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

(11) **EP 4 560 599 A1**

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.05.2025 Bulletin 2025/22

(21) Application number: **23383199.9**

(22) Date of filing: **22.11.2023**

(51) International Patent Classification (IPC):
G08B 25/00 *(2006.01)* *G08B 29/18* *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G08B 25/001; G08B 25/008; G08B 29/18

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA
Designated Validation States:
KH MA MD TN

(71) Applicant: **Verisure Sàrl**
1290 Versoix (CH)

(72) Inventors:
- **AHLBECK, Linnea**
  211 19 Malmö (SE)
- **MORGAN, Russel**
  211 19 Malmö (SE)

(74) Representative: **Elion IP, S.L.**
Paseo Castellana, 150-4 dcha
28046 Madrid (ES)

(54) SECURITY MONITORING SYSTEMS AND METHODS

(57) Provided is a method, performed by a system that comprises a security monitoring system installation at premises protected by the installation, the security monitoring system having a disarmed mode and at least one armed mode, method comprising:
i) detecting the occurrence of an event at the premises while the security monitoring system is in the disarmed mode;
ii) transmitting a notification in respect of the event to a user device, the notification including event data; and
iii) only in response to receiving a user reaction to the notification indicating a desire/wish to raise an alert in respect of the event with a monitoring station remote from the premises, notifying the monitoring station and providing the monitoring station with access to the event data.

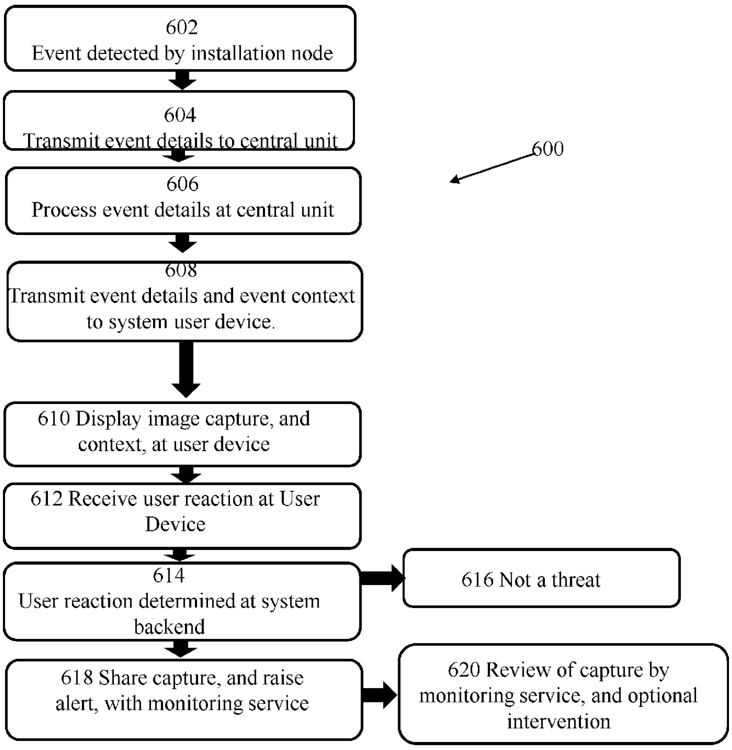
602
Event detected by installation node
604
Transmit event details to central unit
606
Process event details at central unit
608
Transmit event details and event context to system user device.
610 Display image capture, and context, at user device
612 Receive user reaction at User Device
614
User reaction determined at system backend
616 Not a threat
618 Share capture, and raise alert, with monitoring service
620 Review of capture by monitoring service, and optional intervention
600

Figure 6

Description

Technical field

[0001] The present invention relates to security monitoring systems and methods.

Background

[0002] Security installations that are or include security monitoring systems for monitoring premises, often referred to as alarm systems, typically provide a means for detecting the presence and/or actions of people at the premises and reacting to detected events. Commonly such systems include sensors to detect the opening and closing of doors and windows to provide a secure perimeter to the premises, creating one or more protected interior spaces, movement detectors to monitor spaces (both within and outside buildings) for signs of movement, microphones to detect sounds such as breaking glass, and image sensors to capture still or moving images of monitored zones, and optionally smoke and/or fire detectors. Such systems may be self-contained, with alarm indicators such as sirens and flashing lights that may be activated in the event of an alarm condition being detected. Such installations typically include a control unit (which may also be termed a central unit), generally mains powered, that is coupled to the sensors, detectors, cameras, etc. ("nodes"), and which processes received notifications and determines a response. The central unit may be linked to the various nodes by wires, but increasingly is instead linked wirelessly, rather than by wires, since this facilitates installation and may also provide some safeguards against sensors/detectors effectively being disabled by disconnecting them from the central unit. Similarly, for ease of installation and to improve security, the nodes of such systems typically include an autonomous power source, such as a battery power supply, rather than being mains powered.

[0003] As an alternative to self-contained systems, a security monitoring system may include an installation at a premises, domestic or commercial, that is linked to a remote Central Monitoring Station (CMS) or Alarm Receiving Centre (ARC) (the terms are interchangeable) where, typically, human operators manage the responses required by different alarm and notification types. In such centrally monitored systems the central unit at the premises installation typically processes notifications received from the nodes in the installation and notifies the Central Monitoring Station of only some of these, depending upon the settings of the system and the nature of the detected events. In such a configuration, the central unit at the installation is effectively acting as a gateway between the nodes and the Central Monitoring Station. Again, in such installations the central unit may be linked by wires, or wirelessly, to the various nodes of the installation, and these nodes will typically be battery rather than mains powered.

[0004] In such centrally monitored systems, the personnel of the CMS may raise an alarm with the police or other emergency services (such as a Fire Brigade, or a medical service) in the event that an alarm notification is received from the monitored premises. But frequently penalties (e.g. significant fines) are applied if a provider of a managed alarm service raises with the emergency service an alarm (or more than a certain number of alarms within a predetermined period) where the alarm(s) turn out to be false alarms. Under certain circumstances a service provider may even be prohibited from reporting alarm events at all. Consequently, service providers try to ensure that alarm events are only notified to the emergency services once they have been confirmed in some way - for example by performing a visual check of feeds from cameras installed at the premises, or by listening to sounds (e.g. sounds characteristic of a burglar ransacking premises following the triggering of a door or window sensor, the sounds of an argument, altercation or fight, after the triggering of an SOS or personal alarm sender, etc.), or by contacting someone associated with the premises, e.g. the owner, to confirm whether or not an alarm has been triggered accidentally - as is often the case.

[0005] Such security monitoring systems contribute to the safety and wellbeing of occupants of the protected premises, as well as safeguarding articles within the protected perimeter - which may of course not simply be limited to a house or dwelling but may also extend to the grounds of the house, protected by a boundary fence and gate, for example.

[0006] Generally, a centrally monitored security monitoring system only reports alarm events if the system is armed - with the possible exceptions of fire and smoke detection, SOS alerts or the triggering of a personal alarm of the type worn or carried by the elderly or infirm. But the applicants have realised that there may be occasions in which it may be beneficial to be able report an event to the central monitoring station even though the security monitoring system is disarmed. For example, the security monitoring system may be disarmed when children are home alone but a potential threat may be recognised in the presence of a person in the garden of the premises (although the same threat may also be recognised when the security monitoring system is in an "armed at home" mode). Equally, the security monitoring system may be disarmed to allow a cleaner to perform cleaning duties within the protected premises but part of the premises may be "out of bounds", for example a home office, and thus detection of the presence of someone within the home office may be cause for alarm (again, the same threat may also be recognised when the security monitoring system is in an "armed at home" mode). There are of course many other potential scenarios where detection of a person, or of some other event, may indicate the existence of a threat or cause for alarm even though the security monitoring system is disarmed. But of course the same events may be entirely innocent and non-threatening - it all depends upon their context.

[0007] Embodiments of the present invention seek to provide enhanced security monitoring systems, and corresponding applications, methods and other implementations that improve the ability of security monitoring systems for handling potential alarm events that are detected preferably while a premises security monitoring system is in a disarmed mode or optionally in an armed at home mode, as well as providing corresponding new functionality and methods.

Summary

[0008] According to a first aspect there is provided a method, performed by a system that comprises a security monitoring system installation at premises protected by the installation and optionally a system back end remote from the premises, the method comprising:

i) detecting the occurrence of an event at the premises;
ii) transmitting a notification in respect of the event to a user device, the notification including event data;
iii) in response to receiving a user reaction to the notification indicating a desire/wish to raise an alert in respect of the event with a monitoring station remote from the premises, notifying the monitoring station and providing the monitoring station with access to the event data.

[0009] As noted above, the detecting the occurrence of an event and the transmission of a notification in respect of the event may occur while the security monitoring system is in its disarmed mode.

[0010] The method of the first aspect may further comprise the step of reporting, prior to step ii), the occurrence of the event to a system back end remote from the premises, wherein the system back end performs either of steps ii) or iii).

[0011] In the method of the first aspect the step of transmitting a notification in respect of the event to a user device is performed by the security monitoring installation, wherein the security monitoring installation performs either of steps ii) or iii),
optionally wherein the installation comprises a controller, and the step of transmitting a notification in respect of the event to a user device is performed by the controller, and wherein the controller performs either of steps ii) or iii).

[0012] In any variant of the first aspect, the notification in respect of the event may include at least one of:

an image related to the event, and optionally wherein the image is a still image; and/or
a link giving access to a video capture related to the event.

[0013] In any variant of the first aspect, the event may be at least one selected from:

sensor based detection of motion;
sensor based detection of presence.
triggering of a window sensor, optionally a contact switch, magnetic sensor, or a shock sensor; triggering of a door sensor, optionally a contact switch, magnetic sensor, or a shock sensor;

[0014] In any variant of the first aspect, whether the notification of step ii) is transmitted or not may depend upon at least one condition selected from:
the time of day, day of the week, date, nature of the event, or some combination thereof.

[0015] In any variant of the first aspect, the notification may further include context information, the context information distinct from the event data and complementing the event data, optionally wherein the context information includes one or more selected from: the arm state; occupation state of the premises; camera identity; status of other detectors at the premises.

[0016] According to a second aspect there is provided a method, performed by a system that comprises a security monitoring installation at premises protected by the installation and optionally a system back end remote from the premises, the security monitoring installation having a plurality of arm states and being configured to report to a monitoring station remote from the premises, the method comprising:

i) capturing the occurrence of an event at the premises;
ii) transmitting a notification in respect of the event to a user device, the notification including event data and optionally context information; and
iii) only in response to receiving a user reaction to the notification indicating a desire to raise an alert in respect of the event with the monitoring station, notifying the monitoring station and providing the monitoring station with access to the event data and optionally the context information.

[0017] According to a third aspect, there is provided a system that comprises a security monitoring installation at premises protected by the installation and a system back end remote from the premises, the security monitoring installation having a disarmed mode and at least one armed mode the security monitoring installation having a controller and a plurality of sensors configured to transmit event notifications to the controller, the controller being configured when the system is in an armed mode to report alarm events to a monitoring station remote from the premises, the controller having at least one operating mode in which it is configured to respond to receiving certain event notifications, optionally while the installation is in the disarmed mode, by transmitting an alert, in respect of the notification of an event, to the system back end remote from the premises,
the system back end being configured to:

i) transmit a notification in respect of the event to a user device, the transmitted notification including event data and optionally context information;
ii) raise an alert in respect of the event with a monitoring station remote from the premises only in response to receiving from a user at the device a user reaction to the transmitted notification indicating a desire to raise an alert in respect of the event; and,
iii) if an alert is raised with the monitoring station in respect of the event to provide the monitoring station with access to the event data and optionally context information.

[0018] According to a fourth aspect, there is provided a security monitoring installation at premises protected by the installation, the installation having a disarmed mode and at least one armed mode, the installation comprising a controller and a plurality of sensors configured to transmit event notifications to the controller, the controller having at least one operating mode in which it is configured to respond to certain event notifications, optionally while the installation is in the disarmed mode, by:

i) transmitting a notification in respect of the event to a user device, the transmitted notification including event data and optionally context information;
ii) in response to receiving a user reaction to the transmitted notification indicating that the event is a false alarm or that the user does not wish to report the event to the monitoring station, determining not to notify the monitoring station of an alarm event in respect of the event;
iii) in response to receiving a user reaction to the transmitted notification indicating a desire to raise an alert in respect of the event with the monitoring station, notifying the monitoring station of an alarm event and providing the monitoring station with access to the event data and optionally the context information; and
iv) in response to not receiving within a predetermined time period a user reaction to the transmitted notification, not notifying the monitoring station of an alarm event (in respect of the event).

[0019] In a system according to the third aspect or an installation according to the fourth aspect, the context information may be distinct from the event data and complementing the event data, the context information may include one or more selected from: the arm state; occupation state of the premises; camera identity; status of other detectors at the premises.

[0020] In a system according to the third aspect or an installation according to the fourth aspect, the transmitted notification in respect of the event may include at least one of:

an image related to the event, and optionally wherein the image is a still image; and/or
a link giving access to a video capture related to the event.

[0021] In a system according to the third aspect or an installation according to the fourth aspect,, the event may be at least one selected from:

sensor based detection of motion;
sensor based detection of presence;
triggering of a window sensor, optionally a contact switch, magnetic sensor, or a shock sensor;
triggering of a door sensor, optionally a contact switch, magnetic sensor, or a shock sensor.

[0022] In a system according to the third aspect or an installation according to the fourth aspect, whether the notification of i) is transmitted or not may depend upon at least one condition selected from: the time of day, day of the week, date, nature of the event, or some combination thereof.

Brief description of Figures

[0023] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying Figures, in which:

Figure 1 is a schematic view of the front of a premises 100 protected by a security monitoring installation according to an aspect of the present invention;
Figure 2 is a schematic plan view of the premises of Figure 1 illustrating elements of the installation and a system of which it forms part;
Figure 3A illustrates schematically, at a high level, a method according to an aspect of the invention;
Figure 3B illustrates schematically, at a high level, another method according to an aspect of the invention;
Figure 4 is a flow chart illustrating a method according to an aspect of the invention;
Figure 5 illustrates schematically, at a high level, another method according to an aspect of the invention;
Figure 6 is a flow chart illustrating a method according to an aspect of the invention;
Figure 7 illustrates schematically, at a high level, another method according to an aspect of the invention; and
Figure 8 is a flow chart illustrating a method according to an aspect of the invention.

Specific description

[0024] Figure 1 shows a view of the front of a premises 100 protected by a security monitoring system according to an aspect of the present invention. The premises, here is in the form of a house, surrounded by a garden defined in part by a border fence 101 to the rear and sides of the property. The house has at least one exterior door, here front door, 102. The door gives access to a protected interior space. The security monitoring system secures at least part of a perimeter to the premises 100, and the door constitutes an exterior closure 102 in the secure perimeter giving access to a protected interior space 201 of the premises. A lock 104 on the exterior door is optionally electrically controlled so that it can be locked and unlocked remotely.

[0025] To the side of the door, on the facade of the house, is a first video camera in the form of a video doorbell 106 which looks out from the facade of the premises so that anyone approaching the door along the path 108 can be seen, and in particular when a visitor stands at the door their face should clearly be visible. The video doorbell includes an actuator, e.g. a push button, for a visitor to indicate their presence at the closure. The video doorbell also includes an audio interface to enable bidirectional audio communication with a visitor at the closure 102.

[0026] The video doorbell preferably includes an infrared light source to illuminate whatever or whoever is in front of the video doorbell. Optionally, as shown, the facade of the house also carries an external keypad, or access node, 110 by means of which a user can disarm the security monitoring system, and unlock the lock 104 if fitted, by entering an access code or by presenting a security tag, dongle, or suitably coded mobile device - for example using NFC. Also shown is an optional second video camera 112 which is coupled to a presence and/or movement detector 114. The detector may optionally be a thermal detector, for example a PIR sensor. The second video camera 112 may be arranged to capture video of the front of the house and the private area, e.g. the garden, in front of the house and to signal events to a controller of the security monitoring system. As with the doorbell camera, the second video camera is preferably provided with an audio interface 116 to enable bidirectional audio communication with anyone observed by the second video camera. Although the first video camera is illustrated in the form of a video doorbell, the first video camera may additionally or alternatively have the features described above for the second video camera, whether or not plural video cameras are used. A further video camera may also be provided to the rear and or side of the house to capture video of the side and/or rear of the house and the private area, e.g. the garden, to the side or rear of the house and to signal events to a controller of the security monitoring system. As with the second video camera the further video camera is preferably provided with an audio interface 116 to enable bidirectional audio communication with anyone observed by the further video camera.

[0027] The security monitoring system may provide the following arm state options:

i) armed away, in which alarm events include perimeter breaches (including optionally shock sensing in addition to door/window opening), internal presence/movement (plus fire/smoke/SOS as necessary)

ii) armed at home, in which perimeter breaches are detected (plus fire/smoke/SOS as necessary)

iii) disarmed - only fire/smoke/SOS

But an option for modes ii) and iii) is escalation following user notification in respect of any detected event, as will be explained later.

[0028] Figure 2 is a schematic part plan view of a premises 100 protected by security monitoring system according to an aspect of the invention, together with other elements of the system, corresponding generally to the premises of figure 1. The front door 102, with the optional electrically controlled lock 104, leads into an entrance hall 200 that is part of the protected interior space of the premises which also includes a study or home office 201. Each of the windows 202, and external doors (including rear door 204) is fitted with a sensor 206 (e.g. contact switch) to detect when the door is opened. Each of the sensors 206 preferably includes a radio transceiver to report events to a controller , or central unit, 208 of the security monitoring system. If one of the sensors 206 is triggered a signal is sent to the central unit 208 which in turn may (typically depending upon that arm state of the security monitoring system) signal an alarm event to a remote central monitoring station 210. The central unit 208 is preferably connected to the remote central monitoring station 210 via the Internet 211, via a wired or a wireless connection, or both.

[0029] The security monitoring installation at the premises is also coupled to a system back end 230 (typically comprising one or more servers with associated memory, programs and data storage) which may be functionally separate from the central monitoring station 210 or they may form part of a common back end function 240 - although of course whether or not the back end function and the central monitoring station form a common back end function, their hardware may be co-located or located at different geographical sites, and the human operators may be co-located with the relevant system hardware or access it through terminals that are themselves remote from the relevant hardware. The central monitoring station 210 is able to call upon the emergency services (e.g. police, fire brigade, medical) 250.

[0030] Also coupled (optionally wirelessly) to the central unit 208 are the video doorbell 106, the electrically controlled lock 104 (if present), and also if present the second video camera 112 and the rear video camera 212, and its/their associated presence and/or movement detectors 114 (although the latter may be integral with the relevant video camera 112/212) and the audio interface 116. A control panel 227 may also be provided, for example within the protected space of the premises, for the arming and disarming of the security monitoring system. These items, and the sensors 206, are preferably coupled to the central unit 208 using transceivers operating in the industrial scientific and medical (ISM) bandwidths, for example a sub-gigahertz bandwidth such as 868 MHz, and the communications are encrypted preferably using shared secret keys. The security monitoring system may also include other sensors within the protected interior space, such as an interior video camera 214 and associated movement detector 216 (which again may be integral with the camera 214), and each of the interior doors 218 may also be provided with a sensor 206 to detect the opening/closing of the door. One or more fire and/or smoke detector nodes 252 may also be provided within the protected premises. Also shown in figure 2 are a user device 220 (such as a smartphone), preferably loaded with an appropriate app - as will be described later, and a public land mobile network (PLMN) 222 by means of which the central monitoring station 210, and the central unit 208, may communicate with the user device 220.

[0031] The study 201, like the rest of the rooms in the protected premises, may include a stand-alone motion sensor, such as a PIR, 216' to detect presence or motion within the room. The motion sensor may be a "smart" motion sensor such as one that uses artificial intelligence to help distinguish between the presence of an animal, such as a pet dog or pet cat, and a human. Such sensors can distinguish reliably between movement of a pet animal and movement of a human who crawls along the floor, for example, and can readily distinguish between a standing or crouching human and a pet animal. As such, such smart motion/presence sensors can contribute significantly to a reduction in the incidence of false alarms. The study 201 may also include a camera, optionally a video camera, 214' which may include or be associated with a smart motion/presence sensing detector.

[0032] In some embodiments, rather than using a motion/presence detector to trigger a camera of the installation, one or more cameras of the installation may be configured to capture images continuously or quasi continuously, the captured images then being shared with an image analysis system or arrangement that detects the existence of motion by analysing differences between images taken at different times. The image analysis system or arrangement being arranged to provide a "motion detected" signal, for example to a controller of the installation, so that the detection of motion can be used as a trigger for further action. Examples of such an approach are described further with reference to figures 7 and 8.

[0033] In various embodiments operation of the security monitoring system may be controlled by one or more of: the controller 208, the control panel 227, the remote monitoring station 210, and a security monitoring app installed on the user device 220. For example, the remote monitoring station 210, may receive one or more signals from any of the first camera and/or video doorbell 106, the second camera 112/212, the keypad 110, the sensors 206,252 . The remote monitoring station 210 may transmit commands for controlling any one or more of: the arm state of the alarm system (e.g. armed or unarmed); commanding a tripped alarm state to be signalled by the alarm system (e.g. by triggering one or more sirens to generate alarm noise); commanding a lock state of the door lock 104 (e.g. locked or unlocked), commanding operation of one or more functions of the video doorbell 106, commanding operation of one or more cameras to transmit images to the remote monitoring unit. Communication with the remote monitoring station 210 may pass through the controller 208, as described above. In other embodiments without the remote monitoring station 210, or should communication with the remote monitoring station 210 be interrupted, operation of the alarm system may be controlled by the controller 208. In yet other embodiments, the controller 208 may be omitted, and the individual peripheral devices may communicate directly with the remote monitoring station 210 and/or system back end 230/240.

[0034] The security monitoring system app is installed on a user device 220, here shown as a smartphone, although of course it could be almost any kind of electronic device, such as a laptop or desktop computer, a tablet such as an iPad, a smart watch, or even a television

[0035] In other embodiments the security monitoring installation may be configured without a central unit 208, the various nodes/sensors/cameras of the installation instead working on an edge computing basis, either each communicating directly with the remote monitoring station 210, system back end 230, or common back end function 240 (or at least having the inbuilt capability to do this), or one or more of the nodes/sensors/cameras/control panels acting as a gateway for the other nodes/sensors/cameras/control panels. Optionally at least the nodes/sensors/cameras/control panels that act(s) as the gateway may be powered from a mains power source (with battery back-up). The nodes/sensors/cameras/-control panels may form a self-organising system.

[0036] The security monitoring system may further comprise an audio interface to enable audio communication with a visitor at the closure 102, or at or within sight of any of the image capture devices (e.g. cameras or video cameras) of the installation, the controller 208 being configured to enable the remote monitoring centre 210 to use the audio interface to speak to the visitor (who may be a potential intruder). Likewise, the control panel 227 may include an audio interface to enable audio communication with the central monitoring station and optionally the user device (for example via the system back end 230/240).

[0037] Now imagine a situation in which a working parent has children of school age who get home some hours before the parent, or any other guardian or responsible adult, is able to get back to the protected premises of figures 1 and 2. Upon returning home the children disarm the security monitoring system, for example by presenting a security tag or dongle to an access node 110 adjacent an entrance door of the premises. Because the children are free to roam anywhere in the house, once a child has returned home - so that the home is no longer unoccupied, the security monitoring system is typically set to a disarmed state. Alternatively, the security monitoring system may be set instead to an armed at home state in which the periphery is secured so that later arrivals either need to disarm the system before opening an external access door, or the new arrival or one of the earlier arrivals needs to take appropriate action to avoid triggering an alarm event when an external access door has been opened - such as entering a code or presenting a security token to an internal control panel 227.

[0038] The children's parent(s) may be sufficiently concerned about the children's safety and wellbeing while they are home alone (i.e. without a responsible adult) that the parent(s) want to be alerted in the event that, for example, a human presence (or what could be a human presence) is detected in the vicinity of the home - for example in the back garden. Human presence may be detected by a motion sensor, especially by a smart motion sensor - either freestanding or associated with (e.g. part of) an image capture device such as a camera or video camera. Human presence may additionally or alternatively be sensed based on analysis of one or more images captured by a camera or video camera, for example using image analysis within or external of the image capture device.

[0039] In such a case the security monitoring system may be configured (e.g. programmed) to cause notifications to be sent to the parent(s) e.g. to one or more WTRU device associated with the parent(s) in the event that one or more sensors/nodes/cameras detects possible human presence within the monitored area. Such notifications preferably contain information that provides a context of the event - for example that the house is occupied only by vulnerable people (one or more children, or another vulnerable person/people) or predominantly vulnerable people - something which may be determined by capturing identities of the person/people disarming the installation using tag/device identity or PIN identity (i.e. by using individual PINs for different authorised users).

[0040] The installation may allow one or more particular individuals to indicate that a responsible adult is now present, for example by entering a particular code or presenting a particular tag/dongle or mobile device, or choosing a different setting at a control panel for the installation, so that the sending of notifications in this way can be turned off when no longer appropriate.

[0041] Such a configuration may be applied by the security monitoring installation both in a fully disarmed state and in an armed at home state (i.e. a state in which entrances (primarily doors and windows) to the premises are monitored to detect door and window opening events, shocks received by windows/doors (indicative of an attempt to break in)). It may be the case that notifications may be sent in response to the detection of events that would not be considered to be alarm events in an armed (e.g. armed away) mode. For example, in an armed away mode the mere presence of a person in the back garden of the premises does not necessarily constitute a threat sufficiently serious to justify involvement of emergency services - for example it may be a neighbour looking for a lost pet or a lost ball or toy. An alarm event may only be determined to exist based on outputs of a combination of sensors - such as, in addition to an image capture device or motion sensor sensing potential human presence, a door/window sensor sensing vibration or shock if the detected person tries to open or attack a door or window, or a microphone capturing sounds indicative of a potential break-in (e.g. the sound of breaking glass).

[0042] But a parent or guardian may have understandable fears for the safety of children or other vulnerable people who are at home - and these fears may manifest themselves in wanting to react quickly to potential threats before they develop into actual threats: in other words, a parent may want an intruder in the garden scared off or taken away before they actively attempt to break into or otherwise enter the protected space housing the children or other vulnerable people. This may make it interesting to notify someone such as the owner/occupier of the premises (e.g. a parent/guardian) of the existence of a potential threat so that that person may raise an alert in the event that the perceived threat is determined to be significant - while avoiding burdening the central monitoring station with alerts in respect of potential threats that are assessed as harmless.

[0043] If a user (e.g. parent or guardian) receiving such a notification is alarmed by the notification - for example if the notification includes an image capture which shows the presence of a person in the garden of the premises, and the person is either unknown or is known but their presence potentially represents a threat to the child/-children in the home, the user may be given an opportunity to escalate the event to the remote monitoring station 210, system back end 230, or common back end function 240. By also making the relevant event data and context information available to the remote monitoring station 210, system back end 230, or common back end function 240, personnel responsible for remote monitoring can make a determination of the best way to handle the incident. In this way, a parent's concerns based on a notified event can be acted upon even though the event would not otherwise have given rise to an alert to the remote monitoring personnel.

[0044] It must be realised that this approach is not restricted to the scenario set out previously. There are numerous other situations where a similar approach of a notifying a user of the detection of an event, when the installation is disarmed or in an armed at home mode, to give the user an opportunity to flag the event to monitoring personnel on the basis that the user found the content of the notification sufficiently alarming to warrant intervention. For example, protected premises may contain a room or other place from which the owner wants to exclude others - or at least to exclude unauthorised visitors - for example a home office or an art gallery or collection space with valuable or prized exhibits. The owner may employ a cleaner or other support staff who are free to wander over the protected premises apart from such no-go areas. Giving the support staff freedom to move into and through the bulk of the protected premises will typically mean needing to set the security monitoring installation to a disarmed or armed at home mode. But if one of the support staff enters (or possibly even approaches) a no-go area, the user wants to be notified so that for example the event can be handed over to the monitoring service. Under some circumstances it might be possible to treat one or more no-go areas as special security zones and to configure the security monitoring installation to provide an armed protection mode for such no-go areas while the rest of the installation is disarmed or only in an armed at home mode - but this would be inappropriate if certain household members, and possibly others, are likely to enter one or more of the no-go areas innocently and without any kind of threat. For example, school children may need to enter the home office to access the home's printer or other office equipment, or the art gallery or collection room may be where children like to hang out after school. Hence there may be value in providing the above-described user-notification option, so that a user can raise an alert when appropriate without the risk of false alarms being raised as threats/alarms with the monitoring service.

[0045] This method in various guises will now be explained further with reference to the remaining figures.

[0046] Figure 3A illustrates schematically, at a high level, a method according to an aspect of the invention. Here we assume that the premises installation 200, which may correspond to the installation described with reference to Figures 1 and 2, is in a disarmed or armed at home state, for example following the return of young schoolchildren from school. At 300 an event is detected by a sensor or node of the installation, for example a motion sensor associated with a camera, such as camera 212, overlooking the back garden is triggered.

[0047] If the installation includes a central unit, such as central unit 208, the triggered sensor will send an event alert message to the central unit, and the central unit will then process the alert message at 302. The event alert message/report preferably includes parameters of the event, the sensor's identity and if relevant the nature of the event detected. For example camera 212 may be arranged to capture an image (e.g. a still image or a brief video clip) upon its associated (possibly internal) motion sensor being triggered, and then to send an event alert, optionally including the captured image, to the central unit. Based on the prevailing system settings the central unit determines that despite the arm state of the installation being disarmed, or merely armed at home, a user is to be notified of the event. Based on this determination, the central unit then reports to the back end system 230/240 the occurrence of an event at the premises 100.

[0048] If the installation is configured without a central unit, a processor of the triggered sensor will at step 302 process the event data to determine how it should be handled. Based on the prevailing system settings the processor may determine that despite the arm state of the installation being disarmed, or merely armed at home, a user is to be notified of the event. Based on this determination, at step 304 the sensor's processor then reports to the back end system 230/240 the occurrence of an event at the premises 100, for example using a PLMN. The event alert message/report preferably includes parameters of the event, the sensor's identity and if relevant the nature of the event detected. Again, if the sensor is a camera, such as camera 212, it may be arranged to capture an image upon its associated (possibly internal) motion sensor being triggered, and then to send an event alert, optionally including the captured image, to the back end system 230/240.

[0049] At step 305 the back end system 230/240 processes the alert, determining the nature of the alert and identifying the installation from which the report was received, and based upon this identification determining relevant user contact details (such as SIP address, mobile device number, etc.) to be used for any user contact.

[0050] At step 306 the back end system 230/240 transmits parameters of the event to a user device 220, for example in the form of a push notification. The parameters transmitted at this stage may be the same as those received from the installation 200, for example if the received parameters comprise an image file or video clip the image file or video clip (optionally including both sound and visual components) is forwarded to the user device. Optionally, received image/video content may be labelled or tagged to identify the precise source of the image/video capture. Additional or alternative parameters may be transmitted to the user device, for example a textual or graphical message may be composed to inform the user of the type of sensor (e.g. door or window sensor, shock sensor, smoke detector, fire detector, motion detector) and/or its location (e.g. door or window name, room name or other location descriptor), and the nature of the event detected (e.g. tamper detected, door/window opened, door/window shock sensed, smoke detected, fire detected, sound detected, etc.). A graphical display format may be used to facilitate comprehension both of the location of the event (e.g. by including an outline map to indicate the location of the detected event with respect to an outline or plan of the protected premises, and/or by labelling the display with a name of the location) and the nature (motion detection, person detection, door/window sensor (+ type) triggered) and/or severity of the event.

[0051] At step 308 the parameters received at the user device are displayed on a display of the device 220. The user device 220 will typically host an app for the security monitoring system, to enable the user to view communications from the system back end 230/240, images/video from cameras at the installation (e.g. from a doorbell camera of the installation) and also optionally to enable a user to speak to someone at the video doorbell, or at other nodes of the installation.

[0052] The parameters are preferably sent in a push notification that will display on lock-screen or at least give rise to a user alert on the device to prompt the user to view the notification. The notification may be an action notification that includes, for example, an action button or that permits a user to respond by clicking or "pushing" on the notification as a way to enter a response. Where the received parameters include a video clip or image, the user may be able to indicate a part of the image - e.g. a person or a person's face, by "drawing" (i.e. annotating) on the display using a finger, finger nail, or stylus, for example, to enable the user to identity a person (or some other thing) - e.g. to indicate someone whose presence is unauthorised or otherwise problematic, so that personnel at the central monitoring station can take appropriate action. Alternatively, the notification may include an icon or button for the user to indicate that there is no cause for alarm (e.g., an "all OK" button).

[0053] Optionally, the app may be configured to communicate with the system backend 230/240 to inform the backend that the notification has been displayed. If the user is not concerned by the displayed event and its details they may choose to provide no response. In which case no response is sent to the system back end, and hence there is no escalation of the event to the remote monitoring station. The notification may include an option for the user to respond to indicate the absence of any perceived threat/risk, in which case, at step 312 the user response is transmitted to the system backend 230/240. Again there is no escalation of the event to the remote monitoring station.

[0054] Conversely, if the user's response at 310 indicates that the user is concerned/threatened or worried by the reported event, at step 314 the system back end notifies the remote monitoring centre 210 - signifying the user's concern. The remote monitoring centre 210 is also provided with access to the parameters of the event, together with any annotations or other input received from the user. The parameters may be transmitted to the remote monitoring centre 210 by the system back end 230, or they may be made available in some other way - for example by being shared within the back end system 240, or a link provided to the remote monitoring centre 201 by means of which the parameters (such as any image capture or video content) may be downloaded or otherwise accessed by the remote monitoring centre 210.

[0055] The personnel in the remote monitoring centre 210 upon receiving notification of the event are made aware that a user was alarmed by the details of the event, based on the event context (e.g. the fact that the event occurred when children were home alone, and possibly the time of day) and the event data made available to the user (for example any image capture, video capture, audio, etc.). The monitoring personnel are also able to review the event details and are further able to communicate with the monitoring installation, for example to request 316 access to further images or video from the relevant camera and also from any other cameras of the installation, and also to acquire audio from any microphones of the installation - all either via a central unit of the installation or directly with the relevant nodes if the installation does not include a central unit. Any requested captures or streams are provided by the installation to the remote monitoring centre 210 at step 318.

[0056] In this way, personnel in the remote monitoring centre 210 may for example be able to communicate orally with any intruder in the garden, for example by an audio interface in camera 212, hopefully to persuade them to leave the grounds of the premises, or the personnel may assess the situation and may report the incident to the emergency services or private security personnel if their involvement is required. Meanwhile, the personnel may liaise with the user via the user device, and optionally with those within the protected premises - for example via an audio interface in a control panel 227 of the installation.

[0057] Figure 3B corresponds generally to Figure 3A but illustrates a method in which the premises installation 200 is able to send notifications directly to the user device 220 rather than only via the system back end as in Figure 3A. Here we assume the same scenario as for Figure 3A. That is we assume that the premises installation 200, which may correspond to the installation described with reference to Figures 1 and 2, is in a disarmed or armed at home state, for example following the return of young schoolchildren from school. At 320 an event is detected by a sensor or node of the installation, for example a motion sensor associated with a camera, such as camera 212, overlooking the back garden is triggered.

[0058] If the installation includes a central unit, such as central unit 208, the triggered sensor will send an event alert message to the central unit, and the central unit will then process the alert message at 322. The event alert message/report preferably includes parameters of the event, the sensor's identity and if relevant the nature of the event detected. For example camera 212 may be arranged to capture an image (e.g. a still image or a brief video clip) upon its associated (possibly internal) motion sensor being triggered, and then to send an event alert, optionally including the captured image, to the central unit. Based on the prevailing system settings the central unit determines that despite the arm state of the installation being disarmed, or merely armed at home, a user is to be notified of the event. Based on this determination, the central unit prepares a notification to report the event and its context to a user device whose contact details (e.g. SIP address or mobile phone number) may be stored in the central unit. Using these contact details the central unit pushes a notification to the user device at step 324.

[0059] If the installation is configured without a central unit, a processor of the triggered sensor will at step 322 process the event data to determine how it should be handled. Based on the prevailing system settings the processor may determine that despite the arm state of the installation being disarmed, or merely armed at home, a user is to be notified of the event. Based on this determination, at step 324 the sensor's processor then prepares a notification to reports the event and its context to a user device whose details may be stored in the relevant sensor, for example using a PLMN. The event alert notification preferably includes parameters of the event, the sensor's identity and if relevant the nature of the event detected. Again, if the sensor is a camera, such as camera 212, it may be arranged to capture an image upon its associated (possibly internal) motion sensor being triggered, and then to send an notification, optionally including the captured image, to the relevant user device 220.

[0060] The display of the notification on the display of the user device, at step 326, and the following steps 328 to 336 correspond generally to steps 310 to 318 of Figure 3A and the above description of these applies equally in respect of Figure 3B.

[0061] Figure 4 illustrates schematically a method 400 according to an aspect of the invention in which an event at the premises 100 is captured as an image capture or video.

[0062] At step 402 a security monitoring installation at premises is in a disarmed state or in an armed at home state, and an event occurs at the protected premises leading to an image capture, for example as the result of a motion detector of or associated with a camera having been triggered. The camera may, for example, be a camera such as camera 212 having a view of the back garden of the protected premises. Triggering of the motion sensor results in activation of the associated camera and an image capture of the event either as one or more still images or in the form of a video sequence.

[0063] At step 404 the camera transmits the captured image to the system backend, preferably together with status information for the security monitoring installation such as arm state, occupant details or occupancy status (either in detail, e.g. with names of those determined to be present, or in terms of the presence of a least one "vulnerable" individual (e.g. a child or elderly or infirm person_ and the absence of a carer or responsible adult (e.g. possibly determined by the fact that no such person has touched in or entered the appropriate passcode or PIN)), and such other information as may be helpful in terms of giving a user context for the detected event. For example these data may be transmitted from the triggered node (e.g. camera) over a Wi-Fi link to a Wi-Fi router of the premises and thence via the Internet to backend 230/240.

[0064] Even if the camera is a video camera it may initially just provide a still image capture. Alternatively the camera may stream the video so that the back end receives a continuous or quasi-continuous video stream, or the camera may transmit a subset of the available video, in the form of one or more still images or video clips. The capture may also include an audio channel which is also transmitted to the system backend 230/240. The transmission(s) to the system backend 230/240 includes an identifier of some kind so that the backend knows from which security monitoring installation (and hence which premises) the event capture is being received. The system backend includes a database that maps installations/premises with a user identity. For each user identity the system backend preferably also stores contact details, including for example a SIP address, device phone number, other contact numbers and email addresses for each user identity, optionally in the same database that maps installations/premises with a user identity. On receiving an event capture from a premises installation, the system back end determines contact details for a user device to be contacted in case of alarm events. Using the relevant contact details, the system backend pushes a notification to the relevant device at step 406. The pushed notification includes the event capture (e.g. the image capture) and/or a link to any video stream, preferably together with an identifier or indication of the source of the event capture - e.g. a name assigned to the camera such as "Back Garden Camera", optionally also with an indication of the time and date of the event capture.

[0065] Following delivery of the push notification to the user device, the user interacts with the user device to access the notification, causing the event capture (e.g. image capture) to be displayed on a display of the user device at step 408. This may involve the user clicking on (or otherwise selecting) a link to a remote site from which the video may be downloaded or streamed. The user then views the image capture (image or video clip or stream) on the user device to determine whether or not the notified event raises any cause for concern. If the event doesn't give rise to any concerns, the user may click on an icon, button or the like to indicate that no issues arise - the icon or button optionally being labelled with a designation signifying that no issues arise - e.g. "all OK", "no concerns", "no problem", and/or colour coded (e.g. colour coded green for safe), causing an appropriate indication to be captured at step 410. Optionally, a user may indicate a lack of concern, and hence no interest in the event being escalated to the remote monitoring centre, by failing to provide an active response - in which case the detected event will not be reported to the monitoring station as an alarm event (and in general my not be reported to the monitoring station at all, but may be logged as a "negative event" -i.e. one in response to which the user did not raise an alert) . If this mode of providing an indication of indifference is supported the app in the user device is preferably configured to signal to the system backend the fact of the event capture having been displayed. The system backend may then set a timer at the expiry of which, if no active response has been received, it can be assumed that the user has no interest in escalating the event to the ARC. This method of indicating user indifference may be used selectively, for example only for events that are perceived to be unlikely to be threatening - and that may be based on time of day, location of the relevant video camera, and whether other nodes of the installation have also been triggered.

[0066] Conversely, if the event capture is a cause for alarm, the user may take an action to indicate that they wish the event to be flagged to the remote monitoring station 210. Such an action may be to interact with an icon or button colour coded red, or labelled with a designation signifying that there is a problem or that the event notification causes the user alarm - e.g. "Escalate to ARC", "action required", "I don't like this", etc.. Additionally or alternatively, the user may be able to indicate concern by pressing on the display on which the event capture is being displayed. Also, as previously mentioned, the user may have the option to draw on the image capture (either in the form of a still or in the form of a video sequence) to draw around a feature of the displayed image or to add a label or tag, to indicate a person or some other feature of the displayed image (video) whose presence gives rise to concern - e.g. to indicate a stranger or a known person whose presence is unwelcome. The drawing, tagging, or labelling may be captured in the form of a layer or overlay whose details may be transmitted to the system backend for sharing, by onward transmission or otherwise, with the remote monitoring centre 210.

[0067] At step 412 the system backend determines the user reaction, optionally by receiving an indication of the perception of a threat or by receiving an indication that the event gives the user no cause for concern. As already noted, a user may also indicate that an event is not a cause for concern by not providing any overt response, with the system backend determining no cause for concern if no response is received from the user within a predetermined period.

[0068] If it is determined that a reported event does not give the user any cause for concern, the system back end ends the process at step 414 and does not escalate the event to the remote monitoring centre.

[0069] Conversely, if it is determined that the user is concerned, alarmed, or threatened by the reported event, the system back end at step 416 shares the event details and context (e.g. installation status/occupation status, etc) and raises an alert with the remote monitoring centre. The sharing of event details may involve the system backend transmitting the event capture (e.g. image capture or video capture) to the remote monitoring centre, particularly if the system backend 230 and the remote monitoring centre 210 are not integrated, but as an alternative the backend may simply share a link with the remote monitoring centre 210. If the system backend 230 and the remote monitoring centre 210 are integrated, the system may be so arranged that the remote monitoring centre 210 is able to access any image (e.g. video) capture for which it receives a relevant identifier - so that the system backend, by raising an escalation event (which will typically include a unique identifier and/or an identifier for the premises installation together with a timestamp) with the remote monitoring centre 210 also makes available the corresponding event parameters (e.g. video capture or video stream) and context.

[0070] At step 418 the remote monitoring centre 210 reviews the event, based on the knowledge that the user is concerned by what they saw in the event capture (e.g. image capture or video), and makes any necessary escalation to emergency services, or calls in private security personnel as required. The remote monitoring centre 210 preferably has the ability to command the central unit 208 of the installation to activate other cameras, microphones, speakers, etc., so that its personnel can obtain a fuller picture of the situation at the protected premises - enabling them to make better informed decisions about escalating an event to the emergency services. In this way the incidence of an event being escalated to the emergency services as the result of a false alarm is likely to be reduced.

[0071] Figure 5 illustrates schematically, at a high level, another method 500 according to an aspect of the invention. In this case we consider the role of a security monitoring installation controller, such as the device 208 shown in Figure 2. When we considered the method illustrated in Figure 3, the security monitoring installation was treated as an entity without further consideration of interaction between elements of the installation. The nodes of the security monitoring installation may be configured as IoT terminals which communicate with each other and with the system backend, the installation being configured without a local control unit such as 208. But we will now consider a method performed in a system in which the installation does include a local control unit to which the installation nodes report, and which in turn reports to the system backend and the central monitoring station (if these are separate). As before, the system back end 230 and the alarm receiving centre (central monitoring station 210) may be separate entities, or they may each form part of an integrated whole 240 within which event data and parameters received by the system back end 240 may be made available to the central monitoring station 210 without the need for an explicit transmission step.

[0072] At step 502 a node of the security monitoring installation is triggered. This may happen irrespective of the arm state of the installation. Generally the nodes of a security monitoring installation that includes a central unit such as 208 are unaware of the arm state of the installation. The node may for example be a video camera with an associated motion sensor (e.g. an internal or external PIR or radar sensor) such as camera 112, 212, 214, a door or window contact sensor such as 206, a shock sensor mounted on a window or door, a fire or smoke sensor 252, a keypad 110 or control panel 227, a movement detector 216, a video doorbell 106, a microphone, or some other device.

[0073] At step 504 the triggered node sends an alert message to the local control unit 208 over a wired or wireless interface. At step 506 the control unit 208 processes the received alert (the event details) based on the identity of the node reporting the event, the nature of the reported event (e.g. the magnitude of a shock reported by a shock sensor, the type and details of an interaction with a disarm node or control panel, etc.) stored rules that dictate the circumstances under which alerts are to be shared with a user device for "pre-alarm consideration" and which not, and optionally the time (hour, date, day) and the arm state of the installation (the same or similar factors may of course be taken into account by the system back end when performing the methods of Figures 3 and 4).

[0074] At step 508 the control unit 208 transmits event parameters to the system back end 230/240. In the case that the event has given rise to an image capture, the event parameters include the image capture and control unit 208 may start to stream video from the relevant camera (if it is a video camera) to the system backend 230/240. If the event has not given rise to a image capture, the event parameters may include the identity of the node that has been triggered, the nature and optionally magnitude of the event detected, optionally the arm state of the alarm, and such other details (such as occupancy status) as may be appropriate.

[0075] At step 509 the system backend 230/240 processes the information received from the control unit of the installation. The transmission to the system backend 230/240 includes an identifier of some kind so that the backend knows from which security monitoring installation (and hence which premises) the event capture is being received. The system backend includes a database that maps installations/premises with a user identity. For each user identity the system backend also stores contact details, including for example SIP addresses, device phone numbers, other contact numbers and email addresses for each user identity, optionally in the same database that maps installations/premises with a user identity. On receiving an event capture from a premises installation, the system back end determines contact details for a user device to be contacted in case of alarm events. Using the relevant contact details, the system backend pushes a notification to the relevant device at step 510. The pushed notification includes the event parameters. If the event capture includes an image capture, the notification may include the captured image, a video clip or a link to the video stream, preferably together with an identifier or indication of the source of the video capture - e.g. a name assigned to the camera such as "Back Garden Camera", optionally also with an indication of the time and date of the capture, together with relevant context information (such as arm state and occupancy status).

[0076] Following delivery of the push notification to the user device 220, the user interacts with the user device to access the notification, causing the video capture to be displayed on a display of the user device at step 512. This may involve the user clicking on (or otherwise selecting) a link to a remote site from which a video may be downloaded or streamed. The user then views the event capture (image, video clip or stream) on the user device to determine whether or not the event capture raises any cause for concern. If the event capture doesn't give rise to any concerns, the user may click on an icon, button or the like to indicate that no issues arise - the icon or button optionally being labelled with a designation signifying that no issues arise - e.g. "all OK", "no concerns", "no problem", and/or colour coded (e.g. colour coded green for safe), causing an appropriate indication to be captured at step 514. Optionally, a user may indicate a lack of concern, and hence no interest in the event being escalated to the remote monitoring centre, by failing to provide an active response. If this mode of providing an indication of indifference is supported the app in the user device is preferably configured to signal to the system backend the fact of the event parameters having been displayed. The system backend may then set a timer at the expiry of which, if no active response has been received, it can be assumed that the user has no interest in escalating the event to the ARC.

[0077] Conversely, if the event parameters are a cause for alarm, the user may take an action to indicate that they wish the event to be flagged to the remote monitoring station 210, with the result that the user device transmits a user response message at step 516. Such an action may be to interact with an icon or button colour coded red, or labelled with a designation signifying that there is a problem or that the video causes the user alarm - e.g. "Escalate to ARC", "action required", "I don't like this", etc.. Additionally or alternatively, the user may be able to indicate concern by pressing on the display on which the event capture is being displayed. Also, as previously mentioned, the user may have the option to draw on any image or video (e.g. a frame of the video - generally on an image capture) to draw around a feature of the displayed image or to add a label or tag, to indicate a person or some other feature of the displayed image (video) whose presence gives rise to concern - e.g. to indicate a stranger or a known person whose presence is unwelcome. The drawing, tagging, or labelling may be captured in the form of a layer or overlay whose details may be transmitted to the system backend at step 516 for sharing, by onward transmission or otherwise, with the remote monitoring centre 210.

[0078] At step 518 the system backend determines the user reaction, optionally by receiving an indication of the perception of a threat or by receiving an indication that the event gives the user no cause for concern. As already noted, a user may also indicate that an event is not a cause for concern by not providing any overt response, with the system backend determining no cause for concern if no response is received from the user within a predetermined period.

[0079] If it is determined that a reported event does not give the user any cause for concern, the system back end ends the process and does not escalate the event to the remote monitoring centre 210.

[0080] Conversely, if it is determined that the user is concerned, alarmed, or threatened by the reported event, the system back end at step 520 shares the event details and context and raises an alert with the remote monitoring centre. The sharing of event details may involve the system backend transmitting an image or video capture to the remote monitoring centre, particularly if the system backend 230 and the remote monitoring centre 210 are not integrated, but as an alternative the backend may simply share a link with the remote monitoring centre 210. If the system backend 230 and the remote monitoring centre 210 are integrated, the system may be so arranged that the remote monitoring centre 210 is able to access any image/video capture for which it receives a relevant identifier - so that the system backend, by raising an escalation event (which will typically include a unique identifier and/or an identifier for the premises installation together with a timestamp) with the remote monitoring centre 210 also makes available the corresponding event parameters (e.g. image/video capture or video stream).

[0081] At step 522 the remote monitoring centre 210 reviews the event, based on the knowledge that the user is concerned by what they saw in the event capture in association with the parameters provided for the captured event, and makes any necessary escalation to emergency services, or calls in private security personnel as required. The remote monitoring centre 210 preferably has the ability to command the central unit 208 of the installation to activate other cameras, microphones, speakers, etc., so that its personnel can obtain a fuller picture of the situation at the protected premises - enabling them to make better informed decisions about escalating an event to the emergency services. In this way it is possible to escalate to the monitoring station an event occurring while the installation is disarmed or in an armed at home mode while minimising the incidence of events being escalated to the emergency services as the result of a false alarm.

[0082] Figure 6 is a flow chart corresponding generally to Figure 5, illustrating a method 600 according to an aspect of the invention performed by a system including a security monitoring installation that includes a central unit, such as element 208 of Figure 2. In this example it is assumed that a camera, such as any one of cameras 112, 212, 214, is triggered by some kind of motion detector/sensor (e.g. PIR or radar sensor) that is either integral with the camera, or external to the camera but operatively associated with the camera.

[0083] At 602 an event is detected by a motion sensor of or associated with a camera such as camera 214' of Figure 2. Here we assume that the security monitoring installation is in a mode other than a fully armed mode, for example a disarmed mode or an armed at home mode. Furthermore we here assume the presence of domestic staff, such as a cleaner, who is allowed to enter and move through much of the interior space of the protected premises, and possibly also the grounds of the premised, but that there is at least one zone, room or area that is out of bounds and which they are not permitted to enter. Here we will use the example of the study or office 201 of Figure 2, but the out of bounds area could be any kind of room, space or zone. Further we will assume that the motion sensor that has been triggered is one associated with the camera 214' in the out of bounds study 201. The cleaner has, against his instructions, entered the study 201.

[0084] Triggering of the motion sensor activates the camera 214' which captures an image of the interior of the study 201. At 604 the image capture is transmitted by the camera 214' to the central unit 208, for example over Wi-Fi of using a narrow bandwidth channel such as a channel of an ISM radio band. The camera may continue to capture images/video after being triggered until commanded to stop (by the central unit, for example), or may continue to capture images for a predetermined time after movement was last detected.

[0085] At step 606 the central unit 208 processes the reported event details based on the state of the installation and any stored rules. Here we assume that the stored rules dictate that the triggering of a motion sensor in the study 201, when the installation is in a disarmed or armed at home mode, be reported to a (specified) user. Conversely, in an armed away mode triggering of a motion sensor in the study 201 results in an alarm event being reported to the system backend 230/240 or to the remote monitoring station 210.

[0086] At step 608 the central unit 208 transmits the event details, including the image capture, and context data to a (or the) relevant user device. This transmission may be direct, for example using a 4G/5G transmitter (or transceiver) in the central unit to transmit a message by a suitable PLMN to the user device using address details stored by or accessible by the central unit. Alternatively, the transmission may be via a system backend as described generally with reference to Figure 5.

[0087] At step 610 the user device 220 displays the image capture on the display of the device, preferably together with at least some of the supplied context (arm status, when the arm status was changed, by whom (if known from dongle/device ID or from the passcode's allocation if available).

[0088] At step 612 the user device 220 receives a user input, for example in the form of a touch input on a touch sensitive display of the device, in response to the displayed image capture e.g. a force touch input to signify the user's desire to escalate the event to the remote monitoring station. The notification received at the user device may include one or more "action elements" providing the user with predefined actions that can be invoked by interacting with the relevant action element. For example, the action elements may be icons or "buttons" with which the user may interact (by touching, force touching/pressing, or otherwise selecting) to select the relevant element to produce a corresponding action or to indicate a reaction. The reaction may be one signifying that the user is unconcerned by the reported event, or one requesting that the event be escalated to (passed to) the remote monitoring station, or some other action such as connecting the user device to an audio interface at the installation - for example an audio interface of the camera 214', so that the user can speak to the cleaner while the cleaner is in the study, or via another audio interface if the cleaner has already left the study. So, for example, if the cleaner is new, the user can remind the cleaner that he is not supposed to clean the study. Conversely, the cleaner may be able to explain that they entered to study to retrieve the family cat that was mewing to be let out.

[0089] The action elements may also permit staged responses - such as an initial response in which the user can start a dialogue with the cleaner and then a follow up action in the event that the cleaner does not leave the study when asked, or is seen performing actions suggestive of theft or snooping - in which case the user may have the option to raise a high level alert with the remote monitoring station.

[0090] At step 614 the system backend determines the user reaction based on any response received from the user device, or based on a lack of overt response, which indicates or is suggestive of indifference or a lack of perceived threat. If the user provides an active response indicating that no threat is perceived, or if user indifference can be inferred, for example by the lack of any timely active response, the system back end halts the process at 616 without reporting the event to the monitoring station.

[0091] Conversely, if the user provides an active response indicating that threat is perceived, the system backend at 618 shares the event capture (including the image capture and optionally any video), and raises an alert, based on the user's input, with the remote monitoring service, also providing any relevant context information. The personnel of the remote monitoring service are preferably able to instruct the control unit of the installation to connect the monitoring station to the camera 214', any audio interface, and optionally any other camera of the installation so that the personnel are able to see and hear what is happening at the protected premises, and also to have a dialogue with the cleaner and anyone else at the premises in an attempt either to de-escalate the situation or to get the cleaner to leave the study. Failing which the monitoring service may involve the police or other security personnel.

[0092] Figures 7 and 8 correspond generally with figures 5 and 6 but in this was with off-site motion detection based on image analysis. Here we assume that a camera such as study camera 214' or back garden camera 212 is arranged to capture 704 images on a continuous or quasi continuous (e.g. a capture every few seconds) basis. The captured images are then passed 706 to an image (e.g. video) analysis system 702 for the detection of movement based on differences between images. The image analysis system 702 may be internal to the camera (214' or 212), internal to the control unit 208, or provided by a hardware arrangement that is remote from the installation - optionally part of the system backend 230 or 240, or provided by some other entity. In Figure 7 we assume that the image analysis system 702 is located somewhere intermediate the camera and the system backend - for example either provided by the installation controller 208, or provided by an off-premises function somewhere.

[0093] At step 708 the image analysis system 702 determines, based on differences between captured images, that there is movement at the premises. If the image analysis system is provided by an entity remote from the premises it will typically be arranged to provide the result of its analysis to the installation control unit 208 or to the relevant requesting node if the installation includes no intermediate control unit. If the image analysis system 702 is provided by the control unit, or if the control unit receives an output from the image analysis system 702 to the effect that movement has been detected, the control unit taking account of any stored rules for event handling, based on arm state of the installation, time of day, day of week etc. and any other status data as necessary, provides details of the detected event - for example including an image capture or video clip, etc. together with event parameters, in the form of a notification for a relevant user device. As described previously, the central unit may use an internal transceiver to transmit the notification to the user device, e.g. over a 4G or 5G PLMN, or it may send the relevant information to the system backend 230/240 for the backend to handle the provision of a notification to the user device. Figure 7 assumes that latter approach but it will be understood that the direct approach may be used in other embodiments of the invention.

[0094] Thus, at step 710 a message is sent to the system backend 230/240, optionally from a control unit 208 of the installation. The message includes one or more relevant image captures and/or one or more video clips or a link to an image capture or video clip(s).

[0095] At step 712 the system backend processes the received message to determine how the message is to be handled, and in particular if it should be sent to a user device 220, and if so to which one, or direct to the monitoring station 210. Again the system backend is able to determine based on the received message the identity of the installation and also contact details for the relevant user device 220. The various approaches mentioned previously apply equally here. Based on this determination, the system back end may send a push notification to the user device 220, the notification including one or more of the image capture, the video capture or a link thereto.

[0096] The remainder of the steps illustrated in Figure 7 correspond to those of the comparable earlier figures.

[0097] Figure 8 is a flow chart illustrating a method 800 in which the detection of motion based on analysis of repeated images of a scene is a trigger for action. The method may be performed by a security monitoring installation in a domestic setting, such as at a home as illustrated in Figures 1 and 2, or in a commercial setting such as a retail outlet (e.g. a restaurant or shop) or at some other kind of business, such as at an office. The security monitoring installation may be in an arm state other than fully armed - e.g. disarmed or "armed at home".

The camera may be surveying an out of bounds area, or may be surveying an open access area for detection of a potential threat under certain circumstances (for example in a commercial setting the installation may be used to alert to the arrival of potential customers or potential villains while the commercial enterprise is short-staffed, e.g. before or after the main operating hours).

[0098] At step 802 a camera of the installation captures at least two images of a scene at the installation. The camera may only be able to capture still images, or it may be configured to capture video with a frame rate high enough to generate a watchable video sequence. For example, the camera may be any one of the cameras shown in Figures 1 or 2. The camera may be a stills camera configured to capture still images periodically - for example every 10 to 20 seconds, or a few times each minute. Conversely, the camera may be a video camera configured to capture video with a frame rate of between several times a second and, for example, 20 to 24 frames per second.

[0099] At step 804 images captured by the camera are analysed in an attempt to detect movement of image elements between an earlier image and a later image. The analysis may be based on consecutive image captures or may be based on non-adjacent images from a sequence of image captures. The image analysis may be performed on the camera that captures the images but may alternatively be performed by a processor remote from the camera, the camera images having been transmitted or otherwise sent directly or indirectly to the processor. For example, the camera may be configured to send image captures to a controller of the installation, e.g. controller 208, for processing on the controller or to a controller or other gateway for onward transmission by the controller/gateway (directly or indirectly) to another entity that will perform the image analysis. Thus, the image analysis may be performed by a system backend, such as 230 or 240, remote from the installation.

[0100] At step 806 the processor performing the image analysis detects movement based on differences between image captures made at different instants in time. The processor may be programmed to react to any detected movement, or it may be programmed to ignore some categories of movement or only to respond to certain categories of movement or to respond only if certain feature types (e.g. humans and/or vehicles) are present. Commercially available image analysis systems based on A.I., e.g. software packages, may be used to perform the image analysis.

[0101] Based on the detection of movement (according to the rules being applied by the processor or system performing the image analysis) a report is generated for notification of the detected motion to a user device. Depending upon the location of the entity performing the image analysis the report may be in the form of the notification for the user device, or the report may be provided, directly or indirectly, to another entity (e.g. the installation controller or the system backend) for the preparation and despatch of the notification. The report and notification, if different, each both preferably include at least the later of the compared images, and preferably the object of interest whose movement has been detected is marked, annotated, or highlighted in some way so that the basis of the motion detection will be clear from the notification. The notification may include two or more of the images from which motion was determined, or only one image (suitably annotated or marked) may be included. If the image analysis was performed on a video sequence, that video sequence or a relevant clip from that sequence may be included in the notification. The notification is transmitted to the user device, e.g. device 220, at step 808, based on the identity of the installation and e.g. a database linking the installation to a relevant user device identifier. The notification preferably also includes context data (for example arm state, occupancy, camera identity, other node sensing data, etc.) regarding the installation at the time of the relevant image captures.

[0102] At step 810 the notification is displayed on a display of the user device in such a way as to provide the user with a clear indication of the basis for movement detection. The notification may include textual information (e.g. labelling) and/or audio description to aid the user's understanding of the nature of the reported event - e.g. "person spotted in the back garden". The notification may also include one or more "action elements" e.g. buttons or icons with which the user may interact to provide a response.

[0103] At step 812 the user may provide a reaction - for example, if the notification is a cause for alarm, the user may interact with an actionable element such as a button or icon, or perform a deep touch, to indicate a desire to escalate the event to the remote monitoring centre. Conversely, the reaction from the user may indicate that no threat is perceived - either based on an action taken by the user (interacting with a "not a threat" or "all OK" button, for example) or based on the lack of a request (within a predetermined period after notification) to escalate.

[0104] At step 814 the user reaction is determined at a processing entity, such as the system backend 230/240 or the installation controller 208, based either on an overt response received from the user device or based on the lack of an overt response.

[0105] Based upon the determined response the processing entity either, based on a determination of no threat, discounts the event at 816, or based upon a determination of a perceived threat escalates 818 the event to the remote monitoring centre 210. Escalating to the remote monitoring centre includes making the relevant image capture(s) available to the remote monitoring centre and also providing any relevant information from the user's reaction (in particular that the user perceives the existence of a threat).

[0106] At step 820 the personnel of the remote monitoring centre review the relevant captures and the contextual information, and if necessary instruct the installation to make available video feeds, provide a bidirectional audio channel, etc., so that the personnel are better able to determine the nature of any incident. If necessary, based on the captures, contextual information, and later gathered information, the personnel may decide to involve security personnel or the police, of others.

[0107] The processor/system used to determine motion based on image analysis, and/or the processor/system that decides whether or not to notify a user device based on any detected movement, may use user feedback (e.g. escalations, "all OK" responses, and passive "responses") in a machine learning approach to improving system performance.

Claims

1. A method, performed by a system that comprises a security monitoring system installation at premises protected by the installation, the security monitoring system having a disarmed mode and at least one armed mode, method comprising:

i) detecting the occurrence of an event at the premises while the security monitoring system is in the disarmed mode;
ii) transmitting a notification in respect of the event to a user device, the notification including event data; and
iii) only in response to receiving a user reaction to the notification indicating a desire/wish to raise an alert in respect of the event with a monitoring station remote from the premises, notifying the monitoring station and providing the monitoring station with access to the event data.

2. A method as claimed in claim 1, further comprising the step of reporting, prior to step ii), the occurrence of the event to a system back end remote from the premises, wherein the system back end performs either of steps ii) or iii).

3. A method as claimed in claim 1, wherein the step of transmitting a notification in respect of the event to a user device is performed by the security monitoring installation, wherein the security monitoring installation performs either of steps ii) or iii),
optionally wherein the installation comprises a controller, and the step of transmitting a notification in respect of the event to a user device is performed by the controller, and wherein the controller performs either of steps ii) or iii).

4. A method as claimed in any one of the preceding claims, wherein the notification in respect of the event includes at least one of:

an image related to the event, and optionally wherein the image is a still image; and/or
a link giving access to a video capture related to the event.

5. A method as claimed in any one of the preceding claims, wherein the event is at least one selected from:

sensor based detection of motion;
sensor based detection of presence.
triggering of a window sensor, optionally a contact switch, magnetic sensor, or a shock sensor;
triggering of a door sensor, optionally a contact switch, magnetic sensor, or a shock sensor;

6. A method as claimed in any one of the preceding claims, wherein whether the notification of step ii) is transmitted or not depends upon at least one condition selected from: the time of day, day of the week, date, nature of the event, or some combination thereof.

7. A method as claimed in any one of the preceding claims, wherein the notification further includes context information, the context information distinct from the event data and complementing the event data, optionally wherein the context information includes one or more selected from: the arm state; occupation state of the premises; camera identity; status of other detectors at the premises.

8. A system that comprises a security monitoring installation at premises protected by the installation and a system back end remote from the premises, the security monitoring installation having a disarmed mode and at least one armed mode, the security monitoring installation comprising a controller and a plurality of sensors configured to transmit event notifications to the controller, the controller being configured when the system is in an armed mode to report alarm events to a monitoring station remote from the premises, the controller having at least one operating mode in which it is configured to respond to receiving certain event notifications while the installation is in the disarmed mode by transmitting an alert, in respect of the notification of an event, to the system back end remote from the premises, the system back end being configured to:

i) transmit a notification in respect of the event to a user device, the transmitted notification including event data and optionally context information;
ii) raise an alert in respect of the event with a monitoring station remote from the premises only in response to receiving from a user at the device a user reaction to the transmitted

notification indicating a desire to raise an alert in respect of the event; and,
iii) if an alert is raised with the monitoring station in respect of the event to provide the monitoring station with access to the event data and optionally context information.

9. A security monitoring installation at premises protected by the installation, the installation having a disarmed mode and at least one armed mode, the security monitoring installation comprising a controller and a plurality of sensors configured to transmit event notifications to the controller, the controller having at least one operating mode in which it is configured to respond to certain event notifications while the installation is in the disarmed mode by:

i) transmitting a notification in respect of the notification of an event to a user device, the transmitted notification including event data and optionally context information;
ii) in response to receiving a user reaction to the transmitted notification indicating that the event is a false alarm or that the user does not wish to report the event to the monitoring station, determining not to notify the monitoring station of an alarm event in respect of the event;
iii) in response to receiving a user reaction to the transmitted notification indicating a desire to raise an alert in respect of the event with the monitoring station, notifying the monitoring station of an alarm event and providing the monitoring station with access to the event data and optionally the context information; and
iv) in response to not receiving within a predetermined time period a user reaction to the transmitted notification, not notifying the monitoring station of an alarm event (in respect of the event).

10. A system as claimed in claim 8 or an installation as claimed in claim 9, wherein the context information is distinct from the event data and complementing the event data, the context information including one or more selected from: the arm state; occupation state of the premises; camera identity; status of other detectors at the premises.

11. A system or installation as claimed in any one of claims 8 to 10, wherein the transmitted notification in respect of the event includes at least one of:

an image related to the event, and optionally wherein the image is a still image; and/or
a link giving access to a video capture related to the event.

12. A system or installation as claimed in any one of claims 8 to 11, wherein the event is at least one selected from:

sensor based detection of motion;
sensor based detection of presence;
triggering of a window sensor, optionally a contact switch, magnetic sensor, or a shock sensor;
triggering of a door sensor, optionally a contact switch, magnetic sensor, or a shock sensor.

13. A system or installation as claimed in any one of claims 8 to 12, wherein whether the notification of i) is transmitted or not depends upon at least one condition selected from: the time of day, day of the week, date, nature of the event, or some combination thereof.

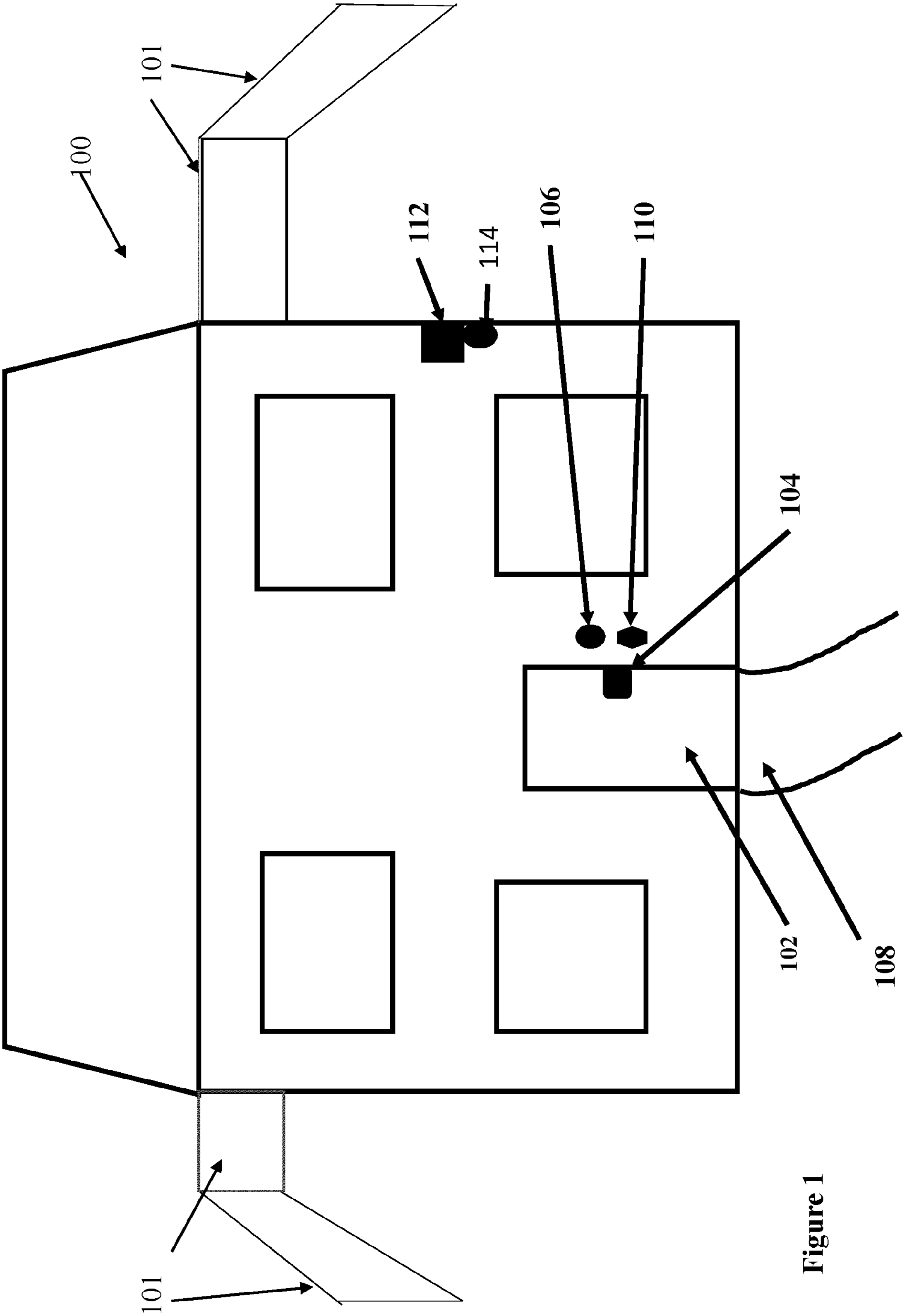

Figure 1

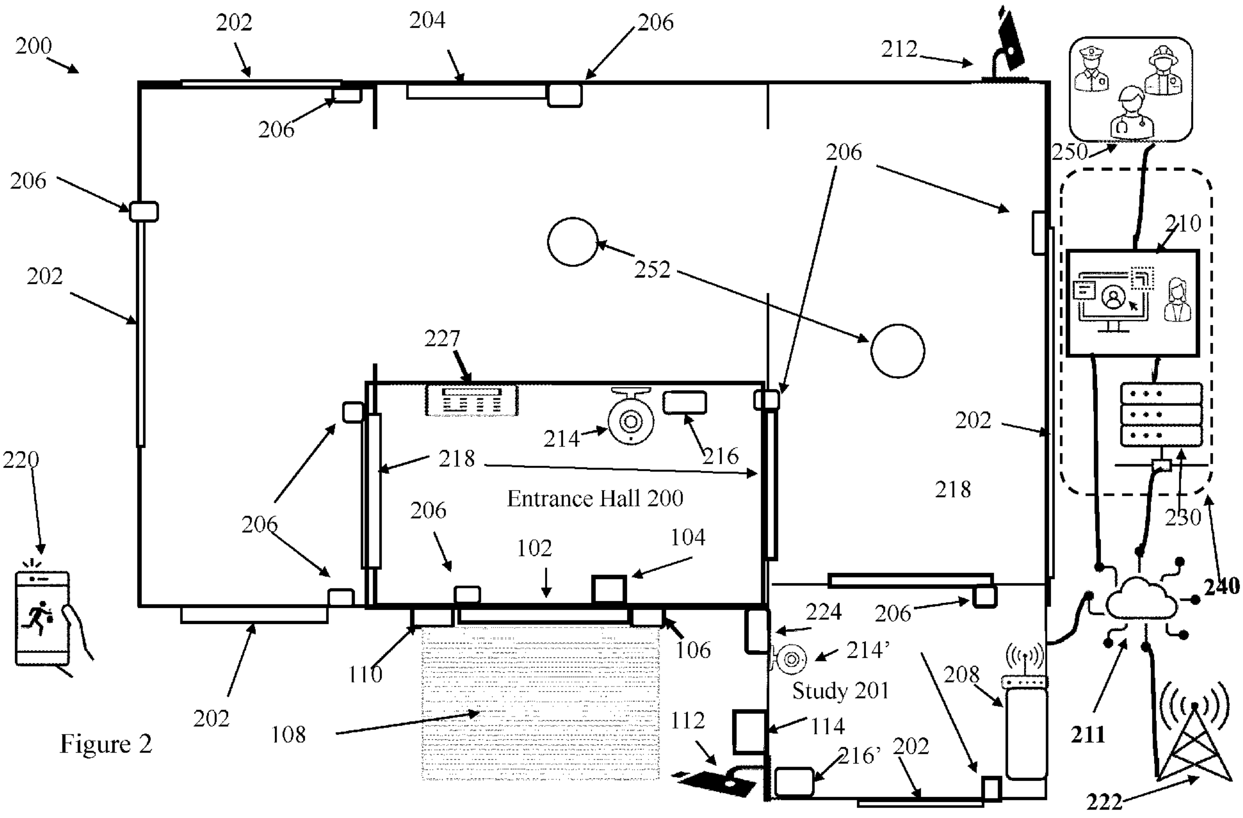
200
202
204
206
212
206
206
250
206
210
202
252
227
202
214
216
218
218
220
Entrance Hall 200
206
206
104
102
240
224
206
230
110
106
214'
208
Study 201
211
202
108
112
114
216'
202
222

Figure 2

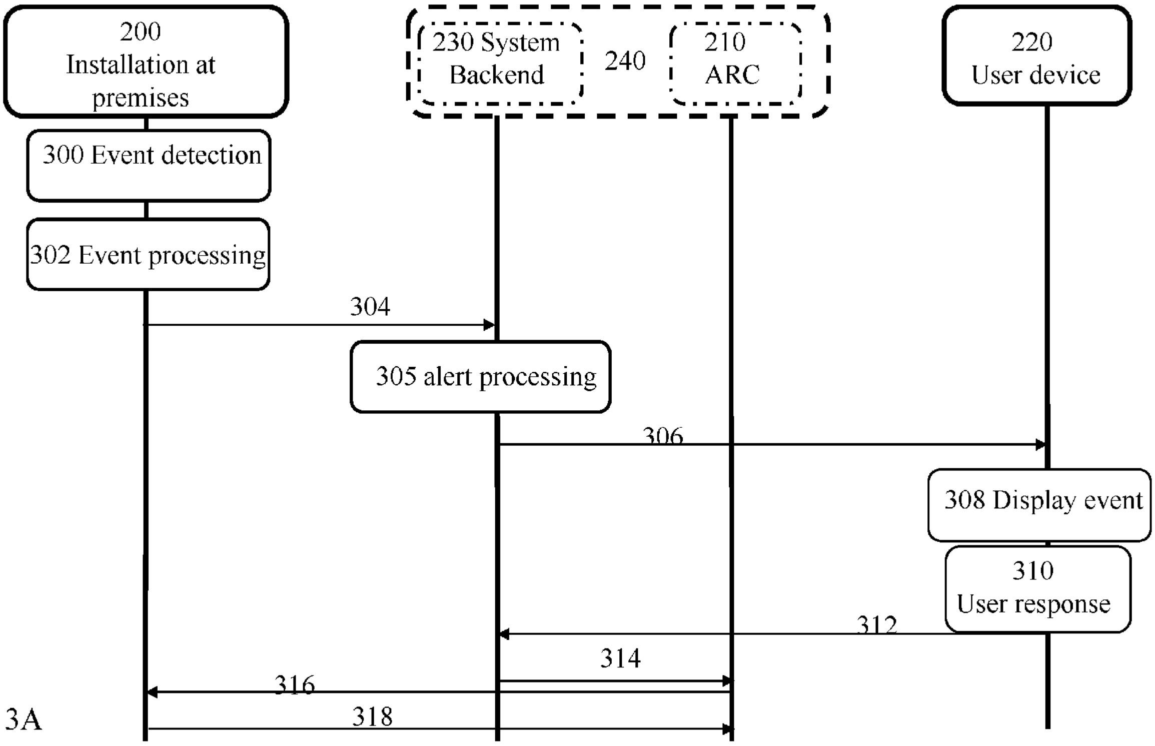
200
Installation at premises
230 System Backend
240
210
ARC
220
User device
300 Event detection
302 Event processing
304
305 alert processing
306
308 Display event
310
User response
312
314
316
318

Figure 3A

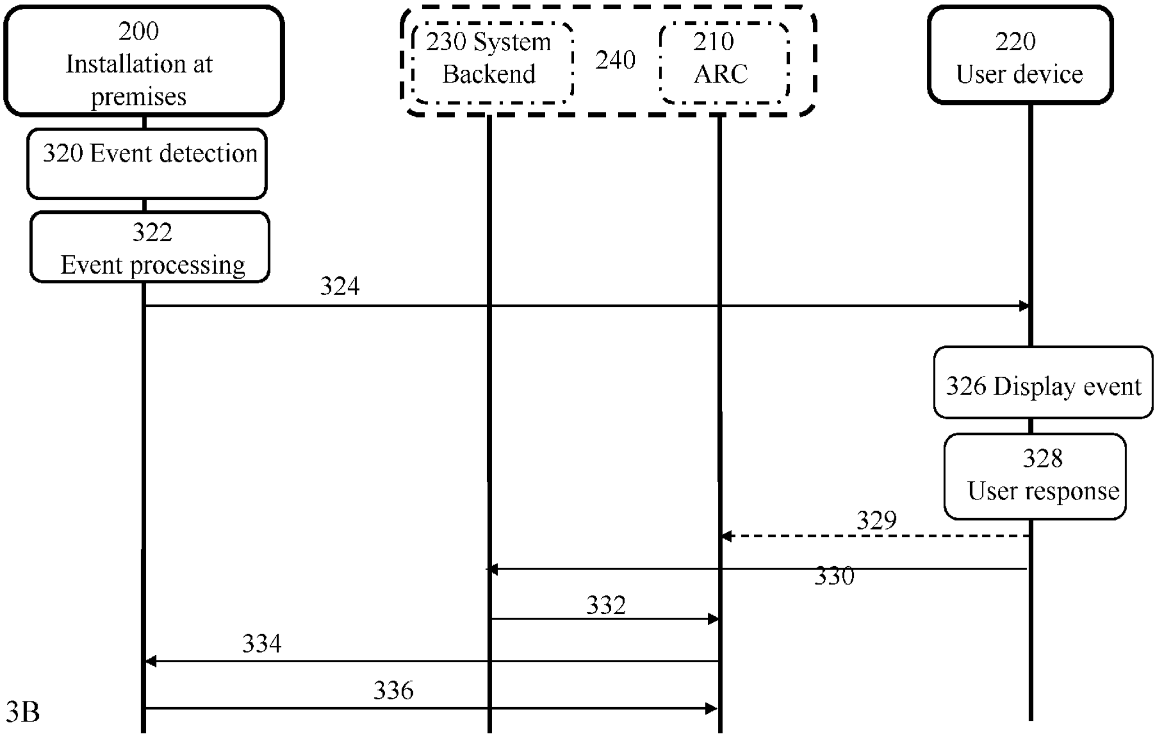
200
Installation at premises
230 System Backend
240
210
ARC
220
User device
320 Event detection
322
Event processing
324
326 Display event
328
User response
329
330
332
334
336

Figure 3B

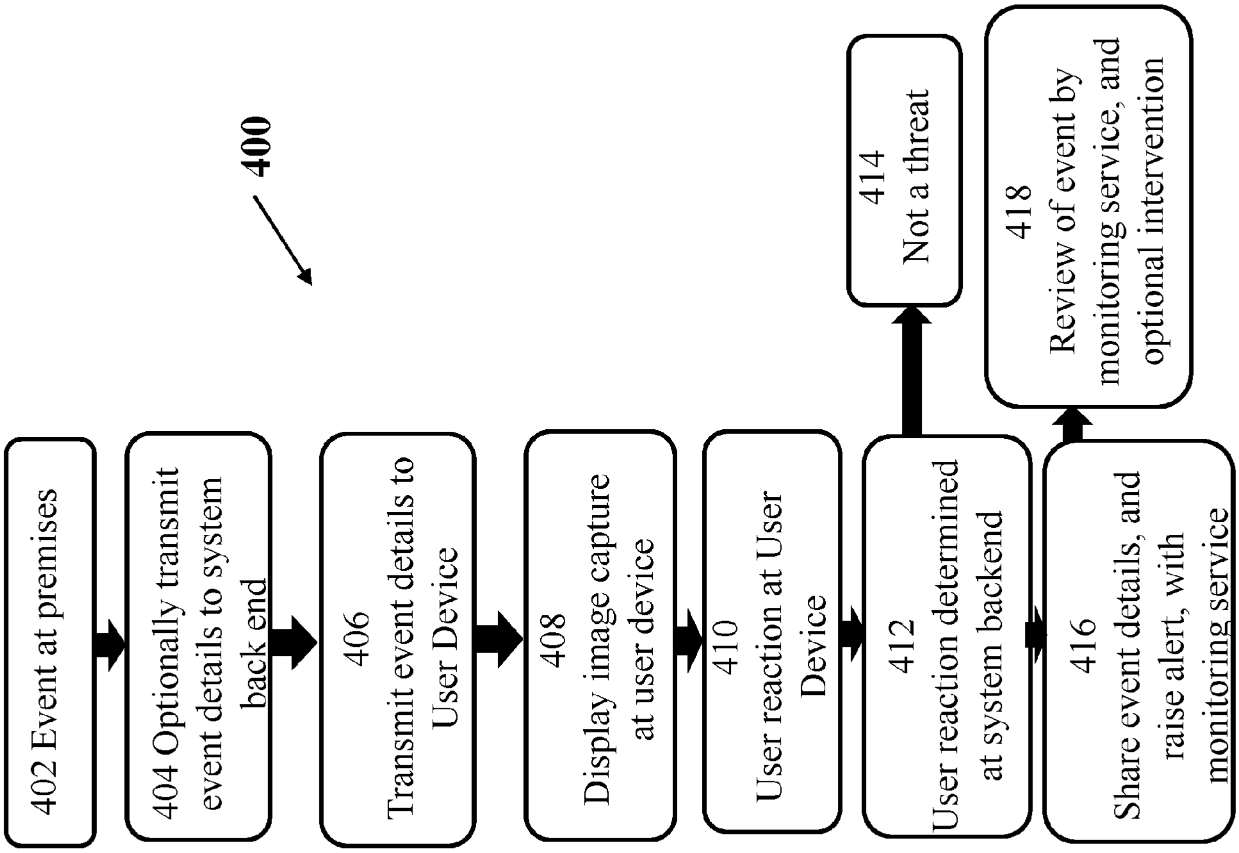
400
402 Event at premises
404 Optionally transmit event details to system back end
406 Transmit event details to User Device
408 Display image capture at user device
410 User reaction at User Device
412 User reaction determined at system backend
414 Not a threat
416 Share event details, and raise alert, with monitoring service
418 Review of event by monitoring service, and optional intervention

Figure 4

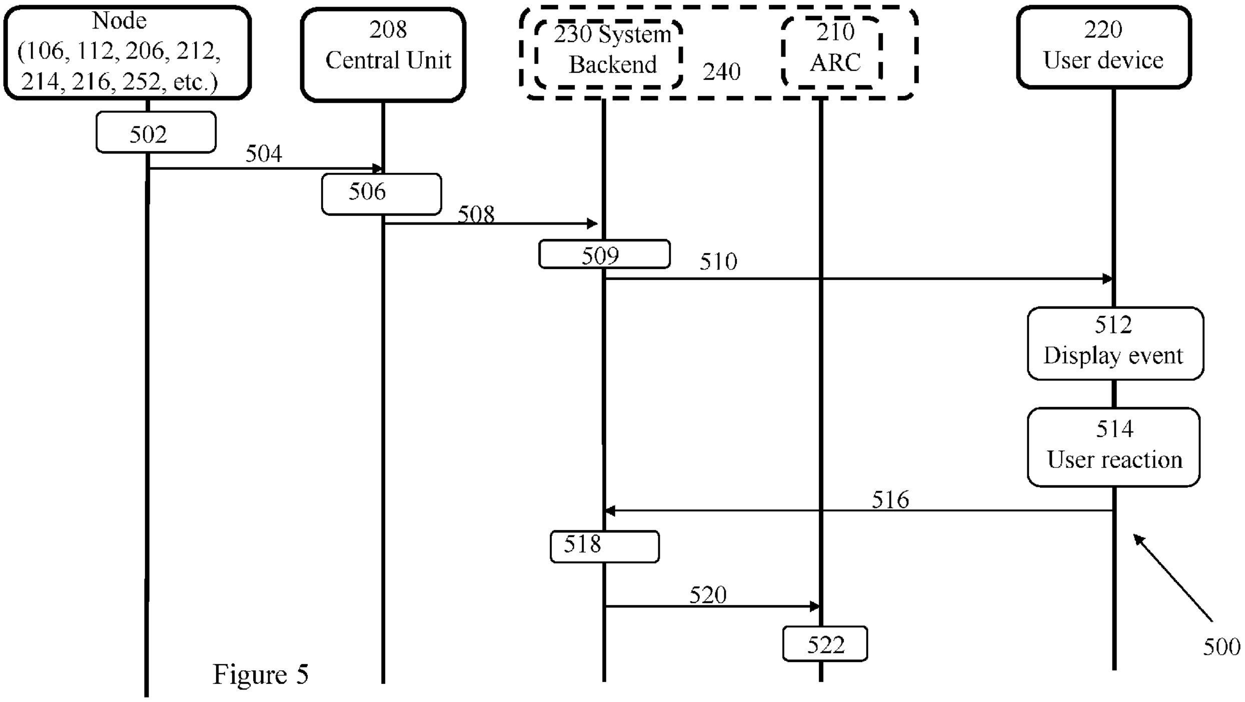
Node
(106, 112, 206, 212,
214, 216, 252, etc.)
208
Central Unit
230 System
Backend
240
210
ARC
220
User device
502
504
506
508
509
510
512
Display event
514
User reaction
516
518
520
522
500

Figure 5

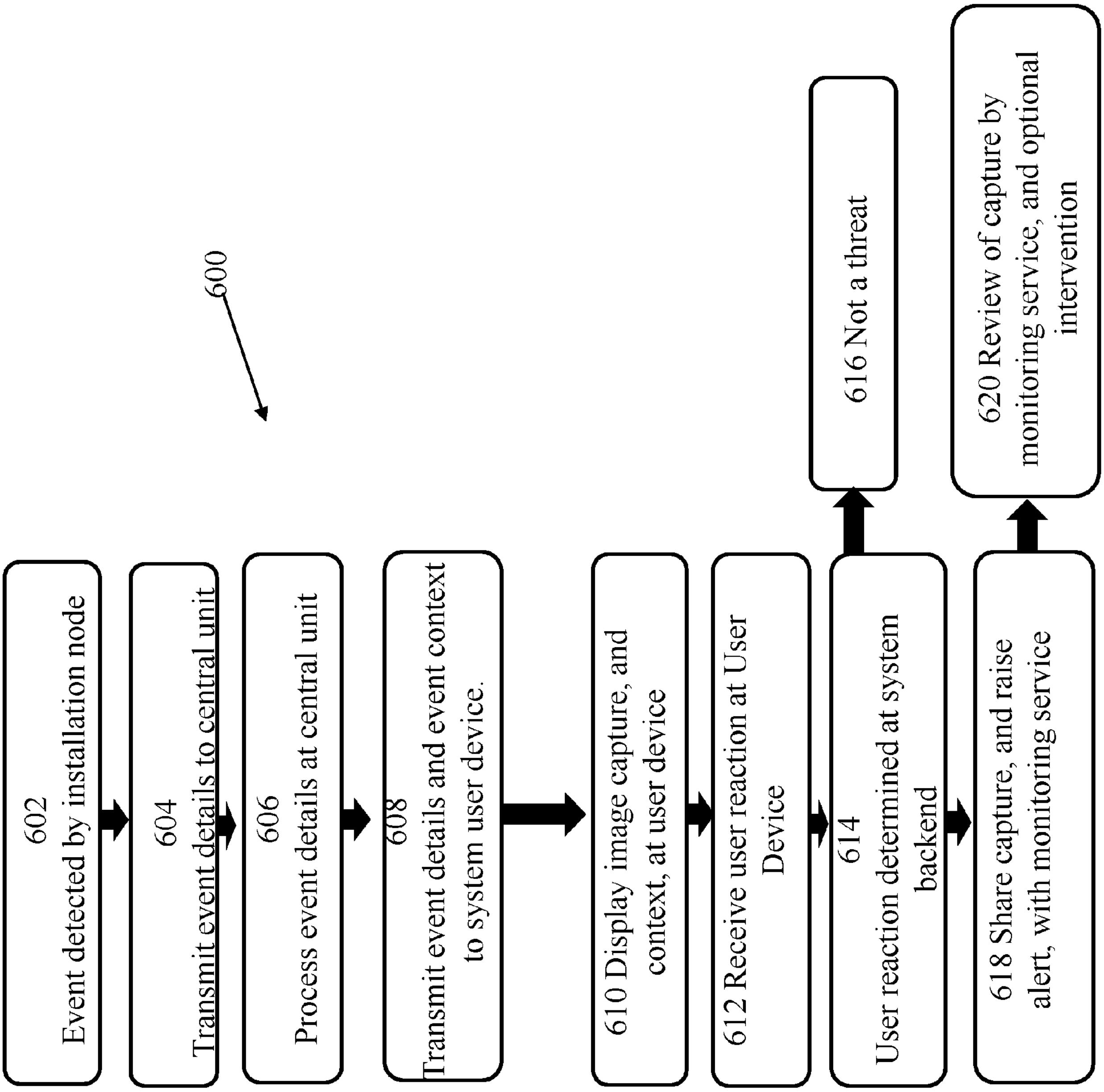
600
602
Event detected by installation node
604
Transmit event details to central unit
606
Process event details at central unit
608
Transmit event details and event context to system user device.
610 Display image capture, and context, at user device
612 Receive user reaction at User Device
614
User reaction determined at system backend
616 Not a threat
618 Share capture, and raise alert, with monitoring service
620 Review of capture by monitoring service, and optional intervention

Figure 6

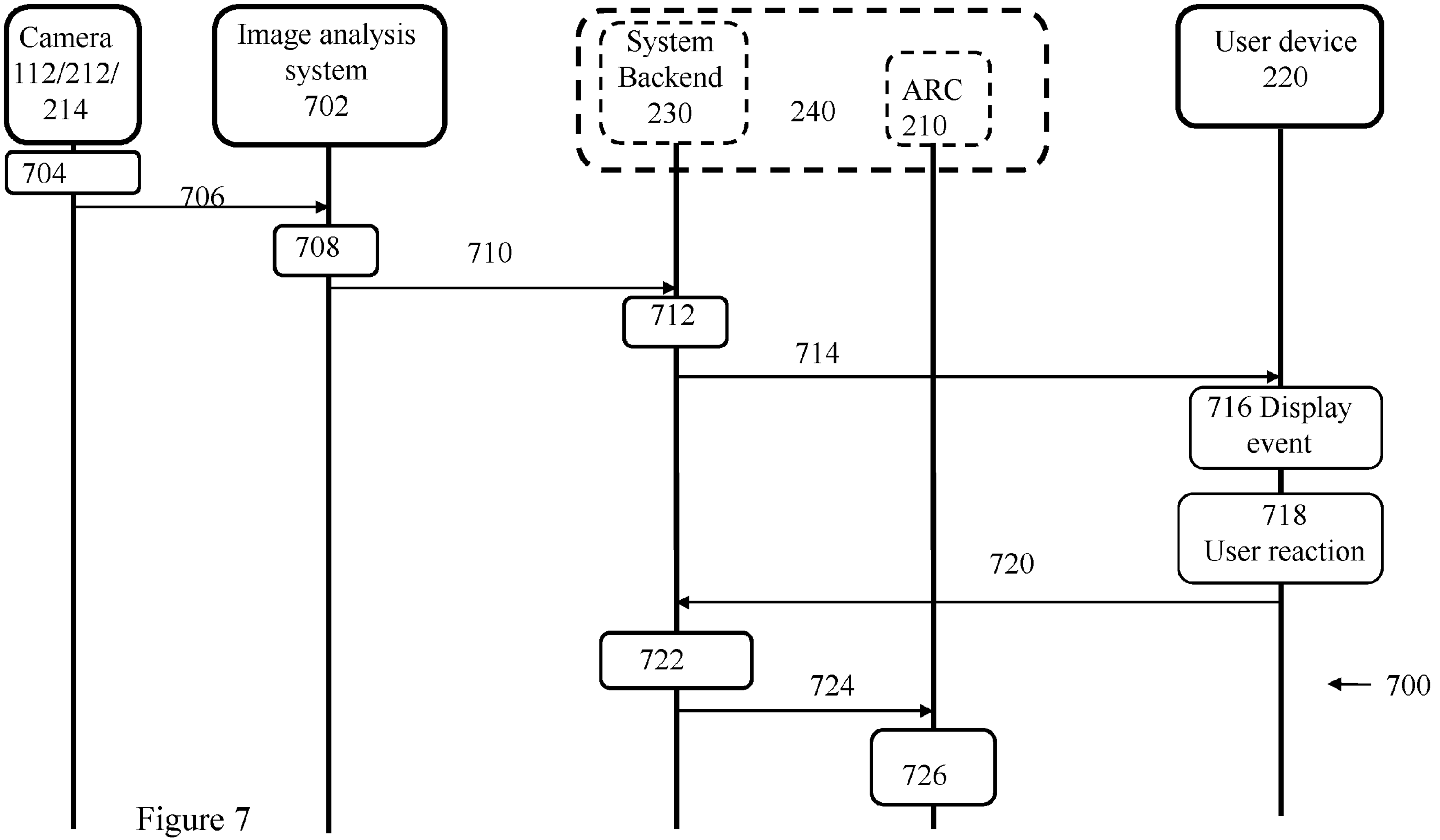
Camera
112/212/
214
Image analysis
system
702
System
Backend
230
240
ARC
210
User device
220
704
706
708
710
712
714
716 Display
event
718
User reaction
720
722
724
726
700

Figure 7

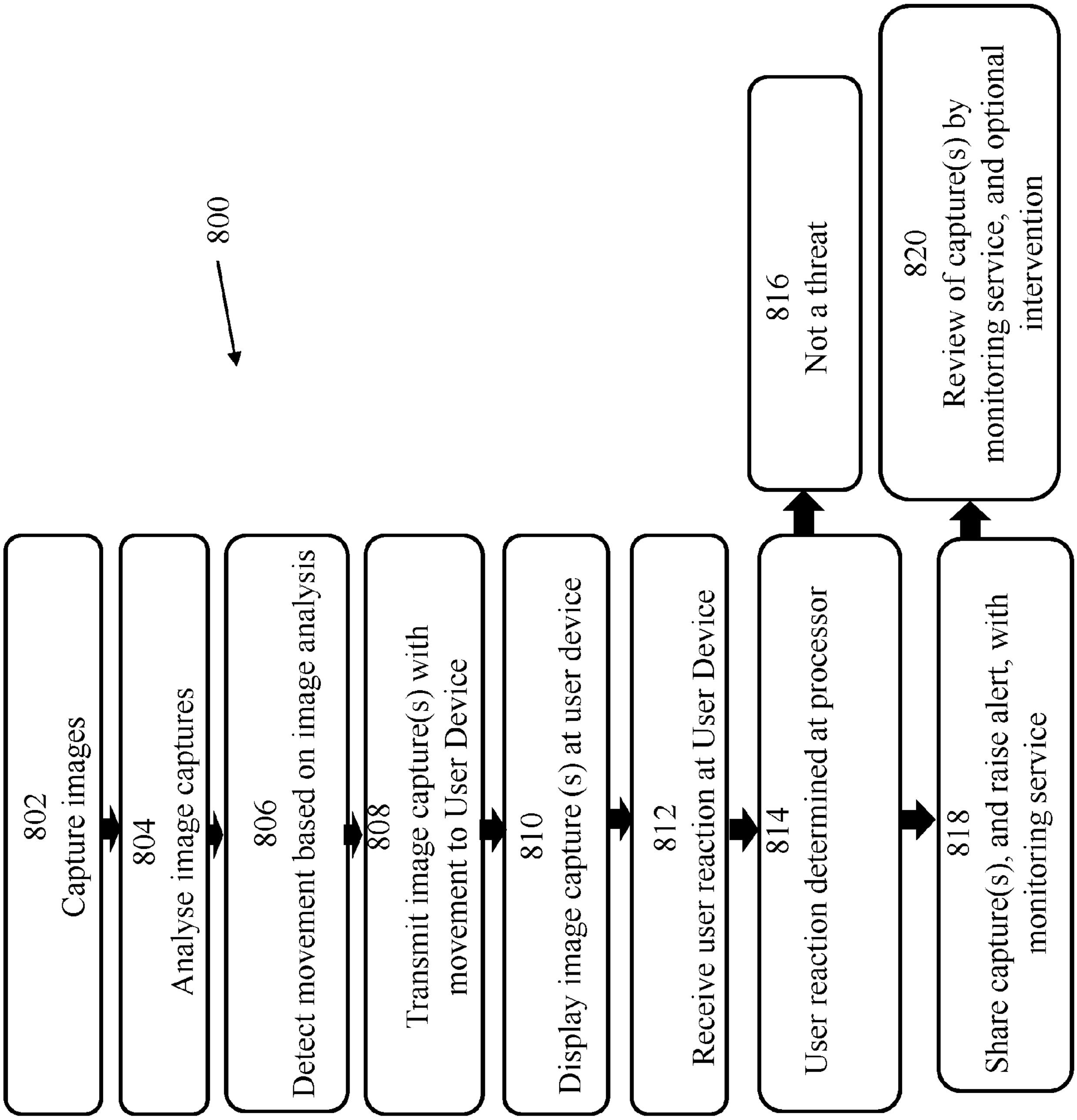
800
802
Capture images
804
Analyse image captures
806
Detect movement based on image analysis
808
Transmit image capture(s) with movement to User Device
810
Display image capture (s) at user device
812
Receive user reaction at User Device
814
User reaction determined at processor
816
Not a threat
818
Share capture(s), and raise alert, with monitoring service
820
Review of capture(s) by monitoring service, and optional intervention

Figure 8

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 38 3199

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2022/243449 A1 (VERISURE SARL [CH]) 24 November 2022 (2022-11-24) * page 1 * * page 3 - page 5 * * page 9 - page 10 * * figures * -----	1-13	INV. G08B25/00 ADD. G08B29/18
X	US 2023/035710 A1 (SZCZEPANSKI DOMINIK [US] ET AL) 2 February 2023 (2023-02-02) * paragraph [0014] - paragraph [0020] * * paragraph [0037] * * paragraph [0054] * * paragraph [0061] - paragraph [0064] * * paragraph [0073] * * figures * -----	1-13	
			TECHNICAL FIELDS SEARCHED (IPC)
			G08B

The present search report has been drawn up for all claims

3

Place of search	Date of completion of the search	Examiner
Munich	10 April 2024	Königer, Axel

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
....
& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 23 38 3199

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

10-04-2024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2022243449 A1	24-11-2022	AR 125876 A1	23-08-2023
		CL 2022003726 A1	28-04-2023
		EP 4150597 A1	22-03-2023
		WO 2022243449 A1	24-11-2022
US 2023035710 A1	02-02-2023	US 2023035710 A1	02-02-2023
		US 2024029543 A1	25-01-2024
		WO 2023014521 A1	09-02-2023

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