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

(11) **EP 2 011 093 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
20.06.2018 Bulletin 2018/25

(21) Application number: **07751528.6**

(22) Date of filing: **23.02.2007**

(51) Int Cl.:
G08B 13/00 *(2006.01)* ***G08B 19/00*** *(2006.01)*
H04N 7/18 *(2006.01)* ***G08B 1/08*** *(2006.01)*
G08B 13/196 *(2006.01)*

(86) International application number:
PCT/US2007/004773

(87) International publication number:
WO 2007/111802 (04.10.2007 Gazette 2007/40)

(54) SECURITY MONITORING WITH PROGRAMMABLE MAPPING

SICHERHEITSÜBERWACHUNG MIT PROGRAMMIERBAREM MAPPING

SURVEILLANCE DE SECURITE PAR MISE EN CORRESPONDANCE PROGRAMMABLE

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

(30) Priority: **24.03.2006 US 388764**
24.03.2006 US 785570 P
24.03.2006 US 389673

(43) Date of publication of application:
07.01.2009 Bulletin 2009/02

(73) Proprietor: **RSI Video Technologies, Inc.**
Vadnais Heights, MN 55110 (US)

(72) Inventors:
- **JENTOFT, Keith**
Circle Pines, MN 55014 (US)
- **REIBEL, Jean-Michel**
F-67200 Strasbourg (FR)

(74) Representative: **Chiva, Andrew Peter**
Dehns
St Bride's House
10 Salisbury Square
London
EC4Y 8JD (GB)

(56) References cited:
WO-A1-01/27763
WO-A2-2006/017402
GB-A- 2 382 485
US-A- 5 473 368
US-A1- 2005 162 268
US-B1- 6 501 502
US-B1- 6 504 479

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 2 011 093 B1

Description

FIELD OF THE INVENTION

[0001] The present invention is directed to a security arrangement and method for monitoring the inside of a facility or residence.

BACKGROUND

[0002] Home, office and other building-security systems are often used for safeguarding valuable possessions and for personal protection. These systems are typically implemented using different monitoring devices, such as cameras, motion sensors, keypads or contact sensors. Many buildings have multiple locations that are monitored for security purposes, requiring multiple monitoring devices in the different locations. For increased security and functionality, the monitoring devices can be configured to communicate with one or more central control devices. The central control device can, among other things, perform monitoring or recording functions, determine whether the building-security has been breached and whether to contact security personnel.

[0003] One method of communicating between the monitoring devices and the central control device is by a physical connection, such as electrical or other wiring. Using wiring to establish communication between the security devices can be troublesome for a number of reasons, such as the high cost of installation and maintenance. For example, exposed wiring is often unacceptable in a building, and thus, the installation of the security system requires passing the wires through the walls of the building. This type of installation can significantly increase the time required-to-oomplete a security system installation. Moreover, the troubleshooting and repair of the security system can be difficult because there is limited access to the unexposed wiring. The cost of the wire is another factor, especially in large buildings requiring numerous monitoring devices.

[0004] One potential solution is to use wireless monitoring devices to reduce or eliminate the need for physical connections between the devices, however, wireless security systems also have a set of problems, such as battery life. Ideally, the security devices would be self-powered by, for example, a battery. Self-powered devices are more secure because they are not subject to failure upon loss of power to the building. They also require less installation problems because they do not need to be connected to a separate power source; however, self-powered devices often have reliability issues due to the finite life of their power source. Increasing the useable time of a power source reduces the cost for replacement of the power source and increases the security of the entire system by having less potential downtime of the system or its components. Several recent developments have increased the potential power requirements of wireless security devices.

[0005] For example, the use of wireless communications in home, office and other buildings has been steadily increasing, creating additional issues with wireless security systems. One such issue is the increased potential for corrupted data due to interference between different wireless communications devices. This issue may also be present when an unauthorized person attempts to disrupt the security system by "jamming" the wireless communications using a wireless interference device. Techniques exist for reducing unwanted interference, however, the implementation of some of the techniques result in increased power requirements. Two such techniques, both of which can result in increased power requirements, include increasing the power of the transmission or varying the frequency of the transmission.

[0006] Another problem with power requirements arises from the desire to have increased monitoring capabilities with smaller devices. As security systems become more advanced, the power requirements of the monitoring devices are often increased. For instance, monitoring devices that contain digital cameras require enough power to run the camera, to store the digital picture in memory and to transmit the digital picture to the control device. The increased functionality of the monitoring devices, along with the desire to have smaller, less noticeable devices with less room for batteries or other power sources, has impacted the reliability of the monitoring devices.

[0007] Implementing a wireless building-security system can be further complicated by industry or government regulations. One such set of regulations is imposed by the Federal Communications Commission (FCC). The current regulations cover numerous aspects of wireless communications systems including, but not limited to, a range of restricted frequencies, a minimum number of different hopping frequencies within the allowable frequencies, the maximum output power of a transmitter and a requirement related to equal use of the hopping frequencies.

[0008] Attempts have been made to implement wireless security systems using a variety of methods. One such method is taught by European Patent Application Publication No. EP 1 363 260 filed on May 6, 2003, entitled "Procédé de communication radiofréquence entre plusieurs dispositifs et système de surveillance mettant en oeuvre un tel procédé." Yet, there methods still leave room for improvement.

[0009] In order to protect residents, employees, personal property, and the like, security monitoring systems are used to monitor a variety of facilities and to sense the presence of unwanted intruders. Many such security systems are connected to a central control unit and monitored by an operator who can alert the appropriate emergency services in the event of an unwanted intruder. Typically, a home monitoring security system includes a combination of sensing devices and alarm devices and some also include cameras. To achieve the maximum monitoring coverage, these devices are distributed throughout the interior of the facility.

[0010] Security systems that employ cameras are advantageous in that they are able to record activity associated with a suspected breach of the facility and also can be used by a monitoring station to prevent false alarms. In some instances, however, the cameras record the regular activities of the facilities' residents and/or employees. The cameras also record activities that are falsely perceived to be security breaches such as pet behaviors and authorized users that have been accidentally locked out.

[0011] In specific situations, such as those having the potential to violate the privacy of authorized residents and/or employees of the facility, such comprehensive recordation by the security cameras may be undesirable. Since unwanted intrudors could breach the security of a facility while the inhabitants are present, it is necessary for the security monitoring system to be functioning at all times. However, having cameras constantly being triggered to record the inhabitants' daily living and working routines is a dramatic invasion of the inhabitants' privacy, and is burdensome with respect to false triggers. Further, the monitoring and recording of guests' activities can be just as invasive.

[0012] Moreover, the installation and configuration of the various cameras and devices often requires complex and time-consuming installation procedures.

[0013] US 2005/0162268 discloses a video surveillance system, wherein at least one sensor condition defines an alarm state for each camera.

[0014] The above-discussed issues have presented challenges to developing a home and/or facility security monitoring system that provides maximum coverage while minimizing one or more of the above-identified issues.

SUMMARY

[0015] The present invention is directed to the above and related types of integrated security systems.

[0016] The present invention provides an integrated security arrangement as claimed in claim 1.

[0017] The present invention also provides an integrated security arrangement as claimed in claim 11.

[0018] In an embodiment of the present invention, an integrated security arrangement includes an intrusion sensor to detect an intrusion, a plurality of motion sensors, and a plurality of image-capture devices. Each of the image-capture devices is responsive to a respective one of the motion sensors and when the image-capture devices are enabled they capture images of respective target areas in response to movement in the respective target areas as indicated by the respective motion sensors. The integrated security arrangement also includes a mapping database that contains data used to associate one or more of the plurality of image-capture devices with the intrusion sensor. The mapping database is configurable by a user. The integrated security arrangement further includes a control unit that enables one or more of the plurality of image-capture devices in response to the intrusion sensor detecting an intrusion. The control unit determines whether to enable one or more of the image-capture devices based upon data in the mapping database.

[0019] The above summary of the present invention is not intended to describe each illustrated embodiment or every implementation of the present invention. The figures and detailed description that follow more particularly exemplify these embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] The invention may be more completely understood in consideration of the detailed description of various embodiments of the invention in connection with the acoompanying drawings, in which:

FIG, 1 depicts a building-security system according to an example embodiment of the present invention;

FIG. 1A illustrates an example embodiment of an integrated security system, according to the present invention;

FIG. 2 shows a block diagram of a security system for mapping a plurality of sensors to a camera, according to an example embodiment of the present invention;

FIG. 3 shows a block diagram of a security system for mapping a plurality of cameras to a sensor, according to an example embodiment of the present invention;

FIG. 4 shows an example mapping or lookup table, according to an example embodiment of the present invention;

FIG. 5 shows a flow diagram for logic for implementing a process to enable security cameras in response to mapped sensors, according to an example embodiment of the present invention;

FIG. 6 shows a flow diagram for logic used to enable cameras for a security system, according to an example embodiment of the present invention;

FIG. 7 shows a block diagram of an interface for implementing differing levels of access to a security system, to an example embodiment of the present invention;

FIG. 8 shows a block diagram of another interface for implementing differing levels of access to a security system, to an example embodiment of the present invention; and

FIG. 9 shows a block diagram of another interface that provides administrative monitoring of configuration settings for a security system, to an example embodiment of the present invention.

[0021] While the invention is amenable to various modifications and alternative forms, specifics thereof have been shown by way of example in the drawings and will be described in detail. It should be understood, however,

that the intention is not necessarily to limit the invention to the particular embodiments described. On the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

DETAILED DESCRIPTION

[0022] The present invention is believed to be applicable to a variety of different approaches and arrangements for providing security services. The invention has been found to be particularly advantageous for addressing security monitoring needs in a residence or private-office environment.

[0023] According to an example embodiment, a security system utilizes cameras to detect and identify intruders. The system includes an integrated camera/motion detector that is responsive to intrusion sensors and other types of sensors/alarms (*e.g.,* a smoke detector, a carbon monoxide detector, a gas detector, or a panic button). For simplicity, the following discussion focuses on the integrated camera/motion detector being responsive to intrusion detection; however, the discussion is equally applicable to the integrated camera/motion detector being responsive to other types of sensors and alarms as well. The camera's smart-behavior results in reduced power consumption and mitigates privacy concerns on various levels. A system user sets up zones with at least one intrusion sensor (*e.g.,* door/window contacts, glass-break detectors, hyper frequency radar detector, or an infrared barrier) for each zone around the perimeter of a facility and sets up corresponding camera/motion detectors in the interior of the facility. The intrusion sensors are activated (armed) by a system user, using, *e.g.,* a keypad on a security panel, a remote control keyfob, a phone call using DTMF, a personal computer or a remote server. This allows for a complete activation of the system when the system user leaves the facility as well as a partial perimeter activation of the facility when the system user (or other authorized person) is present. Thus, when the user is present the camera remains "off" unless appropriately triggered by the motion detector. However, the motion detector also remains "off" unless it is armed by a corresponding intrusion sensor. Therefore, cameras record images inside the facility when both an intrusion sensor has been tripped and a motion detector has detected motion. In one implementation, the system user enters a code (*e.g.,* using a keypad on a security panel) to identify the desired mode of system operation. In another implementation, the system user enters a system access code and then selects that desired mode of operation from a display.

[0024] Another example embodiment is directed to an integrated security arrangement. The arrangement includes an intrusion sensor to sense an intrusion at a target area of a facility, a second sensor to sense movement, an image-capture device, and a base unit. The image-capture device captures images in response to an intrusion indication from the intrusion sensor and in response to a movement indication from the second sensor. The base unit integrates a direction of view of the second sensor and of the image-capture device, thereby directing the second sensor to sense in the target area in which the images are captured by the image-capture device.

[0025] FIG. 1 depicts a building-security system according to an example embodiment of the present invention. FIG. 1 includes building 100, control panel 102, and peripheral devices 104-110. The security system is implemented in such a manner so as to reduce the power consumption of one or more of the control panel and peripheral devices as related to the wireless communications between the devices. When implementing the wireless communications, the devices use multiple frequencies (channels) as well as communication intervals. The devices are able to reduce the power consumption by utilizing information regarding a specific frequency from the multiple frequencies used and the communication interval. For example, if the transmitting devices modify their transmissions based upon the information, a receiving device may reduce the power consumption by decreasing the time the receiving device is listening for a transmission from another device. By reducing the power consumption, the system lends itself to implementing bi-directional communications between the devices, which typically require more power consumption than unidirectional communications.

[0026] The jagged lines and ellipses found between control panel 102 and the peripheral devices represent wireless communications between the control panel and the peripheral devices. The wireless communications may be implemented using suitable frequencies. For instance, wireless communications frequencies in industrial, scientific and medical (ISM) radio bands (900Mhz, 2.4Ghz and 5.8Ghz) have been found to be suitable for security systems; however, alternate frequencies may be implemented in accordance with the particulars of the system or its intended implementation.

[0027] The various elements of the peripheral devices and the control panel are implemented using one or more of electric circuit arrangements, processors, memory elements, software code, programmable logic devices, input/output interfaces or combinations thereof.

[0028] Building 100 represents a facility for which the building-security system is implemented. Common implementations of building 100 include, but are not limited to, residential homes, retail stores, office buildings, government buildings, museums and other facilities. Typically, the security system will monitor several locations within building 100. Accordingly, FIG. 1 depicts various peripheral devices throughout the building.

[0029] Peripheral communications devices 104-110 may take the form of a variety of different devices, a few of which are depicted in FIG. 1. For instance, device 104 depicts a window sensor that may, among other things, detect when the window has been opened or otherwise

compromised; device 106 depicts a camera for video capture; device 108 depicts an alarm; and device 110 depicts a mobile peripheral, such as a key fob for interfacing with the control panel or another peripheral. Other example sensors include but are not limited to fire alarms, carbon dioxide sensors and panic buttons. These peripheral devices communicate with control panel 102 using wireless communications.

[0030] Block 112 depicts several elements that may be implemented in the peripheral devices, including a transceiver block, a message protocol block, a synchronization block and a transmit (Tx) anticipation block. Various embodiments of the present invention use one or more of these blocks. In one such embodiment, a peripheral device wirelessly transmits a signal using the transceiver block. The peripheral device uses information regarding a transmission period and the listening channel of the control panel in the transmission process.

[0031] In one embodiment, the peripheral devices transmit building-security information to the control panel. For instance, device 106 might transmit video images or device-status information to the control panel, while device 104 might transmit information relating to the window's sensor.

[0032] FIG. 1 depicts control panel 102 as including a transceiver block, a message protocol block, a synchronization block and a transmit (Tx) anticipation block. Various embodiments of the present invention use one or more of these blocks. In one such embodiment, the transceiver block is used for receiving signals from one of the peripheral devices as a function of the communication intervals and the frequency the control panel uses to listen for transmissions. The listening frequency is one of several potential frequencies available for communication between the peripheral devices and the control panel. For instance, the system may use a number of contiguous frequency slots (channels) within a suitable frequency band. One example of such a use includes 25 or more channels within the ISM frequency band from 902-928 MHz. Numerous other combinations of channels and frequency bands are possible using the present invention.

[0033] Typically, the control panel and peripherals are implemented using a similar set of elements as depicted by blocks 102 and 112; however, various components may be implemented differently. For instance, the synchronization block can be implemented differently in the control panel versus the peripheral devices where the control panel provides synchronization information to each of the peripherals and the peripherals must use the synchronization information to maintain synchronization using a local clock. In such an instance, the peripherals would compare the synchronization information with the local clock in order to compensate for any difference between the peripherals' time frames and the control panel's time frame. The synchronization information can take the form of a time index, such as a counter value, a current time of day or any other time based data which the peripheral can use as a reference for synchronization. In another example, the time index can be a reference within each message transmitted. Using such a system the peripheral device can compare when the message was received to when the message was expected. The peripheral device may also be configured to adjust the local clock using a compensation for a timing error. For instance, if the peripheral clock appears to be running slower than the control panel, the peripheral can compensate by increasing the clock frequency or using a counter to compensate for the differences between clocks.

[0034] The control panel and the peripheral blocks are depicted as having a transceiver; however, the system may be implemented using variations of receivers and transmitters. In some instances, a peripheral may be implemented with only a transmitter. In other instances, a peripheral may be implemented with only a receiver. Other implementations allow for one or more of the control panels and peripherals to have both a transmitter and receiver (transceiver). Thus, transceiver is used herein to describe a receiver, transmitter or both a receiver and transmitter.

[0035] One embodiment of the present invention reduces the power of one of the devices as a function of the listening channel and a communications period. The system decreases the length of time that a receiver is active by using the communications period and listening channel to reduce the window of time necessary to receive the start of a transmission. When the receiver is not active, various methods of power reduction are employed, such as removing power from the receiving devices or reducing or stopping selected functions (*e.g.,* amplification or processing).

[0036] Another embodiment synchronizes the various peripheral devices with the control panel. The synchronization can further reduce the active time of the transmitter because, for example, the transmitter may limit the transmission times relative to the times for which the receiver is active. Such a reduction can be accomplished because, for example, in many systems the transmission time cannot be shorter than the Rx activation period of the receiver without knowledge of when the Rx activation occurs; however, synchronization can reduce the transmission times to less than the Rx activation period of the receiver.

[0037] In a specific example, the control panel sends periodic synchronization messages to the peripheral devices. A peripheral device that determines it has lost synchronization with the control panel can increase the active time of the receiver to compensate for the loss in synchronization. In the event that the peripheral device is no longer receiving synchronization messages, the device can increase the active receive time to ensure that a transmission from the control panel will be received. The peripheral device can increase the activation time based upon an expected accuracy of the local tracking (*e.g.*, local clock) of the control panel time-base. For instance, where the expected accuracy of the local tracking

is relatively high, the peripheral device increases the activation time only upon the loss of several synchronization messages.

[0038] Some devices, such as a keyfob or other handheld device (110), are portable and are often removed from the wireless communication range of the rest of the system or may cease to receive or transmit information in response to a period of inactivity. Thus, the portable devices often lose synchronization during the time they are unable to communicate with the control panel. Accordingly, such portable devices frequently increase the activation time to compensate for the lack of synchronization between the portable devices and the control panel. The frequent increase in activation time often leads to a high rate of power consumption. To compensate, portable devices can be implemented to shut down transmission monitoring efforts until an external action occurs, such as a button being pressed.

[0039] In one embodiment of the present invention, the messages sent by the control panel are received by multiple peripheral devices simultaneously. Where the message is not intended for all the peripherals, the message can include information that indicates for which peripheral the message is intended. The message can also be associated with a channel that the control panel uses for an acknowledge message from the peripheral.

[0040] FIG. 1A illustrates an example embodiment of an integrated security system, according to the present invention. A base unit 35 is located in the interior of a facility and integrates a motion sensor 20, a camera 25 (*e.g.,* CCD camera), a data processor 30, and a communication interface 15. In one implementation the motion sensor is a passive infrared (PIR) sensor, which detects infrared energy in a target area and, in connection with a processor 30, recognizes changes in infrared energy (*e.g.,* temperature changes) to detect motion. Depending on the size of the facility, multiple base units are located throughout the facility's interior, with a control panel 45 acting as a conventional communication hub for the facility. The control panel 45 interfaces with the base unit 35 via communications interface 15. In the event that an intrusion signal 10 is received by the control panel 45 from an intrusion sensor, the control panel arms motion sensor 20 allowing the motion senor to activate the camera 25 when movement is detected. The control panel 45 can also directly activate the camera 25 (*e.g.,* without regard to motion sensor 20). In one implementation, the base unit 35 can receive the intrusion sensor input 10 via communications interface 15. The sensor input 10 can therefore inform either the base unit 35 or the control panel 45 to arm the motion sensor 20 and/or activate the camera 25. When unarmed, the motion sensor 20 will not be able to activate camera 25 but may still detect motion. The motion sensor 20 can detect motion in its field of view, and once the motion sensor is armed, the motion sensor is able to activate the camera 25. The motion sensor 20 and the camera 25 are positioned such that both devices have overlapping fields of detection. Thus, images of the source of the detected motion are recorded by the camera without requiring any intervening adjustment or alignment The recorded images are processed by a data processor 30, which can be integrated with the motion sensor 20 and the camera 25 in a base unit 35 as shown, or may be located remotely and electrically coupled to the base unit 35.

[0041] It will be appreciated that the data processor 30 can be implemented, for example, in the form of a high-speed processor such as a DSP (including an ALU) and/or a more general-purpose processor that may be optionally programmed for video data (de)compression. Thus, various embodiments may include a variety of combinations of processing operations with one or more aspects of the processing operations performed at one or more local or remote processors. For example, both video data storage and compression may be performed in the base unit 35 by the data processor 30. When the processor is located remotely, the data storage may still occur in base unit 35, but compression of the video data could be implemented in the remote processor. Another embodiment may involve data storage in the base unit 35 without any compression of the video data. Moreover, each of the above operations may be performed in combination with a central processor 55, as further discussed below.

[0042] In example implementations the base unit 35 is a battery-operated, wireless device having both motion sensing and image-capture capabilities, For further information on such a device, reference may be made to filed provisional application serial no. 60/785,570 filed on Match 24, 2006, entitled "Motion-Image Monitoring Method and Device". In certain implementations, data processor 30 is configured to preserve battery life by communicating in accordance with appropriate power-saving protocols. For example implementations related to communicative coupling and data transfer among the above-discussed devices in accordance with appropriate protocols, reference may be made to U.S. application serial no. 11/389,673 filed on March 24, 2006, entitled "Spread Spectrum Communications for Building-Security" and European Patent Application Publication No. EP 1 363 260 filed on May 6, 2003, entitled "Procédé de oommunication radiofréquence entre plusieurs dispositifs et système de surveillance mettant en oeuvre un tel procédé." The power-saving approaches also provide for limited activation of the above-discussed camera such that the privacy of the inhabitants of a residence or facility is largely maintained.

[0043] The recorded images are transmitted over a bi-directional sensor communication path 40 to a control panel 45. In one implementation, the sensor communication path 40 is wireless and can be employed, *e.g.*, as described in the above two incorporated patent documents. The transmitted images may be encrypted by the data processor 30 before being transmitted to the control panel 45. The control panel 45 includes a local storage area for the recorded images 50, the central processing

unit 55, and a transceiver 60. The control panel 45 is located within the same facility as the base unit 35. The central processor 55 receives images from each of the base units located within the facility. Similar to the above discussion, the central processor 55 may perform a variety of processing operations alone or in combination with data processor 30. The images may optionally be stored in data storage 50 for further review or processing. The control panel 45 includes a battery backup power source 65 in the event of a loss of power, *e.g.,* a natural disaster or an intruder disables power to the facility. The transceiver 60 further transmits signals including system status reports or recorded images via a telephone channel 70 or cable channel 75 to outside monitoring facilities. The telephone channel 70 and cable channel 75 are not limited to PSTN or broadband channels; they may be part of a GSM/CDMA network. Outside monitoring facilities may include a private security company or a local law enforcement station.

[0044] In another example embodiment, when an intrusion sensor senses an intruder breaching the facility (*e.g.,* door/window contact is tripped), the intrusion signal 10 is transmitted directly to the control panel 45. The control panel 45 arms one or more base units 35 in the same zone as where the intrusion signal (via sensor 10) originated. For example, in response to a widow contact being tripped in a room the control panel 45 can arm the sensor 20 of base unit 35 in that room, as well as the sensors of the base units located in adjacent rooms and/or the hallway outside the room. In this manner the system can track intruders as they move throughout the facility. The base unit(s) 35 respond as discussed above. In this system architecture, the control panel 45 is the master and the sensors and control devices (*e.g.,* keypads, keyfobs) are slave devices. The radio link in this architecture is a star topology with the control panel 45 at the center of the network. The branches include base units 35 and external links, *e.g.*, telephone channel 70 and broadband channel 75.

[0045] Other aspects of the present invention are applicable to a security system where a second sensor and image-capture device are not physically integrated inside the same housing. In one such example, an embodiment is arranged with an intrusion sensor to sense an intrusion at a target area of a facility, a second sensor to sense movement, and an image-capture device. The second sensor bears a special relationship (*e.g.,* located sufficiently near and aligned) with the image-capture device to form a common field of view, such that the fields of view for both devices overlap without the devices being located inside a common housing. The image-capture device captures images in response to an intrusion indication from the intrusion sensor and in response to a movement indication from the second sensor.

[0046] In more specific embodiments, the various arrangements permit for the devices to be situated in different ways to provide the common field of view. For example, horizontal movement, vertical movement, or horizontal and vertical movement can be provided for each of the motion sensor and the image-capture device, with their movements mirrored to maintain the integrated field of view. More particularly, such mirrored movement can be provided by using a ratchet-like mechanism with devices to provide increment adjustments in the horizontal and/or vertical directions; the skilled artisan would appreciate that such adjustment can be implemented using servo-control motors or be manually implemented using conventional position-stabilizers that permit stepwise/incremental rotation.

[0047] In a related embodiment, horizontal movement, vertical movement, or horizontal and vertical movement can be provided for either or both the motion sensor and the image-capture device by way of conventional electronically-implemented pan/tilt/zoom operation(s), with their movements coordinated to maintain the integrated field of view. For image-capture, such pan/tilt/zoom operation is commonly used in digital video-recording devices. The motion detector may also be manipulated to alter the field of view.

[0048] In more specific embodiments, the various arrangements can be implemented with a spatial relationship between the motion sensor and the image-capture device by using a common backplate to which each of the motion sensor and the image-capture devices are mounted and/or a template for aligning the motion sensor and the image-capture device for mounting on a wall, where contoured portions of the respective backs of the motion sensor and the image-capture device may provide an offset for biasing the direction of view.

[0049] In other specific embodiments, the various arrangements permit for such above-described devices to be situated such that their movement is pre-set before they are used or dynamically controlled while in use with automated or semi-automated coordination provided by the control circuitry and/or personnel at a remote-site center. Such coordinated movement, while maintaining a common field of view, benefits a variety of monitoring and/or security applications.

[0050] According to one example embodiment of the present invention, an intrusion sensor, such as a window or door contact, located at a perimeter of a facility detects whether the contact subject, window or door, has been breached. If, for example, a window has been opened, the window contact (intrusion sensor) sends a signal to a corresponding integrated motion sensor/camera located at the interior of the facility. Upon receipt of the intrusion signal, the motion sensor is armed and the integrated camera is set to a "ready" mode without initiating recording. The motion detector remains armed and when motion is detected, the integrated motion sensor/camera is again triggered. Once motion is detected, the camera turns "on" and captures images of the source of the motion. The video images are sent to a central control panel for further evaluation. Further evaluation may include determining (manually or automatically using, *e.g.,* machine visions) whether the source of the motion is human, an

animal such as a pet, or another moving object. If the source is determined to be human, further evaluation may reveal whether any identifying images were captured, whether the human is an intruder or an inhabitant of the facility, and face recognition may be used to identify a previously unknown person intruding on the facility.

[0051] In another example embodiment, the home entry intrusion sensor (*e.g.,* front door contact) corresponds to a delayed-respqnse motion sensor such that the transmission of the motion indication is delayed to accommodate a security system control keypad located near the entrance. In another zone located nearby, such as a kitchen, the motion indication is not delayed when motion is detected. The system recognizes that motion sensed in the nearby room (*e.g.,* person setting grocery bags down in the kitchen) following a delayed sensing of motion in the entry zone is likely an authorized user and an alarm will not sound for a predetermined length of time. If the system is not deactivated or reset before the predetermined length of time expires, the alarm will sound. The number of nearby zones configured with such a relationship with the delayed motion indication in the entry zone should be limited to ensure that an actual intruder is not provided enough time to traverse the premises without being detected.

[0052] In a further example embodiment, the security system is equipped to capture an image of the person arming or disarming the system (*e.g.,* by entering a code on a security system control keypad) to determine if the person is an authorized user. In one instance, the captured image can be sent to a remote monitoring station for verification or stored for future reference. In another instance, the security system can be programmed with images of the authorized users and the system uses face recognition to compare the captured image of the person attempting to arm/disarm the system with the images of the authorized users to determine whether the person is an authorized user. If the person's image matches that of an authorized user, then the person is allowed to arm/disarm the system. In one implementation, the security system control keypad is equipped with a camera to capture an image of the person entering a code. In another implementation, a base unit 35 is positioned such that the base unit's camera 25 can capture an image of the person entering a code on the security system control keypad. In response to a code being entered, the security system control keypad activates the camera 25 to capture an image of the person entering the code.

[0053] In an additional example embodiment, the security system is equipped with a self diagnostic mode that is used to determine if the system is functioning properly. The system sends test signals representing intrusion detections by various sensors to the base stations 45 to determine that the appropriate sensors 20 are armed and/or the appropriate cameras 25 are activated. The system can also enable each of the cameras 25 to capture an image to check that the cameras are working. The results of the diagnostic tests can be displayed for the system user, saved for future review or provided to a remote monitoring station.

[0054] FIG. 2 shows a block diagram of a security system for mapping a plurality of sensors to a camera, according to an example embodiment of the present invention. Control block 206 interfaces with sensors 204 (*i.e.,* sensor(1) to sensor(N)) and camera 202. Control block 206 receives input from sensors 204 regarding the status of the sensor. For instance, a particular sensor may send a message to control block 206 in response to a window or door being opened. Control block 206 can then make a determination as to whether camera 202 should be activated. In one implementation, control block 206 has a mapping or lookup table that links one or more of the sensors to camera 202. In this fashion the response of control block 206 to one or more of sensors 204 can be limited to sensors that correspond to the room or field of view covered by camera 202. In some instances, control block 206 can receive images from camera 202 and also forward the images to a monitoring station, using a telephone or network interface. Moreover, in some instances, camera 202 is able to pan, tilt, zoom or otherwise change the field of view to correspond to the particular sensor that was triggered.

[0055] According to an example embodiment of the present invention, sensors 204 and camera 202 announce their presence to control block 206 during an initialization stage. A user of the system can select from these devices when determining what sensors camera 202 should be configured to respond to. In one instance a graphical user interface can be used to allow for ease of configuration. In another instance, a graphical display of the location of the sensors 204 and camera 202 can be used to allow a user to easily select and configure the system. Such configuration can be limited to implementation during installation of the security system, or can be implemented throughout the use of the security system. For instance, given that sensors 204 can optionally be wireless, it is possible that the sensors may be moved from time to time. This may be necessary where the function of a room changes or where the structure undergoes changes. Moreover, sensors can be added or replaced at later dates.

[0056] In certain instances, camera 202 can operate in different modes that may or may not be responsive to sensors 204. For example, one mode may disable camera 202 completely, while another mode may enable camera 202. One such mode would include control block 206 enabling cameras 202 in response to one or more selected sensors 204. In one embodiment of the present invention, different modes may have different sensors mapped to camera 202. For instance, one mode may have a door sensor mapped to camera 202, while another mode may have both a door sensor and a motion sensor mapped to camera 202 (*e.g.,* for when there should be no authorized occupant in the area). The system can be programmed such that a different code is used to identify each of these modes of operation. The system user en-

ters one of the codes (*e.g.,* on a security system control keypad) to select the desired mode of operation. In one implementation, the system user enters a security access code and then selects from one of the programmed modes of system operation that are identified on a display screen (*e.g.,* by selecting a corresponding icon on a touch screen or by entering a number identifying one of the modes). In another implementation, the system user enters a code for each mode of operation. This can be useful for allowing different levels of access/mode settings for different users. For instance, a child, friend or relative could be given only certain codes. This is particularly useful for controlling access to configuration settings or preventing access during restricted time periods, such as late at night.

[0057] In a particular instance, one of the codes may correspond to a sequence of image captures from various cameras. Thus, a user of the system can initiate a sequence of camera shots to view different areas of the facility. This can be particularly useful for assuring a user that there are no intruders or for monitoring the status of an occupant (*e.g.,* a small child or otherwise vulnerable person) and the house in general (*e.g.,* to check for fire or damage due to natural disasters).

[0058] In connection with the embodiments discussed herein as examples of the present invention, the camera can be enabled in various ways. Generally, enabling of the camera includes enabling the camera arrangements discussed in connection with figures 1-3. Accordingly, when a sensor mapped to a camera arrangement detects a potential intruder, the motion detector of the camera arrangement is enabled. If the motion detector senses motion, the camera can then be enabled to capture pictures of potential intruders. In an alternative mode, the camera can also be configured to immediately capture pictures (*e.g.,* regardless of the motion detector) in response to the detection of a potential intruder. This can be particularly useful for sensors that do not necessarily correspond to an intruder (*e.g.,* fire alarm) and for high security modes that do not implement a delay or second level of motion detection. In such a mode, the camera would capture images independent of motion detection by the motion sensor. Another mode or setting could be used to distinguish between video capture (*e.g.,* consecutive shots over a period of time capable of showing motion, such as those stored in an MPEG file) and still image capture (*e.g.,* one or more individual images that can be stored using file formats such as JPEG) by the camera. Accordingly, in response to a sensor and a selected mode, the system can be configured to 1) capture images after detecting motion in the field of view, 2) immediately capture video, and 3) immediately capture a still image. These and other configuration options can be implemented using the various mapping features discussed herein.

[0059] FIG. 3 shows a block diagram of a security system for mapping a plurality of cameras to a sensor, according to an example embodiment of the present invention. As discussed above, sensor 302 and cameras 304 (*i.e.,* camera(1) to camera(N)) communicate with control block 306. In response to input from sensor 302, one or more of cameras 304 can be enabled. As discussed in connection with FIG. 2 and elsewhere herein, the control block 306 can implement the desired correspondence between cameras 304 to sensor 302 using mapping database or lookup table. This can be advantageous where the cameras provide different angles of view and/or different fields of view. For instance, in response to window sensor, several cameras can be enabled, allowing for security monitoring stations to view the entire room, and also to have a better chance of identifying a potential intruder.

[0060] In one embodiment of the present invention, multiple cameras can be selectively linked to multiple sensors. For instance, all cameras and sensors within a room can be linked together. Accordingly, the mapping of both FIG. 2 and FIG. 3 can be used in conjunction with each other.

[0061] FIG. 4 shows an example mapping or lookup table, according to an example embodiment of the present invention. The data contained in the mapping table can be stored in a suitable memory device, such as flash, random-access-memories, hard drives and the like. In some applications it can be advantageous to use nonvolatile memory for guarding against problems due to power loss.

[0062] Column 402 contains camera-1 to camera-N. It should be noted that FIG. 4 and the relevant discussion make reference to camera-1 to camera-N. As discussed herein, such cameras may include an integrated motion detector, and thus, identification information as to whether the camera device includes such an integrated motion detector may also be stored in the mapping or lookup table. Column 404 contains sensors that are configured to enable the camera arrangement in the corresponding row. For instance, sensors A, B and C would enable camera 1, while sensors X, Y and Z would enable camera 2. In this manner a user of the system provides information as to the desired associations between sensors and cameras resulting in a corresponding change in the data in the mapping table. For example, a graphical user interface can be presented to a user through a software application running on a processor. In one instance, the processor is a general purpose computer, such as a personal computer or personal digital assistant, that can interface with the control device of the security system using, for example a universal-serial-bus (USB), Ethernet or similar interface. In another instance, the processor is part of the control device.

[0063] Column 406 contains additional information regarding relationships between sensors and cameras. In one instance, column 406 represents sensors that enable the corresponding camera when the security system is in a particular mode (*i.e.,* a different mode than column 404 would be associated with). This is useful to distinguish between situations where the occupants are awake from when they are sleeping, windows that are opened

from the inside from windows that are opened from the outside, situations where the occupants are on vacation from when they are not, and the like. In another instance, column 406 represents sensors that need to be triggered prior to sensors in column 404 activating a camera in column 402. Thus, the sensors can be linked to each other, thereby requiring a succession of sensors to be triggered prior to activation of a mapped camera. In yet another instance, column 406 represents sensors that are only enabled after a certain delay. This can be particularly useful for enabling sensors that are in the likely path of an intruder. For instance, the camera in a bedroom may be enabled after a window sensor in the bedroom is triggered. After a delay sufficient to allow an intruder to traverse the room, a sensor from column 406 and corresponding to an adjoining room can be enabled.

[0064] Column 408 represents additional data used to supplement the mapping functions. In one instance, column 408 may contain information relating to cameras that are only enabled after a certain delay. This can be particularly useful for enabling cameras that are in the likely path of an intruder. For instance, the camera in a bedroom may be enabled after a window sensor in the bedroom is triggered. After a given delay (*e.g.,* sufficient to allow an intruder to traverse the room) a camera in an adjoining room can be enabled. In another instance, column 408 may contain data that contains delay values for enabling the cameras or sensor of column 404 and 406. In yet another instance, the data in column 408 can be used to denote one or more security modes for which the sensors and cameras stored in the respective mapping table columns are enabled or disabled.

[0065] According to another embodiment of the present invention, a combination of sensor events and the details of the sensor events can be selected to further define enabling events for various cameras. In addition to requiring a sensor to be triggered, combinational events can be used to determine details, such as whether a series of sensor events represent a person leaving or entering an area. More specifically, the order of sensor events and the absence of certain sensor events can be used to determine the direction a person is traveling, the number of people present and other security factors. Using information relative to the sequences of events, the system can be configured to avoid unnecessary video capture of normal occurrences, such as the exit of an authorized person from a secured area, while still capturing abnormal occurrences, such as the entrance of a person to the secured area.

[0066] Additional data storage elements of the mapping table (*e.g.,* similar to columns 406 and 408) are possible and only limited by practical considerations, such as complexity and storage space.

[0067] FIG. 5 shows a flow diagram for logic for implementing a process to enable security cameras in response to mapped sensors, according to an example embodiment of the present invention. Block 502 represents a decision as to whether a sensor has been triggered. The process waits at block 502 for a sensor to be triggered. If a sensor is triggered, the process proceeds to block 504. Block 504 determines whether the sensor is mapped to a camera. If no camera is mapped to the sensor, the process returns to block 502 and waits for another sensor to be triggered. If a camera is mapped to the sensor, the process proceeds to block 506.

[0068] Block 506 represents potential enable logic. In the simplest case, the enable logic depicted by block 506 need not be implemented. In such a case, the process proceeds directly to block 508. In other instances, various determinations, delays and other functions can be carried out at block 506. In a particular embodiment of the present invention, information stored in a mapping table is used to implement the enabling logic. As discussed herein, such information may represent different logic for different modes, delays before enabling and the like. In some instances, the logic may determine that no camera should be enabled and the process proceeds to block 510. One such instance is where the security system is in a mode for which the linked camera is not to be enabled. In another instance, the logic may enable other sensors prior to enabling the camera. After determining that the camera should be enabled the process proceeds to block 508 to enable the camera.

[0069] The process next checks for additional cameras that are linked to the triggered sensor as shown by block 510. If no additional camera is found, the process returns to block 502. If an additional camera is found, the process proceeds to block 512. Block 512 is a logic block similar to block 506, where the process can branch to blocks 510 or 514. Block 514 enables the corresponding camera and returns to block 510 to determine if additional cameras are mapped to the triggered sensor. In this manner, a series of cameras can be enabled in response to one or more triggered sensors. This is particularly useful for enabling cameras along a likely path of an intruder.

[0070] The various components of such a process can be implemented using one or more general purpose processors configured with appropriate software, one or more custom processors, programmable logic devices, analog/digital circuits, integrated circuit devices and combinations thereof.

[0071] FIG. 6 shows a flow diagram for logic used to enable cameras for a security system, according to an example embodiment of the present invention. In a particular embodiment this logic can be implemented in place of enable logic blocks 506 and 512 (*e.g.,* as a function call in a software routine). The process begins at block 602 where it proceeds to block 604. Block 604 can implement a delay before enabling any cameras. If no delay is require, the delay step can be skipped. In one instance, the delay can be a fixed delay for each camera. In another instance, the delay can be a function of data stored in the mapping table along with other variables, such as the current mode of the security system. After the delay, if any, is implemented, the process proceeds to block 606. At block 606, a determination is made as

to whether the sensor is configured to enable the camera relative to the current security mode. This can be accomplished, for example, by a comparison of the data in the mapping table with the current security mode. If it is determined that the camera should not be enabled in response to the sensor, the process exits as shown by block 614. Otherwise the process proceeds to block 608.

[0072] At block 608 a determination is made as to whether additional sensors are linked (*e.g.,* required to be triggered) relative to the corresponding camera. This is useful for configuring the camera to only be triggered in response to more than one sensor. If it is determined that no additional sensors are linked, the process proceeds to block 612 where the corresponding camera is enabled. The process then exits as shown by block 614.

[0073] If at least one additional sensor is linked, the process proceeds to block 610. At block 610 a determination is made as to whether the linked sensor is triggered. If the linked sensor is not triggered, the process can wait at block 610 until the linked sensor is triggered. In some instances, it is desirable to reset or exit from this state even if the linked sensor is not triggered. This can be accomplished using various methods. Using one such method, at timer can precipitate the exit from state 610. Using another such method, the process exits from state 610 in response to an external event, such as the resetting of the triggered sensor(s). If the linked sensor is triggered, the process returns to block 608 to check for other linked sensors.

[0074] FIG. 7 shows a block diagram of an interface for implementing differing levels of access to a security system, to an example embodiment of the present invention. FIG. 7 depicts a security interface 704 that provides two control/access levels 706 and 712 for different users of the system. The different control levels can be particularly useful for simplifying the control aspects available to an end user 702, while allowing additional functionality to be configured by a qualified installer 710. The control levels can also be particularly useful for reducing the risk of an end user 702 improperly configuring the security system, by limiting the control of certain aspects of the system. Thus, the security system can be configured such that a minimum level of security is maintained, regardless of the end user 702 configuration changes.

[0075] Security interface 704 is accessed using a number of different mechanisms. A non-exhaustive list of acceptable interfaces includes a general purpose computer connected through Ethernet, USB or the like, key pads, touch screens, voice response systems and keyfobs. Security interface 704 provides a different level of access depending upon the user. In one instance, the user credentials can be determined by a username and/or password, electronic identification cards, wireless transmitters, biometric identifications or the like. Once the user credentials are determined, the user is granted an appropriate level of control over the system as shown by blocks 708 and 714. The number of different levels of control and user can vary depending upon the particular application. For example, a first level (*e.g.,* full access) may exist for an installer of the system; a second level (*e.g.,* limited access) may exist for home owners and a third level (*e.g.,* mode change only) may exist for children of the home owners.

[0076] FIG. 8 shows a block diagram of an interface for implementing differing levels of access to a security system, to an example embodiment of the present invention. FIG. 8 depicts a security system 808 that allows end user 802 access using end user interface 804 and qualified installer 814 access using qualified installer interface 812. By providing multiple interfaces to the system with different levels of control, the can be further protected. For instance, subset of control features 806 could be provided through a touch screen or local computer. Such interfaces may be subject to potential security risks (*e.g.,* hacking into the computer remotely or gaining access to the touch screen prior when the system is not armed) that may compromise the security system. By limiting the control available through the end user interface, the overall security can be improved. A higher level of control (*e.g.,* installer control features 810) can be provided using a more secure interface method. For example, the interface might only accept a security card that is controlled by the installer, or it may only accept instructions from a known server or input port. Accordingly, the security system is not entirely compromised simply by compromising the end user interface 804. This can also be particularly useful for limiting the complexity by essentially hiding certain configuration options from the end user.

[0077] FIG. 9 shows a block diagram of another interface that provides administrative monitoring of configuration settings for a security system, to an example embodiment of the present invention. FIG. 9 depicts an end user interface 904 that allows end user 902 to access control logic 916. End user interface 904 sends data to and from end user 902 using network 906. End user is able to configure control logic 916 and monitor the status of sensors 912 and cameras 914 through such data transfers. Offsite administrator 908 provides monitoring functions for all or a subset of end user transactions. For instance, offsite administrator 908 can monitor configuration settings for control logic 916 to verify that the system is not compromised due to user error or an unauthorized person. In some instances, the monitoring can be limited to critical functions, such as disabling sensors 912 and cameras 914, In other instances, the monitoring can encompass all transactions. This monitoring can be accomplished using an automated process that follows a rule set designed to identify potential issues. The monitoring can also be accomplished using (alone or in combination with automated processes) human operators that watch for potential problems.

[0078] While certain aspects of the present invention have been described with reference to several particular example embodiments, those skilled in the art will recognize that many changes may be made thereto. For example, aspects of the underlying patent documents

(e.g., aspects that provide integration on fields of view, and implementation details of the integrated image-capture and motion-sensing devices). The scope of the present invention is set forth in the following claims.

Claims

1. An integrated security arrangement, comprising:

a plurality of intrusion sensors (10, 204);
a motion sensor (20, 204) to sense motion in a target area;
an image-capture device (25, 202) physically integrated with the motion sensor (20, 204) to capture images of the target area in response to the motion sensor (20, 204), when the motion sensor is armed in response to at least one selected one of the intrusion sensors (10, 204); and
a control arrangement (45, 206) including a mapping database that contains data used to associate one or more of the plurality of intrusion sensors with the image-capture device and to permit a user to configure the mapping database to select said at least one of the plurality of intrusion sensors to which the image-capture device is responsive, so that the corresponding motion sensor of the image-capture device may be armed in response to the one or more associated intrusion sensors.

2. The arrangement of claim 1, further including a base unit that physically integrates the image-capture device with the motion sensor, and wherein the control arrangement is configurable to override responsiveness of the image-capture device to the motion sensor and said selected one of the intrusion sensors, and to cause the image-capture device to capture images of the target area in response to a security code received at the control arrangement and further including a user interface that receives data for configuring the mapping database.

3. The arrangement of claim 1, wherein the control arrangement is configurable to cause the image-capture device to capture images of the target area in response to a security code received at the control arrangement.

4. The integrated security arrangement of claim 1, wherein configuring the mapping database is limited based upon different control levels for different users, wherein one control level permits configuration of the mapping database.

5. The integrated security arrangement of claim 1, further including a communication device to transmit wireless signals to a remotely-located central controller, and a housing to contain the communication device, the control unit, the motion sensor, a battery, and the image-capture device.

6. The integrated security arrangement of claim 1, wherein multiple sensors are linked in the mapping database, thereby requiring more than one sensor be tripped prior to the image-capture device capturing pictures.

7. The integrated security arrangement of claim 1, wherein, responsive to data stored in the mapping database, a second image-capture device capture images in response to a first image-capture device capturing images.

8. The integrated security arrangement of claim 1, further including a user interface and an installation interface that each receive input for configuring the mapping database, wherein the user interface has a first level of access to the mapping database and the installation interface has a second level of access to the mapping database, and wherein said first level of access is a subset of said second level of access.

9. The integrated security arrangement of any preceding claim, wherein, in a first mode, the image-capture device captures one or more still images and, in a second mode, the image-capture-device captures video images.

10. The integrated security arrangement of claim 1, wherein the image-capture device includes and is integrated with the motion sensor, and further including a user interface that receives data for configuring the mapping database, and wherein the mapping database stores data identifying the image-capture device and each of the plurality of intrusion sensors.

11. An integrated security arrangement, comprising:

an intrusion sensor (10, 204);
a plurality of motion sensors (20, 204) to sense motion in respective target areas;
a selected at least one of a plurality of image-capture devices (25, 202), the selected image-capture device physically integrated with a respective one of the plurality of motion sensors (20, 204), to capture images of the respective target area in response to the respective motion sensor (20, 204), when the motion sensor is armed in response to the intrusion sensor (10, 204); and
a control arrangement (45, 206) including a mapping database that contains data used to associate the intrusion sensor with the selected image-capture device and to permit a user to configure the mapping database to select said

at least one of a plurality of image-capture devices which is responsive to the intrusion sensor, so that the corresponding motion sensor of the selected image-capture device may be armed in response to the intrusion sensor.

12. The integrated security arrangement of claim 11, wherein the image-capture devices are each integrated with respective motion sensors as part of a base unit that is battery operated, and further including a user interface that receives data for configuring the mapping database, and wherein configuring the mapping database is limited based upon a control level associated with a user that is providing the data for configuring the mapping database, and wherein configuring the mapping database is limited based upon a different control level for a different user.

13. The integrated security arrangement of claim 11, wherein after the selected at least one of a plurality of image-capture devices captures an image, and after a delay, another one of the image-capture devices is enabled in response to data stored in the mapping database and independent of additional sensors.

14. The integrated security arrangement of claim 11, further including a user interface and an installation interface that each receive input for configuring the mapping database, wherein the user interface has a first level of access to the mapping database and the installation interface has a second level of access to the mapping database.

15. The integrated security arrangement of claim 11, wherein, in response to a user selected mode, the control arrangement configures two or more image-capture devices of the plurality of image-capture devices to consecutively capture images independent of their respective motion sensors, the control arrangement is configured to receive signals from the plurality of image capture devices as a function of communication intervals and to remove power by reducing or stopping selected functions, and wherein the mapping database stores data identifying each of the plurality of image-capture devices.

Patentansprüche

1. Integrierte Sicherheitsanordnung, umfassend:

eine Vielzahl von Einbruchssensoren (10, 204);
einen Bewegungssensor (20, 204) zum Wahrnehmen von Bewegung in einem Zielbereich;
eine Bilderfassungsvorrichtung (25, 202), welche physikalisch in dem Bewegungssensor (20, 204) integriert ist, um als Reaktion auf den Bewegungssensor (20, 204) Bilder des Zielbereichs zu erfassen, wenn der Bewegungssensor als Reaktion auf zumindest einen ausgewählten einen aus den Einbruchssensoren (10, 204) scharf gemacht ist; und
eine Steuerungsanordnung (45, 206), welche eine Verknüpfungsdatenbank beinhaltet, welche Daten enthält, welche verwendet werden, um einen oder mehrere aus der Vielzahl der Einbruchssensoren mit der Bilderfassungsvorrichtung zu verknüpfen und einem Benutzer zu erlauben, die Verknüpfungsdatenbank zu konfigurieren, um den zumindest einen aus der Vielzahl von Einbruchssensoren, auf welchen die Bilderfassungsvorrichtung reagiert, auszuwählen, sodass der entsprechende Bewegungssensor der Bilderfassungsvorrichtung als Reaktion auf den einen oder die mehreren zugehörigen Einbruchssensoren scharf gemacht werden kann.

2. Anordnung nach Anspruch 1, weiter eine Basiseinheit beinhaltend, welche die Bilderfassungsvorrichtung physikalisch in den Bewegungssensor integriert, und wobei die Steuerungsanordnung konfigurierbar ist, um Ansprechempfindlichkeit der Bilderfassungsvorrichtung auf den Bewegungssensor und den Ausgewählten aus den Einbruchssensoren zu übersteuern und die Bilderfassungsvorrichtung zu veranlassen, als Reaktion auf einen in der Steuerungsanordnung empfangenen Sicherheitscode Bilder des Zielbereichs zu erfassen, und weiter eine Benutzerschnittstelle beinhaltend, welche Daten zur Konfiguration der Verknüpfungsdatenbank empfängt.

3. Anordnung nach Anspruch 1, wobei die Steuerungsanordnung konfigurierbar ist, um die Bilderfassungsvorrichtung zu veranlassen, als Reaktion auf einen in der Steuerungsanordnung empfangenen Sicherheitscode Bilder des Zielbereichs zu erfassen.

4. Integrierte Sicherheitsanordnung nach Anspruch 1, wobei das Konfigurieren der Verknüpfungsdatenbank auf Basis von unterschiedlichen Steuerungsebenen für unterschiedliche Benutzer eingeschränkt ist, wobei eine Steuerungsebene die Konfiguration der Verknüpfungsdatenbank erlaubt.

5. Integrierte Sicherheitsanordnung nach Anspruch 1, weiter eine Kommunikationsvorrichtung zum Übertragen von drahtlosen Signalen an einen in der Ferne positionierten zentralen Controller und ein Gehäuse zur Aufnahme der Kommunikationsvorrichtung, der Steuerungseinheit, des Bewegungssensors, einer Batterie und der Bilderfassungsvorrichtung beinhaltend.

6. Integrierte Sicherheitsanordnung nach Anspruch 1,

wobei mehrere Sensoren in der Verknüpfungsdatenbank vernetzt sind und dadurch erforderlich ist, dass mehr als ein Sensor ausgelöst wird, bevor die Bilderfassungsvorrichtung Bilder erfasst.

7. Integrierte Sicherheitsanordnung nach Anspruch 1, wobei, als Reaktion auf in der Verknüpfungsdatenbank gespeicherte Daten, eine zweite Bilderfassungsvorrichtung als Reaktion auf das Erfassen von Bildern durch eine erste Bilderfassungsvorrichtung Bilder erfasst.

8. Integrierte Sicherheitsanordnung nach Anspruch 1, weiter eine Benutzerschnittstelle und eine Installationsschnittstelle beinhaltend, welche jeweils Eingaben zum Konfigurieren der Verknüpfungsdatenbank empfangen, wobei die Benutzerschnittstelle eine erste Ebene des Zugriffs auf die Verknüpfungsdatenbank hat und die Installationsschnittstelle eine zweite Ebene des Zugriffs auf die Verknüpfungsdatenbank hat, und wobei die erste Ebene des Zugriffs eine Teilmenge der zweiten Ebene des Zugriffs ist.

9. Integrierte Sicherheitsanordnung nach einem der vorstehenden Ansprüche, wobei, in einem ersten Modus, die Bilderfassungsvorrichtung ein oder mehrere Standbilder erfasst, und, in einem zweiten Modus, die Bilderfassungsvorrichtung Videobilder erfasst.

10. Integrierte Sicherheitsanordnung nach Anspruch 1, wobei die Bilderfassungsvorrichtung den Bewegungssensor beinhaltet und darin integriert ist, und weiter eine Benutzerschnittstelle beinhaltend, welche Daten zum Konfigurieren der Verknüpfungsdatenbank empfängt, und wobei die Verknüpfungsdatenbank Daten speichert, welche die Bilderfassungsvorrichtung und jeden aus der Vielzahl von Einbruchssensoren identifizieren.

11. Integrierte Sicherheitsanordnung, umfassend:

einen Einbruchssensor (10, 204);
eine Vielzahl von Bewegungssensoren (20, 204) zum Wahrnehmen von Bewegung in entsprechenden Zielbereichen;
eine ausgewählte zumindest eine aus einer Vielzahl von Bilderfassungsvorrichtungen (25, 202), wobei die ausgewählte Bilderfassungsvorrichtung physikalisch in einem Entsprechenden aus der Vielzahl von Bewegungssensoren (20, 204) integriert ist, um Bilder des entsprechenden Zielbereichs als Reaktion auf den entsprechenden Bewegungssensor (20, 204) zu erfassen, wenn der Bewegungssensor als Reaktion auf den Einbruchssensor (10, 204) scharf gemacht ist; und
eine Steuerungsanordnung (45, 206), welche eine Verknüpfungsdatenbank beinhaltet, welche Daten enthält, welche verwendet werden, um den Einbruchssensor mit der ausgewählten Bilderfassungsvorrichtung zu verknüpfen und einem Benutzer zu erlauben, die Verknüpfungsdatenbank zu konfigurieren, um zumindest den einen aus der Vielzahl von Bilderfassungsvorrichtungen, welcher auf den Einbruchssensor reagiert, auszuwählen, sodass der entsprechende Bewegungssensor der ausgewählten Bilderfassungsvorrichtung als Reaktion auf den Einbruchssensor scharf gemacht werden kann.

12. Integrierte Sicherheitsanordnung nach Anspruch 11, wobei die Bilderfassungsvorrichtungen jeweils als Teil einer Basiseinheit, welche batteriebetrieben ist, in entsprechenden Bewegungssensoren integriert sind, und weiter eine Benutzerschnittstelle beinhaltend, welche Daten zum Konfigurieren der Verknüpfungsdatenbank empfängt, und wobei das Konfigurieren der Verknüpfungsdatenbank auf Basis einer Steuerungsebene, welche mit einem Benutzer verknüpft ist, welcher die Daten zum Konfigurieren der Verknüpfungsdatenbank bereitstellt, eingeschränkt ist, und wobei das Konfigurieren der Verknüpfungsdatenbank auf Basis einer unterschiedlichen Steuerungsebene für einen unterschiedlichen Benutzer eingeschränkt ist.

13. Integrierte Sicherheitsanordnung nach Anspruch 11, wobei, nachdem die ausgewählte zumindest eine aus einer Vielzahl von Bilderfassungsvorrichtungen ein Bild erfasst, und nach einer Verzögerung, eine weitere eine aus den Bilderfassungsvorrichtungen als Reaktion auf in der Verknüpfungsdatenbank gespeicherte Daten und unabhängig von zusätzlichen Sensoren aktiviert wird.

14. Integrierte Sicherheitsanordnung nach Anspruch 11, weiter eine Benutzerschnittstelle und einer Installationsschnittstelle beinhaltend, welche jeweils Eingaben zum Konfigurieren der Verknüpfungsdatenbank empfangen, wobei die Benutzerschnittstelle eine erste Ebene des Zugriffs auf die Verknüpfungsdatenbank hat und die Installationsschnittstelle eine zweite Ebene des Zugriffs auf die Verknüpfungsdatenbank hat.

15. Integrierte Sicherheitsanordnung nach Anspruch 11, wobei, als Reaktion auf einen vom Benutzer ausgewählten Modus, die Steuerungsanordnung zwei oder mehr Bilderfassungsvorrichtungen aus der Vielzahl von Bilderfassungsvorrichtungen konfiguriert, nacheinander Bilder unabhängig von ihren jeweiligen Bewegungssensoren zu erfassen, die Steuerungsanordnung konfiguriert ist, Signale von der Vielzahl von Bilderfassungsvorrichtungen als Funktion von Kommunikationsintervallen zu empfangen

und Leistung durch Verringerung oder Beenden der ausgewählten Funktionen zu entfernen, und wobei die Verknüpfungsdatenbank Daten speichert, welche jede aus der Vielzahl von Bilderfassungsvorrichtungen identifizieren.

Revendications

1. Agencement de sécurité intégré, comprenant :

une pluralité de détecteurs d'intrusion (10, 204) ;
un détecteur de mouvement (20, 204) pour détecter un mouvement dans une zone cible ;
un dispositif d'acquisition d'image (25, 202) physiquement intégré au détecteur de mouvement (20, 204) pour l'acquisition d'images de la zone cible en réponse au détecteur de mouvement (20, 204), lorsque le détecteur de mouvement est armé en réponse à au moins l'un sélectionné à partir d'un des détecteurs d'intrusion (10, 204) ; et
un agencement de commande (45, 206) incluant une base de données de mappage contenant des données utilisées pour associer un ou plusieurs de la pluralité de détecteurs d'intrusion au dispositif d'acquisition d'image et pour permettre à un utilisateur de configurer la base de données de mappage pour sélectionner ledit au moins l'un de la pluralité de détecteurs d'intrusion auquel le dispositif d'acquisition d'image répond, de sorte que le détecteur de mouvement correspondant du dispositif d'acquisition d'image puisse être armé en réponse à l'un ou plusieurs détecteurs d'intrusion associés.

2. Agencement selon la revendication 1, incluant en outre une unité de base qui intègre physiquement le dispositif d'acquisition d'image au détecteur de mouvement, et dans lequel l'agencement de commande est configurable pour neutraliser la capacité de réponse du dispositif d'acquisition d'image au détecteur de mouvement et audit l'un sélectionné à partir des détecteurs d'intrusion, et pour amener le dispositif d'acquisition d'image à acquérir des images de la zone cible en réponse à un code de sécurité reçu à l'agencement de commande et incluant en outre une interface utilisateur qui reçoit des données pour configurer la base de données de mappage.

3. Agencement selon la revendication 1, dans lequel l'agencement de commande est configurable pour amener le dispositif d'acquisition d'image à acquérir des images de la zone cible en réponse à un code de sécurité reçu à l'agencement de commande.

4. Agencement de sécurité intégré selon la revendication 1, dans lequel la configuration de la base de données de mappage est limitée sur la base de différents niveaux de commande pour différents utilisateurs, dans lequel un niveau de commande permet une configuration de la base de données de mappage.

5. Agencement de sécurité intégré selon la revendication 1, incluant en outre un dispositif de communication pour transmettre des signaux sans fil à un organe de commande central situé à distance, et un boîtier pour contenir le dispositif de communication, l'unité de commande, le détecteur de mouvement, une batterie, et le dispositif d'acquisition d'image.

6. Agencement de sécurité intégré selon la revendication 1, dans lequel de multiples détecteurs sont reliés dans la base de données de mappage, en nécessitant de ce fait que plusieurs détecteurs soient déclenchés avant que le dispositif d'acquisition d'image n'acquière des images.

7. Agencement de sécurité intégré selon la revendication 1, dans lequel, en réponse à des données mémorisées dans la base de données de mappage, un second dispositif d'acquisition d'image acquiert des images en réponse à l'acquisition d'images par un premier dispositif d'acquisition d'image.

8. Agencement de sécurité intégré selon la revendication 1, incluant en outre une interface utilisateur et une interface d'installation, chacune d'elles recevant des entrées pour configurer la base de données de mappage, dans lequel l'interface utilisateur comporte un premier niveau d'accès à la base de données de mappage et l'interface d'installation comporte un second niveau d'accès à la base de données de mappage, et dans lequel ledit premier niveau d'accès est un sous-ensemble dudit second niveau d'accès.

9. Agencement de sécurité intégré selon l'une quelconque des revendications précédentes, dans lequel, dans un premier mode, le dispositif d'acquisition d'image acquiert une ou plusieurs images fixes et, dans un second mode, le dispositif d'acquisition d'image acquiert des images vidéo.

10. Agencement de sécurité intégré selon la revendication 1, dans lequel le dispositif d'acquisition d'image inclut le détecteur de mouvement auquel il est intégré, et incluant en outre une interface utilisateur qui reçoit des données pour configurer la base de données de mappage, et dans lequel la base de données de mappage mémorise des données identifiant le dispositif d'acquisition d'image et chacun de la pluralité de détecteurs d'intrusion.

11. Agencement de sécurité intégré, comprenant :

un détecteur d'intrusion (10, 204) ;
une pluralité de détecteurs de mouvement (20, 204) pour détecter un mouvement dans des zones cibles respectives ;
au moins l'un sélectionné à partir d'une pluralité de dispositifs d'acquisition d'image (25, 202), le dispositif d'acquisition d'image sélectionné étant physiquement intégré à l'un respectif de la pluralité de détecteurs de mouvement (20, 204), pour l'acquisition d'images de la zone cible respective en réponse au détecteur de mouvement respectif (20, 204), lorsque le détecteur de mouvement est armé en réponse au détecteur d'intrusion (10, 204) ; et
un agencement de commande (45, 206) incluant une base de données de mappage contenant des données utilisées pour associer le détecteur d'intrusion au dispositif d'acquisition d'image sélectionné et pour permettre à un utilisateur de configurer la base de données de mappage pour sélectionner ledit au moins un d'une pluralité de dispositifs d'acquisition d'image qui répond au détecteur d'intrusion, de sorte que le détecteur de mouvement correspondant du dispositif d'acquisition d'image sélectionné puisse être armé en réponse au détecteur d'intrusion.

12. Agencement de sécurité intégré selon la revendication 11, dans lequel chacun des dispositifs d'acquisition d'image est intégré à un détecteur de mouvement respectif dans le cadre d'une unité de base fonctionnant sur batterie, et incluant en outre une interface utilisateur qui reçoit des données pour configurer la base de données de mappage, et dans lequel la configuration de la base de données de mappage est limitée sur la base d'un niveau de commande associé à un utilisateur qui fournit les données pour configurer la base de données de mappage, et dans lequel la configuration de la base de données de mappage est limitée sur la base d'un niveau de commande différent pour un utilisateur différent.

13. Agencement de sécurité intégré selon la revendication 11, dans lequel, après que l'au moins un sélectionné à partir d'une pluralité de dispositifs d'acquisition d'image acquiert une image, et après un délai, un autre des dispositifs d'acquisition d'image est activé en réponse à des données mémorisées dans la base de données de mappage et indépendamment de détecteurs supplémentaires.

14. Agencement de sécurité intégré selon la revendication 11, incluant en outre une interface utilisateur et une interface d'installation, chacune d'elles recevant des entrées pour configurer la base de données de mappage, dans lequel l'interface utilisateur comporte un premier niveau d'accès à la base de données de mappage et l'interface d'installation comporte un second niveau d'accès à la base de données de mappage.

15. Agencement de sécurité intégré selon la revendication 11, dans lequel, en réponse à un mode d'utilisateur sélectionné, l'agencement de commande configure au moins deux dispositifs d'acquisition d'image de la pluralité de dispositifs d'acquisition d'image pour acquérir consécutivement des images indépendamment de leurs détecteurs de mouvement respectifs, l'agencement de commande est configuré pour recevoir des signaux de la pluralité de dispositifs d'acquisition d'image en fonction d'intervalles de communication et pour couper une alimentation électrique par la réduction ou l'arrêt de fonctions sélectionnées, et dans lequel la base de données de mappage mémorise des données identifiant chacun de la pluralité de dispositifs d'acquisition d'image.

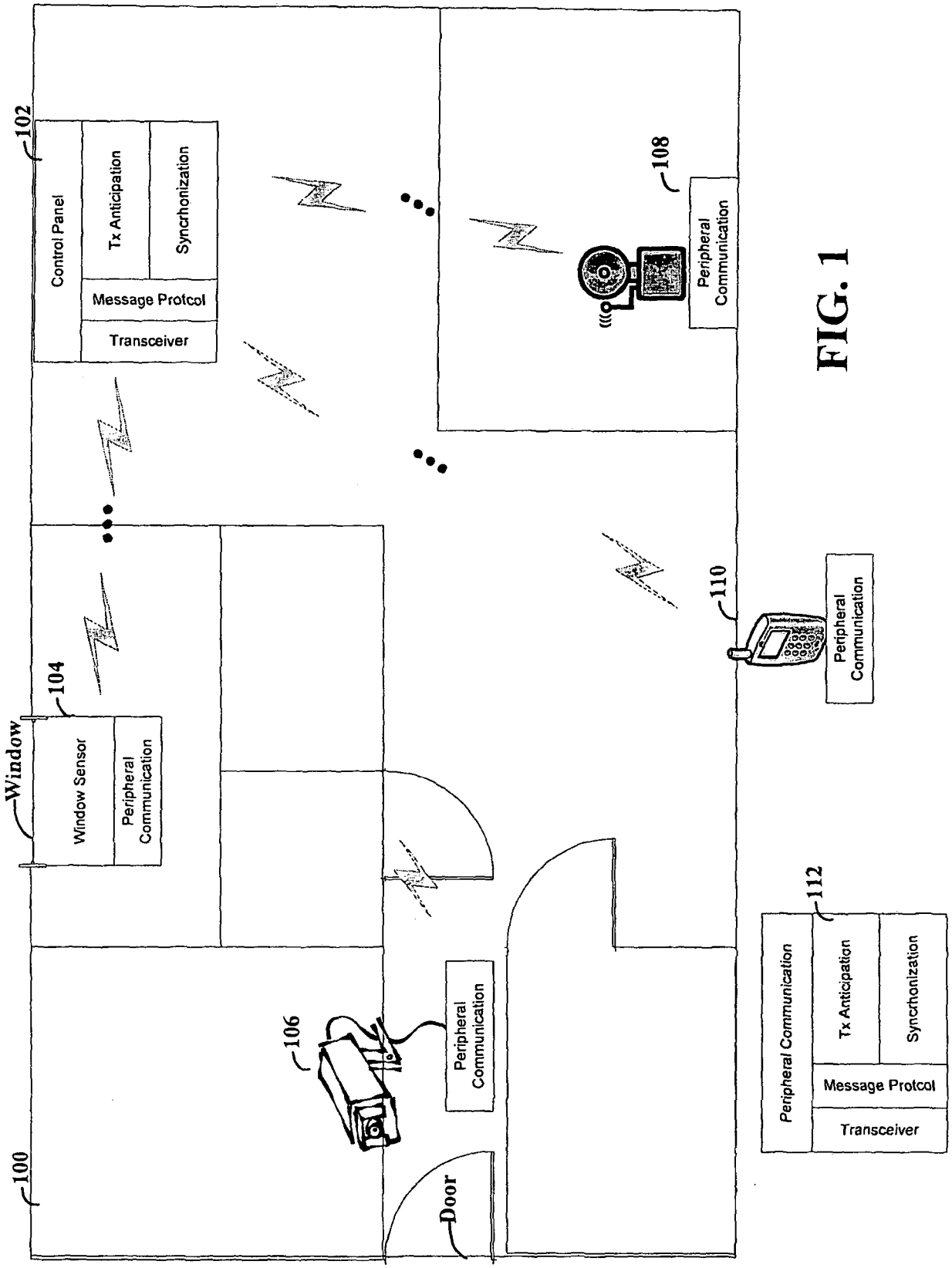

102
Control Panel
Tx Anticipation
Synchronization
Message Protcol
Transceiver
108
Peripheral Communication
110
Peripheral Communication
104
Window
Window Sensor
Peripheral Communication
106
Peripheral Communication
100
Door
112
Peripheral Communication
Tx Anticipation
Synchronization
Message Protcol
Transceiver

FIG. 1

FIG. 1A

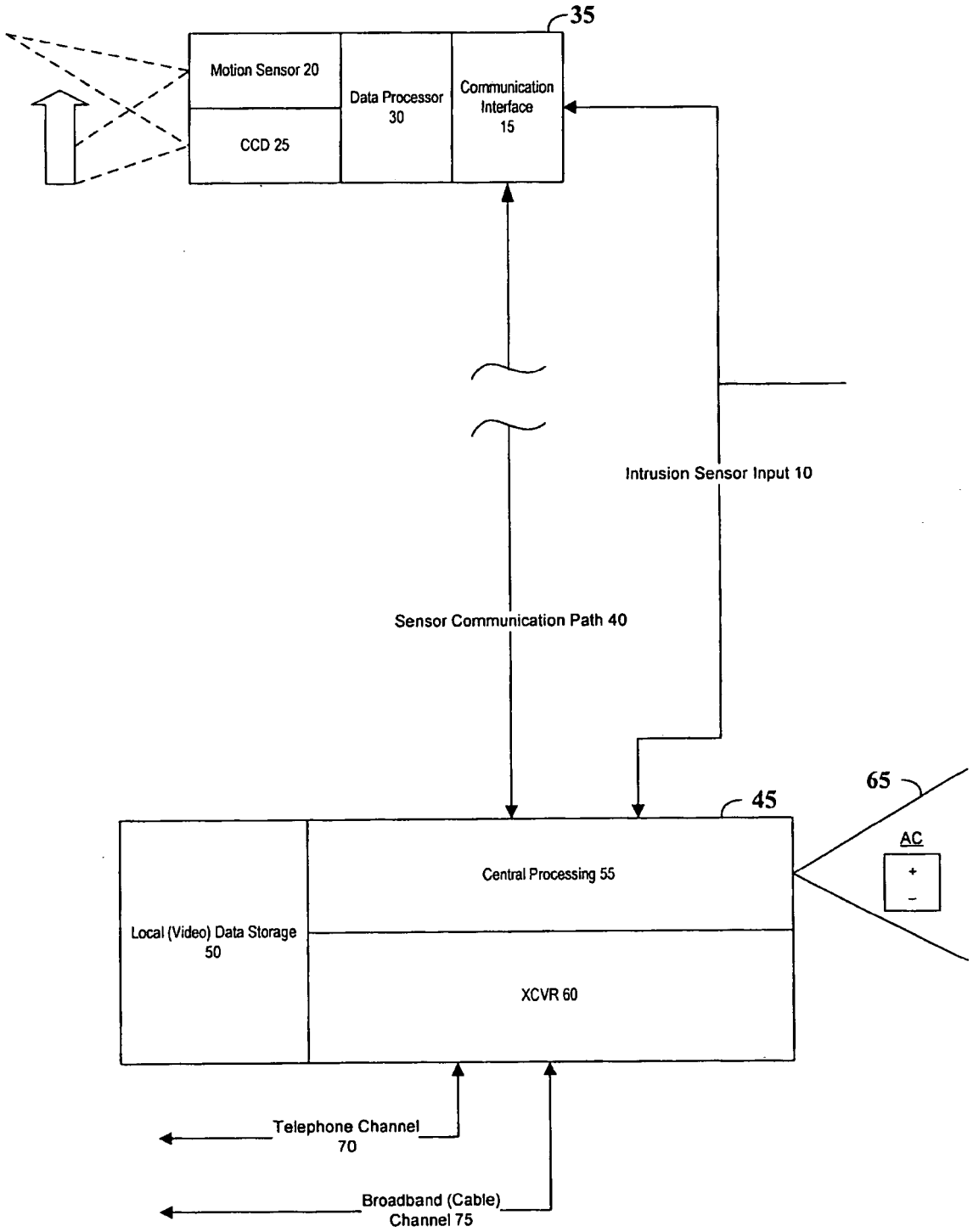

35
Motion Sensor 20
CCD 25
Data Processor 30
Communication Interface 15
Intrusion Sensor Input 10
Sensor Communication Path 40
45
65
AC
+
-
Central Processing 55
Local (Video) Data Storage 50
XCVR 60
Telephone Channel 70
Broadband (Cable) Channel 75

FIG. 2

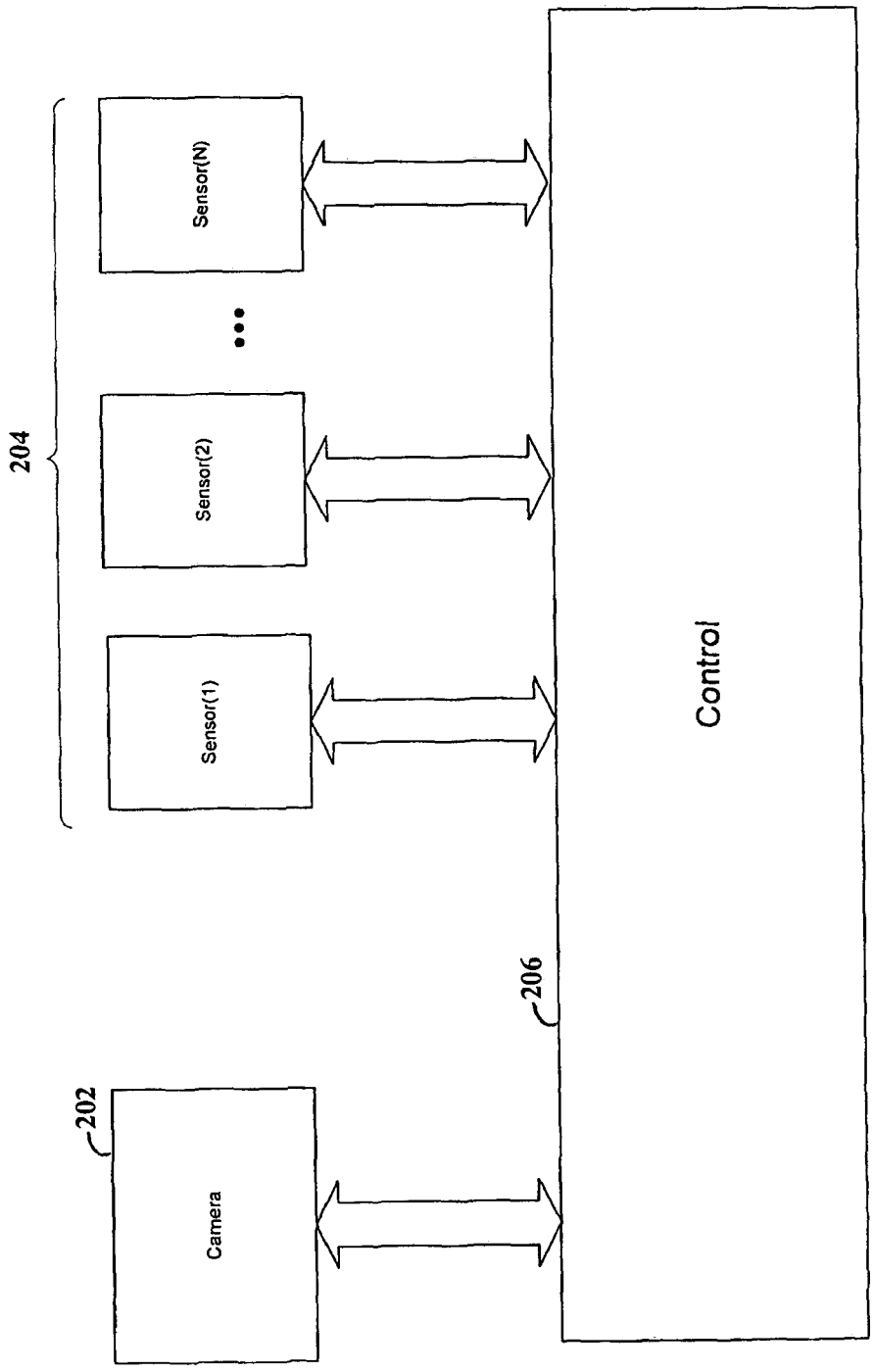


FIG. 3

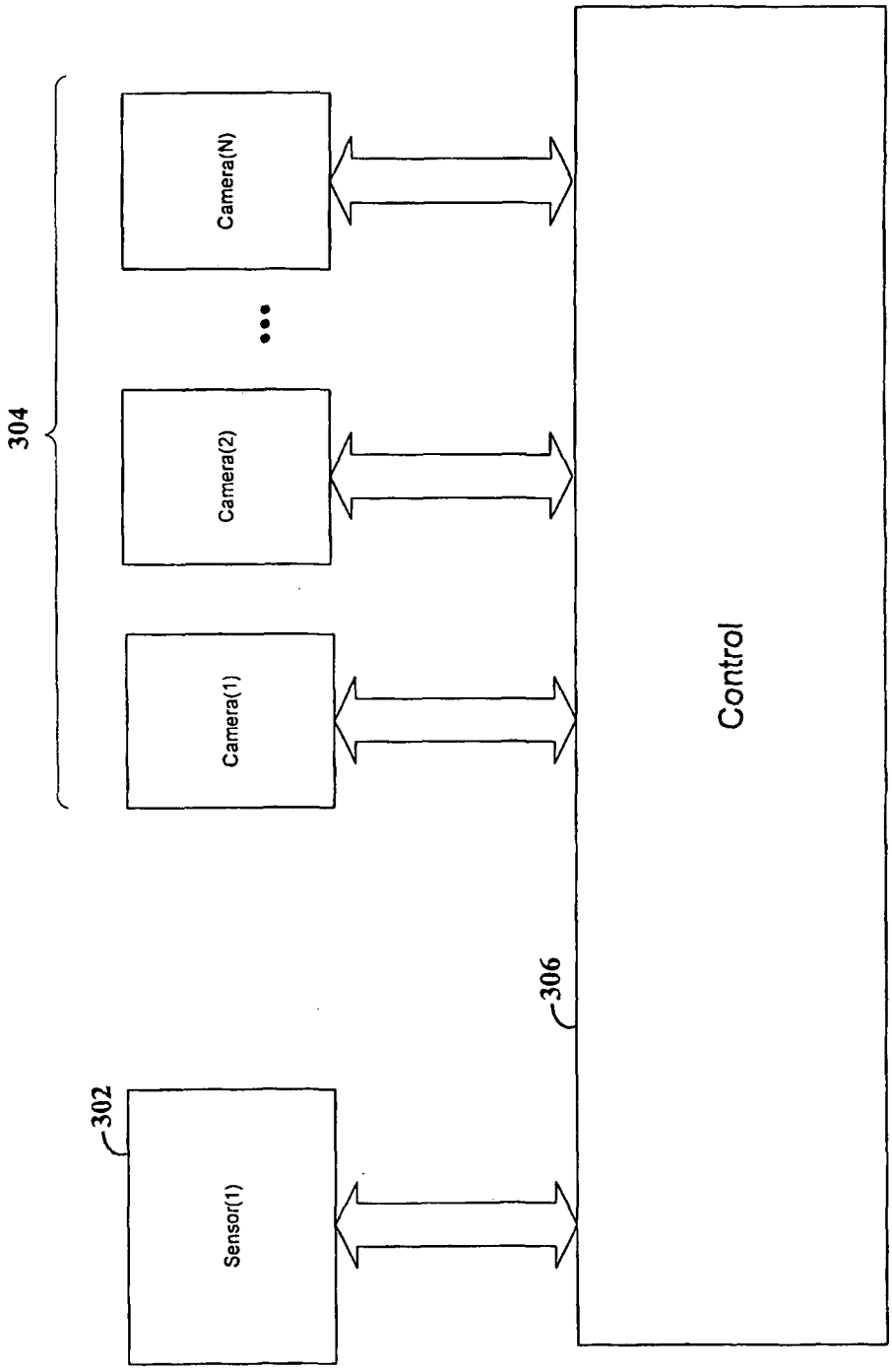
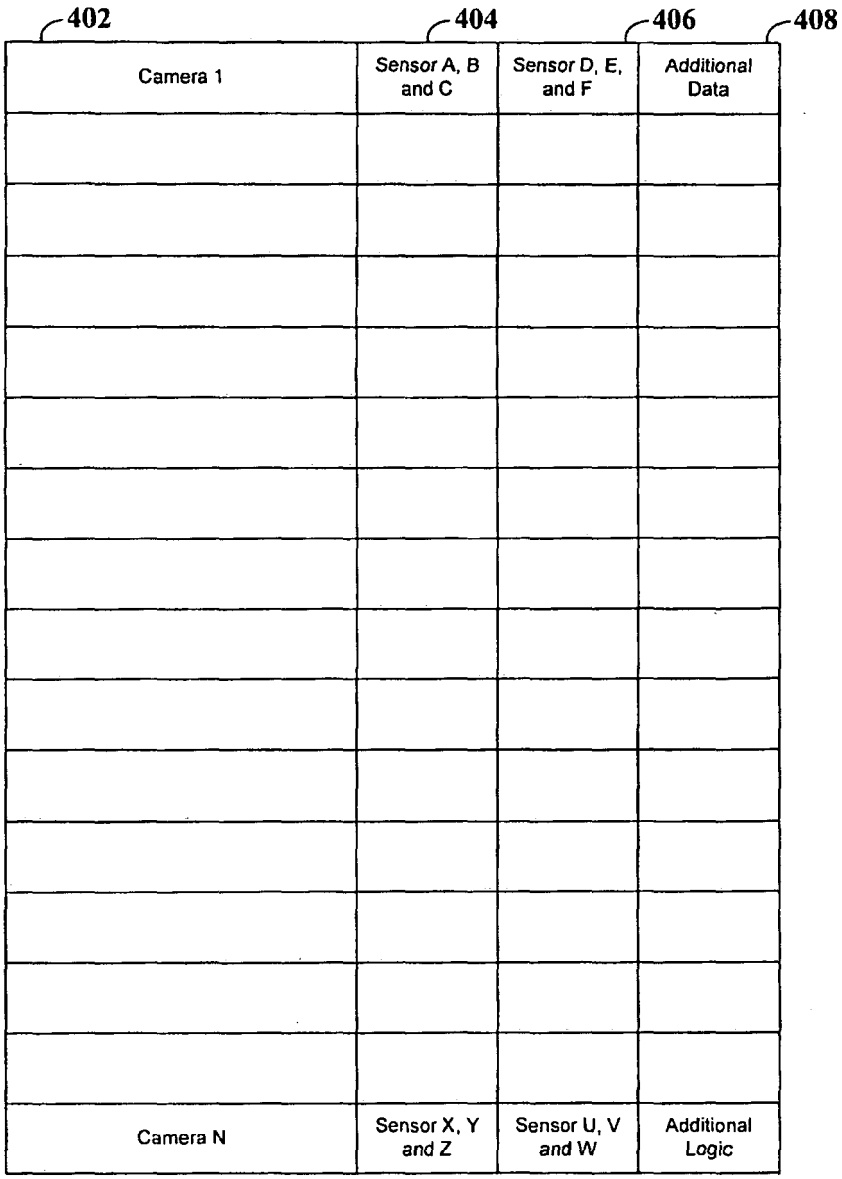


FIG. 4


402
404
406
408
Camera 1
Sensor A, B and C
Sensor D, E, and F
Additional Data
Camera N
Sensor X, Y and Z
Sensor U, V and W
Additional Logic

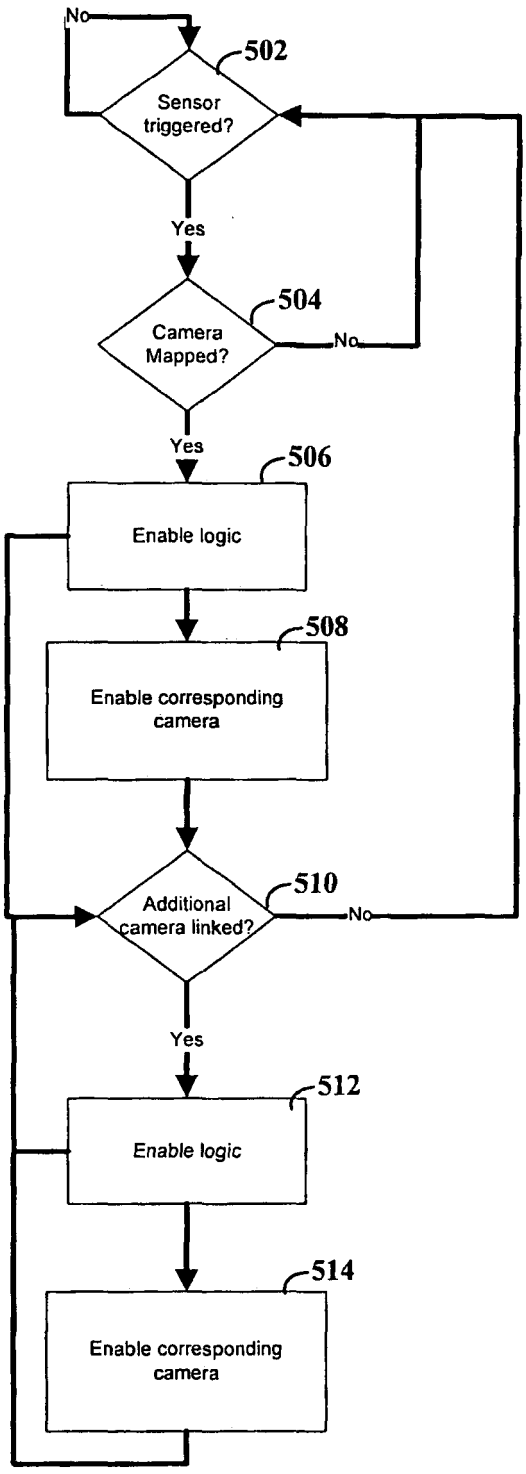

No
502
Sensor triggered?
Yes
504
Camera Mapped?
No
Yes
506
Enable logic
508
Enable corresponding camera
510
Additional camera linked?
No
Yes
512
Enable logic
514
Enable corresponding camera

FIG. 5

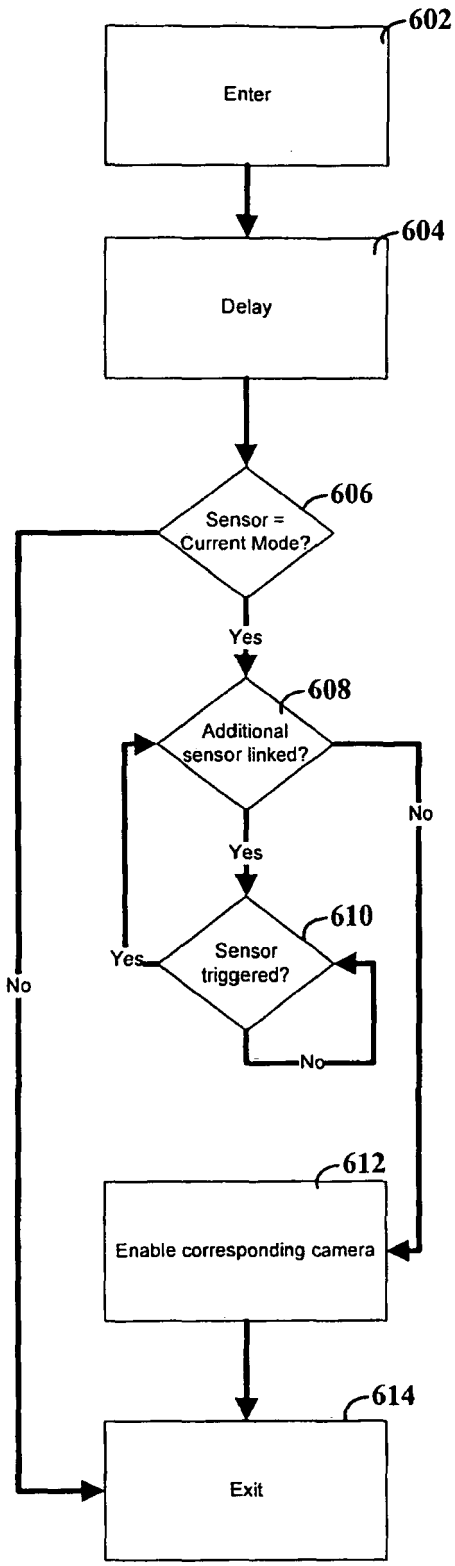

602
Enter
604
Delay
606
Sensor = Current Mode?
Yes
No
608
Additional sensor linked?
Yes
No
610
Sensor triggered?
Yes
No
612
Enable corresponding camera
614
Exit

FIG. 6

FIG. 7

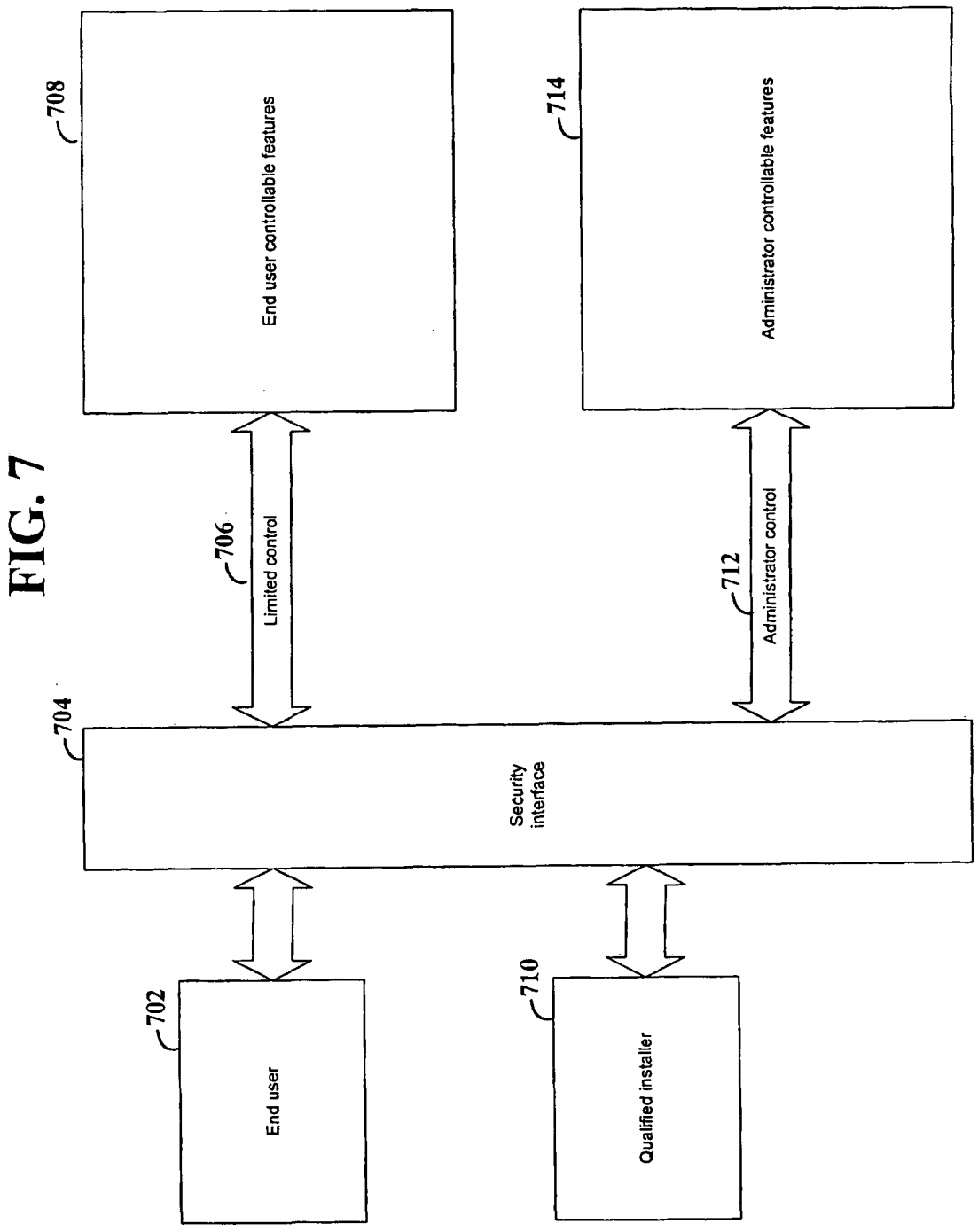

708
End user controllable features
714
Administrator controllable features
706
Limited control
712
Administrator control
704
Security interface
702
End user
710
Qualified installer

FIG. 8

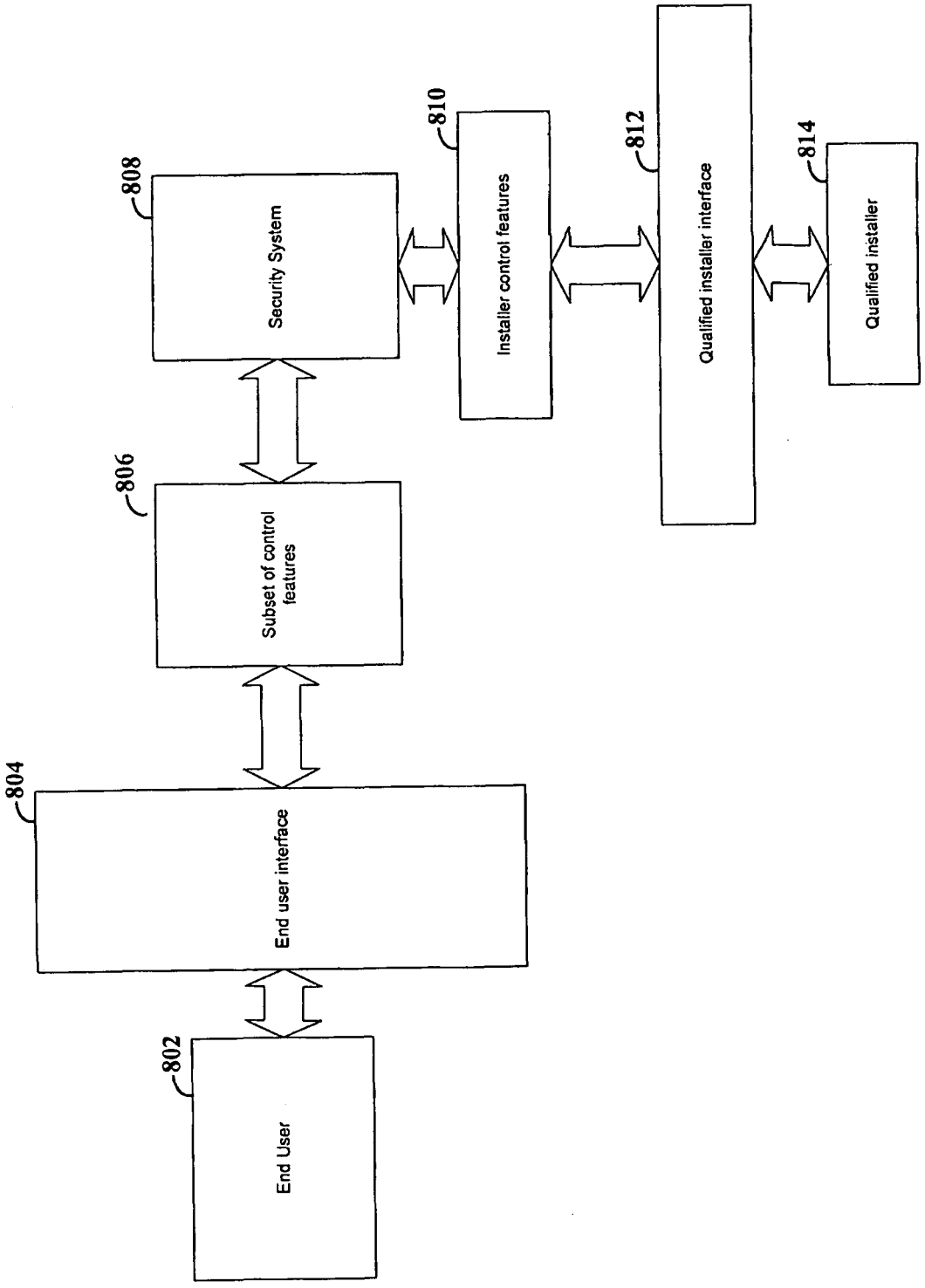
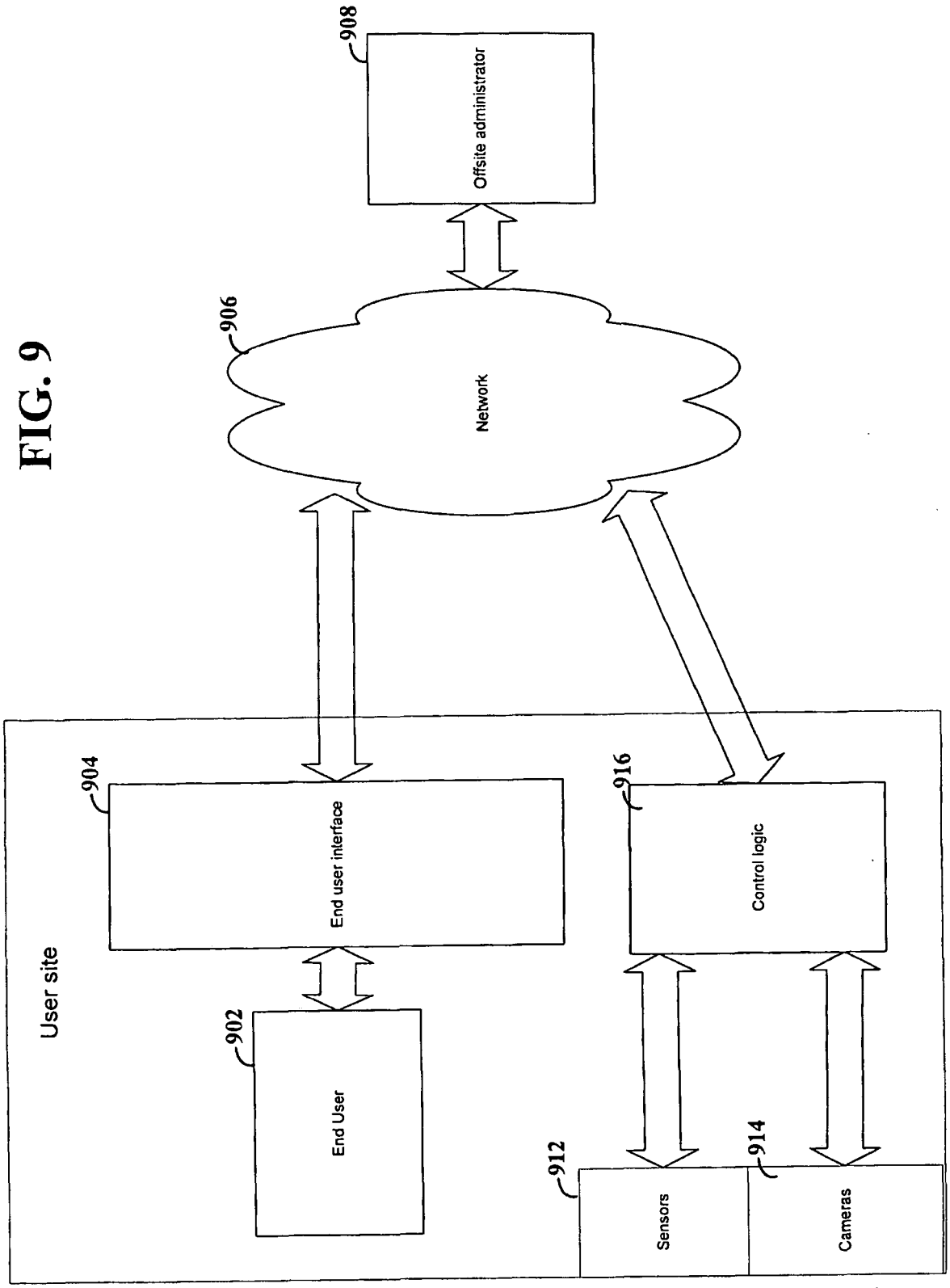

802
End User
804
End user interface
806
Subset of control features
808
Security System
810
Installer control features
812
Qualified installer interface
814
Qualified installer

FIG. 9


908
Offsite administrator
906
Network
User site
904
End user interface
916
Control logic
902
End User
912
Sensors
914
Cameras

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 1363260 A **[0008] [0042]**
- US 20050162268 A **[0013]**
- US 60785570 B **[0042]**
- US 38967306 A **[0042]**