

16 FEB 2000

Electronic locking and monitoring system and method for arming or disarming intruder detection and/or status reporting systems

The invention is an electronic locking and monitoring system and a method of arming or disarming intruder detection and/or status reporting systems, according to the main terms of patent claims 1 and 14.

Field of the Invention

Customer identification in service systems using credit cards, key fobs, badges and other screw-on, flat circular disks is one of the principal applications of wireless code recognition.

Wireless chip cards are described in publications including DE OS 42 27 551, DE OS 42 39 806, DE OS 42 42 112, DE OS 43 02 387 and DE OS 43 37 921.

Power is supplied and data transferred using antennas in the reader device and in the card. These solutions also incorporate special data security measures while writing to or reading from the non-volatile memory in the card.

DE OS 40 03 212 and DE OS 43 27 342 describe industrial applications for identifying goods or the containers they are transported in.

In DE OS 43 27 342 mobile data carriers are attached to re-usable containers for transporting goods. The data carrier contains at least one device for transmitting and receiving data via electromagnetic waves to or from an external station, as well as a non-volatile memory which is connected to the transmitting and receiving device and connected to control circuits. This is designed for writing and reading data. The data carrier is enclosed in a thin, hermetically sealed, roughly rectangular housing. A bag made of an elastic material such as plastic, which can be opened at its narrow top side, is attached to the outside of the transport container. The data carrier is placed in this bag.

DE OS 40 03 212 contains a system for identifying unit goods. The data carrier contains a surface with areas of differing permeability. An external reader head consists of a large number of magnetic sensors arranged in a matrix, can detect the magnetic permeability of the partial areas. Thus, a writeable and readable code carrier is arranged in or on the product. No reference is made to the power supply for these solutions.

Cards which are read in direct contact using a reading device are described in many different publications. Such cards with fixed or externally definable data are in wide use today.

The publications DE 39 28 107 (procedure for coding and availability of a chip card) and DE 40 12 931 (procedure and system for individual electronic identification of badges) describe complete systems including the cards. In these cases the identity of cards is tested using a mother card or pre-programmed badges. The cards also possess a temporal validity limit. If such cards are lost before the validity date expires, it is very difficult to modify the reading system. Unauthorised persons are able to use these cards for a relatively long period of time.

DE 40 25 229 (coding system) describes a system where one card can be used for several readers. The number of cards can be restricted for the cardholder. The user can program several identification parameters himself. However, if a card is lost, the reading system can also only be modified with considerable difficulty.

Especially with respect to the individually programmable parameters there is a great security deficit when cards are lost. The reference to an additional comparison of stored personal features substantially increases the complexity and therefore the cost of the reading system.

The invention stated in patent claims 1 and 14 is based on the problem of creating an electronic locking and monitoring system which can be activated using transponders and a method of arming and disarming intruder detection and/or status reporting systems.

Description of the Invention

The features described in patent claims 1 and 14 solve this problem.

The particular characteristic of the invented electronic locking and monitoring system is that the activation (arming) and deactivation (disarming) of intruder detection and/or status reporting systems, particularly alarm systems, consists of two consecutive two steps using a data carrier. The first step tests whether the locking components are activated and properly locked and/or whether the sensors are functioning properly. If the result of the first step is positive, the second step takes place, namely the arming of an alarm system as an intruder detection and/or status reporting system. This prevents the alarm system from being armed if the blocking elements and/or sensors are not functioning properly and therefore in an open or faulty state.

The alarm system is only armed or disarmed after a consecutive double check and comparison of the data on at least one data carrier. This improves security against unauthorised operation of the locking or monitoring system.

Useful additions to the invention are described in patent claims 2 to 13.

Patent claim 2 describes a configuration where the switching module is spatially offset from the reader device, therefore making unauthorised use of the intruder detection and/or status reporting system, especially in the form of an alarm system, substantially more difficult, and thereby increasing security.

In this version the switching module of the intruder detection and/or status reporting system is mounted inside the secured area and the reader device is outside. Data is transferred on one data line only, thus further increasing the security of the electronic locking and monitoring system.

The additions described in patent claims 3 to 5 create a contact-free electronic locking and monitoring system. This increases security against misuse by unauthorised persons. The opportunity to tamper with the system has been practically eliminated, thus guaranteeing the highest possible standards of security. The intruder detection and or status reporting system is armed and disarmed, and authorisation data is programmed using at least one passively coded authorisation card, a passive programming card and a passive delete card which are all supplied as transponders, thus facilitating touch-free operation. The cards are powered using an LC oscillator in the reader. The transponders themselves are passive and are therefore always ready for operation. Malfunctions due to insufficient power supply cannot occur.

The different types of card provide the user with a sophisticated locking and monitoring system. All tasks, most importantly the system set-up and the authorisation of users, take place on site and can be carried out by the operator himself. A passive programming card is used to store the data of the user cards in the reader device's memory on site. This has the advantage that the operator only needs a limited number of user cards. If more user cards are required at a subsequent time these can be easily authorised at the reader device by switching it to programming mode.

The result is that the system can be used universally and no time is lost through having to reprogram the system. The operator can perform the programming himself on site, so that the cost of calling in the manufacturer's engineers is eliminated. The reader device is also characterised by the fact that a passive delete card can be used to immediately delete all data in the memory. This facilitates universal and economical use of the locking and monitoring system.

Patent claim 7 describes an additional feature by which an active delete card can be used to delete the authorisation data of individual cards from the reader memory on site. These days it is easily possible that cards are lost, given the ever increasing number of cards used for different applications. This means that unauthorised persons can use access intruder detection and/or status reporting systems if they come into possession of cards.

With the system expansion described here, the card's authorisation can be revoked on site as soon as its loss is discovered. In this way, staff are more forthcoming to report the loss of authorisation card, since the correction entailed is much quicker and cheaper.

The operator can also extend or restrict authorisations due to changes in the company structure with a minimum of undue effort. Unnecessary costs due to the installation of new readers or reprogramming by the manufacturer are no longer incurred. No time needs to be wasted by having to replace all the user cards.

The addition described in patent claim 8 of two potential-free keypad buttons for selecting the operating mode of the active delete card guarantees extremely low power consumption while the delete card is inactive.

The additions described in patent claims 9 and 10 facilitate contact-free recording of the data on both passive and active cards. The addition in patent claim 10 uses a single coil for both transmitting and receiving data, which means that the reader device is less complex, thus providing the advantage of reduced power supply.

With an intelligent module spatially offset from the reader device and an encrypted data transmission procedure, the addition described in patent claim 11 provides increased security. Tampering is practically impossible, so that no unauthorised persons are able to get into the secured area.

The additions describes in patent claims 12 and 13 are improved designs for the control layout, circuitry and switching elements.

Examples and Drawings of the Invention

The example of the invention is illustrated in the drawings and will therefore not be described in further detail here:

Fig. 1 - Theoretical structure of the electronic locking and monitoring system

Fig. 2 - Block diagram of the active delete card

The following example application describes in detail an electronic locking and monitoring system for at least one locking mechanism and one control and/or alarm mechanism and a method of arming and disarming intruder detection and/or status reporting systems with connected blocking elements and/or sensors.

The electronic locking and monitoring system for at least one locking mechanism, and at least one control and/or alarm mechanism, consists of at least one data carrier, a reader device (2) for data carriers, a switching module (3) and an armable intruder detection and/or status reporting system, in particular an alarm system (4) (Illustrated in Fig. 1).

The data carriers take the form of transponders (1).

The reader device (2) for transponders (1) essentially consists of a reader, a memory (10) for the transponder (1) data, a control device in the form of a microcomputer (9) and various display devices. The reader device (2) is connected to the offset switching module (3) via a serial data line (11). The switching module (3) consists of two switching elements in the form of two relays (12a and 12b), and a microcomputer (13) as controller.

In addition, the switching module (3) possesses several inputs (14) for connections to monitoring devices. With the relay (12a) and the alarm system (4) the following takes place:

- Firstly a test that all access points, such as doors and windows, and any other locking systems are properly locked
- Secondly the activation of the blocking elements
- Thirdly the status test for the blocking elements

The second relay (12b) is used for arming the alarm system (4) connected to the switching module (3). One input is used to detect whether the alarm system (4) is ready for arming and the other input is used for setting the switching mode.

The following section describes in more detail how the switching module (3) functions with respect to the reader device (2) in more detail by showing how the arming and disarming of the alarm system (4) is effected.

Arming

The alarm system (4) of the invented electronic locking and monitoring system is disarmed, which means that the alarm system is not activated and the blocking elements are open.

First, all access points, such as doors and windows, and locking systems are closed and locked. Then a transponder (1) authorisation card is presented to the reader device (2) and the reader records the data on the transponder (1). If the data on the transponder (1) corresponds to the data held in the memory (10) of the reader device (2), the reader device (2) emits an acoustic and/or visual signal using one or more of its display devices.

At the same time, the electronic locking and monitoring system is blocked. This condition and therefore the fact the alarm system (4) is ready for arming is then signalled. During a set time period the transponder (1) must now be presented a second time to the reader device (2). After another signal by the microcomputer (13) on the switching module (3) an instruction is sent via the serial data line (11) to switch on the first relay (12a).

The alarm system (4), which is connected to the switch contacts of the first relay (12a) then tests whether all access points, in the form of doors and windows, and locking systems are properly locked and that the blocking elements are activated. If the result of this test is positive a signal that the system is ready for arming is sent to the input of the switching module (3). Then the second relay (12b) is switched on by the microcomputer (13) and the alarm system (4) is armed.

Disarming

The alarm system (4) is armed. If a transponder (1) authorisation card is then presented to the reader device (2), the data on the transponder (1) is checked against the data in the memory (10). If the result is positive there follows an indication signal of the status of the alarm system (4). After a set period there follows a signal that the system is ready to be disarmed. If, during a set time period, a second positive reading of the data on the transponder takes place, an instruction is sent via the serial data line (11) to the microcomputer (13) of the switch

module (3) to switch on the second relay (12b). After a set interval the first relay (12a) is also switched on and the alarm system (4) is disarmed.

Arming in the event of a fault

The alarm system (4) is disarmed, which means that the alarm system (4) is not activated and the blocking elements are open. First, all access points, such as doors and windows, and locking systems are closed and locked. Then a transponder (1) authorisation card is presented to the reader device (2) and the reader records the data on the transponder (1). If the data on the transponder (1) corresponds to the data held in the memory (10) of the reader device (2), the reader device (2) emits an acoustic and/or visual signal using one or more of its display devices.

At the same time, the electronic locking and monitoring system is blocked. This condition and therefore the fact the alarm system (4) is ready for arming is then signalled. During a set time period the transponder (1) must now be presented a second time to the reader device (2). After another signal by the microcomputer (13) on the switching module (3) an instruction is sent via a serial data line (11) to switch on the first relay (12a).

The alarm system (4), which is connected to the switch contacts of the first relay (12a) then tests whether all access points, in the form of doors and windows, and locking systems are properly locked and that the blocking elements are activated. If the result of this test is negative there is no signal that the system is ready for arming. The second relay (12b) is not switched on and the first relay (12a) falls off again and unlocks the access points and locking systems.

In the event of manipulation of the reader device (2) by drilling, electric shocker, short-circuiting or cutting the wires, the condition of the relays (12a and 12b) is not changed if the alarm system (4) is armed.

As well as the transponder (1) authorisation cards the locking and monitoring system can also comprise of at least one passive programming card, a transponder (1) passive delete card and an active delete card (15).

The reader for contact-free recording of the data on the transponder (1) authorisation cards works by induction and consists of an LC oscillator (5) as a sine wave generator and of a series connection with a demodulator (6), a selective amplifier (7) a comparator (8) and a microcomputer (9) with a memory (10). The oscillator frequency is $125 \text{ kHz} \pm 5\%$.

The transponder (1) is powered contact-free via the LC oscillator (5) in the reader. The coil of the oscillator (5) is connected to the input of the demodulator so that it functions both for the power supply to the transponder (1) and as a receiver coil for data.

Before the system is first set up or after the memory in the reader device (2) is completely wiped the memory (10) of the reader device (2) is empty. If at least one passive programming card is presented, in other words held within the transmitting and reading range of the LC oscillator (5) the microcomputer (9) of the reader device (2) switches to programming mode. The required encoded transponders (1) can then be presented consecutively to the reader device (2) and authorised as user cards. The data on these transponders (1) is then stored in the memory (10) of the reader device (2). When the passive programming card is presented to the reader (2) again, the microcomputer (9) of the reader device (2) switches back to normal operating mode.

Additional encoded transponders (1) can be stored in the memory (10) of the reader device (2) as authorisation cards at any time by simply presenting the passive programming card. In this way the number of authorised users can be expanded by the operator himself.

All transponders (1) stored as authorisation cards can be deleted immediately using the passive delete card. This resets the system to its original condition and the reader device (2) can continue to be used.

A further advantage can be achieved by using the active delete card (15), the principle of which is illustrated in Fig. 2. The active delete card (15) consists of a housing containing a keypad (16), a visual display (17) a component board and a space for at least one chemical power source (29) in the form of at least one battery, which can be externally sealed.

The operating mode of the active delete card (15) can be selected using two buttons on the keypad (16).

When the active delete card (15) is switched on and held within the transmitting and receiving range of the reader device, the visual display (17) on the active delete card (15) displays instruction menus. Data is exchanged between the reader device (2) and the active delete card (15) via the LC oscillator (5) in the reader device (2) and a transmitting oscillating circuit (19) in the active delete card (15). A microcomputer (18) with an integrated memory in the active delete card (15) controls the electronic modules and therefore all necessary processes. It enables the operator to enter the individual codes of encoded transponders (1) as authorised cards using the keypad (16), which are then deleted from the memory (10) of the reader device (2).

The microcomputer (18) with its integrated memory is connected to the keypad (16), the visual display (17) and the transmitting oscillating circuit (16) (Fig. 2). The keypad has several buttons:

- Numerical buttons for entering the code
- A potential-free ON button, so that the power consumption in idle mode is in the nA-range
- A button for correcting the code entry
- A button for confirming and initiating deletion of the code from the memory (10) of the reader device (2)
- Buttons for scrolling back and forth in the memory (10) so that several card numbers to be deleted can be entered and stored in the active delete card (15)

The last button mentioned is especially useful when several locking and monitoring systems are in use and a particular group of cards are to be deleted from all systems.

The power supply comes from two lithium cells ensuring a long operational life.

When the alarm system (2) is armed the reader device (2) cannot be put into programming mode using the passive programming card or the active programming card (15), so that no additional data can be read in. The same naturally applies to the delete card.



Claims:

1. Electronic locking and monitoring system for at least one locking mechanism, one control and/or alarm mechanism with a reader device for data carriers with (A) a reader for the data on at least one data carrier, a control system, display devices and a memory for the data on at least one data carrier; and (B) at least one armable intruder detection and/or status reporting system, in particular an alarm system; with connected blocking devices and/or sensors; and (C) at least one data carrier. The system is characterised by the fact that the reader device (2) is connected via a data line (11) to a switching module (3), and that the switching module (3) behaves as follows:

When the intruder detection and/or status reporting system is not armed, two separate, consecutive comparisons between the data on one or more data carriers and the data in the memory (10) of the reader device (2) take place. If both comparisons are positive, the first switching element is activated and there then takes place a test of the condition of the blocking elements, sensors and/or of the intruder detection system. If this is positive the second switching element is activated.

When the intruder detection and/or status reporting system is armed, two separate, consecutive comparisons between the data on one or more data carriers and the data in the memory (10) of the reader device (2) take place. If both comparisons are positive, the second switching element is activated, which causes the first switching element to be activated.

The invention is also characterised by the fact that the contacts of the switching elements are connected to the intruder detection and/or status reporting system via data lines.

2. Electronic locking and monitoring system as defined in claim 1, characterised in that the switching module (3) and the intruder detection and/or status reporting system is located inside the secured area and the reader device (2) is located outside the secured area.
3. Electronic locking and monitoring system as defined in claim 1, characterised in that the data carriers are transponders (1) and that the transponders (1) are at least one encoded authorisation card, a passive programming card and a passive delete card.



4. Electronic locking and monitoring system as defined in claim 3, characterised in that there is a memory (10) in the reader device (2) which can be switched to programming mode using the passive programming card and then programmed with the data on a number of encoded authorisation cards.
5. Electronic locking and monitoring system as defined in claim 3, characterised in that there is a passive delete card which can completely delete all transponder (1) data from the memory (10) of the reader device (2).
6. Electronic locking and monitoring system as defined in claim 3, characterised in that there is at least one active delete card (15) that can delete selected data from the memory (10) in the reader device in programming mode.
7. Electronic locking and monitoring system as defined in claim 3, characterised in that the active delete card (15) for deleting individual card data contains a keypad (16) with function buttons, a display (17) for visual representation of the menu and a transmitting oscillating circuit, all connected by a memory and processing circuitry.
8. Electronic locking and monitoring system as defined in claim 7, characterised in that two potential-free keypad (16) buttons for selecting the operating mode.
9. Electronic locking and monitoring system as defined in claim 1, characterised in that the reader consists of an LC oscillator (5) as a sine wave generator and a serial circuit with a receiver coil, a demodulator (6), a selective amplifier (7) and a comparator (8).
10. Electronic locking and monitoring system as defined in claim 1, characterised in that the reader consists of an LC oscillator (5) as a sine wave generator and a serial circuit with a receiver coil, a demodulator (6), a selective amplifier (7) and a comparator (8) and that the coil of the LC oscillator (5) is simultaneously connected to the input of the demodulator (6).



11. Electronic locking and monitoring system as defined in claim 1, characterised in that the reader device (2) is connected via a data line (11) carrying encrypted data with the switching module (3).
12. Electronic locking and monitoring system as defined in claim 1, characterised in that the control system and switches are microcomputers (9,13)
13. Electronic locking and monitoring system as defined in claim 1, characterised in that the switching elements are relays (12a, 12b).
14. Method of arming or disarming intruder detection and/or status reporting systems with connected blocking devices and/or sensors especially as described in patent claim 1, characterised by the following:

When the intruder detection and/or status reporting system is not armed and the blocking elements are closed, there take place two separate, consecutive comparison of the data on at least one transponder and the data in the memory. If both comparisons are positive the first switching element is activated. There follows test of the condition of the blocking elements and/or of the intruder detection system. If this is positive a second switching element is activated;

When the intruder detection and/or status reporting system is armed and the blocking elements are closed, there take place two separate, consecutive comparison of the data on at least one transponder and the data in the memory. If both comparisons are positive the second switching element is activated. This causes the first switching element to be activated and the intruder detection and or status/reporting system is disarmed.