag-reader behaviours, compares an access code read from an access tag (185) with a list of security codes and access rights, and upon determining a matching code modifies its behaviour associated with that code.

8. The security system of any of preceding Claims 5 to 7, further characterised in that the access-tag (140) is continuously scanned by the tag-reader (115), the behaviour of the tag-reader (115) being modified during a time that the access-tag (140) is detected by the tag-reader (115).

9. The security system of any of preceding Claims 4 to 8 whereby the tag-reader (115) communicates alarm condition states, comprising at least one of:

(i) An intrusion condition;

(ii) A service condition.

10. The security system of Claim 9 further characterised in that a loss of contact with a corresponding RFID tag (140) causes the tag-reader (115) to communicate the intrusion condition.

11. The security system of Claim 9 or Claim 10 further characterised in that a subsequent detection of an access-tag (140) with a valid access code causes the alarm condition to be disabled.

12. An RFID tag-reader (115) modified for use in the security system of Claim 1.

13. The RFID tag-reader (115) of Claim 12 further characterised in that, the tag-reader (115) also includes a computing device capable of storing and executing user defined software programs, in which at least one behaviour of the tag-reader (115) is programmable by a user.

14. The RFID tag-reader (115) of Claim 12 or Claim 13, further characterised in that the tag-reader (115) comprises at least one communication interface (210) capable of exchanging data (220) with a further tag-reader (302, 304) or remote computing device (240).

15. The RFID tag-reader (115) of claim 14 further characterised in that the at least one communication interface (210) is a wireless interface and configured to support a tag-reader network (300, 302, 304) for the exchange of data (220).

16. The RFID tag-reader (115) of any of preceding claims 12 to 15 further characterised in that the tag-reader (115) is arranged to access a standard wireless communication network and of transmitting data (250) in a standard wireless network format.

17. The RFID tag-reader (115) of any of preceding Claims 12 to 16, further characterised in that a detection range (160, 105) of the tag-reader (115) is programmable.

18. A radio system base station cabinet (100) incorporating the security system of Claim 1.

19. A security system substantially as hereinbefore described with reference to FIG. 1 of the accompanying drawings.

20. A RFID tag-reader (140) substantially as hereinbefore described with reference to FIG. 1 or FIG. 2 or FIG. 3 of the accompanying drawings

21. A radio system base station cabinet (170) substantially as hereinbefore described with reference to FIG. 1 of the accompanying drawings

The Patent Office

For Innovation

25

Application No: GB0600553.2 **Examiner:** Rhiannon Jenkins

Claims searched: All **Date of search:** 14 March 2006

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X,Y	X: 1-4, 9, 10 & 12-18 Y: 5-8 & 11	US 6577238 B1 (TAGTEC LTD) - See figures 1 & 4, column 1 line 53 to column 2 line 26 and column 4 line 24 to column 6 line 49
Y	5-8 & 11	JP 2003303379 A (SANRIKKUSU KK) - See figure 6 and EPO & WPI abstracts
A	-	US 2004/0150521 A1 (STILP) - See figure 1 and paragraphs 34 & 35
A	-	GB 2279170 A (NEWTON T) - See pages 1 & 2

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category	P	Document published on or after the declared priority date but before the filing date of this invention
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

G4N

Worldwide search of patent documents classified in the following areas of the IPC

G01S; G08B

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC