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

(11) **EP 4 231 266 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
23.08.2023 Bulletin 2023/34

(21) Application number: **22157532.7**

(22) Date of filing: **18.02.2022**

(51) International Patent Classification (IPC):
G08B 29/18 *(2006.01)* *G08B 13/196* *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G08B 13/19695; **G08B 29/181**

(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 MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

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

(72) Inventor: **WELLS, Andrew**
1290 Versoix, Geneva (CH)

(74) Representative: **Prinz & Partner mbB**
Patent- und Rechtsanwälte
Rundfunkplatz 2
80335 München (DE)

(54) PERIPHERAL FOR PREMISES SECURITY MONITORING SYSTEMS

(57) Provided is a peripheral for a home alarm system, the peripheral comprising: a processor operatively connected to a first transceiver that is configured to transmit signals to, and to receive control signals from, a controller of the alarm system; the peripheral being configured to power the processor, the first transceiver and other power-consuming electronics of the peripheral using electricity supplied from an external energy source; a rechargeable energy store arranged to receive power from the external energy source and to power the second processor and the first transceiver, but not at least some of the other power-consuming electronics, in the event of loss of power from the external energy source;
the processor being configured in the event of loss of power from the external energy source to cause the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power, the processor and the first transceiver drawing their power from the energy store.

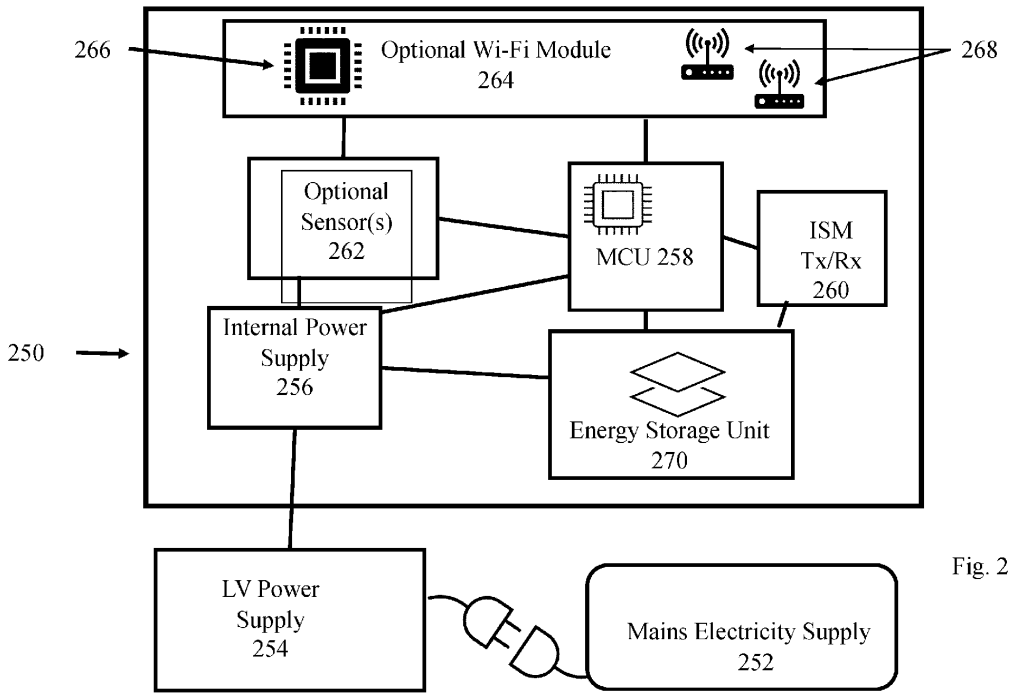

Fig. 2

EP 4 231 266 A1

Description

Field

[0001] The present invention relates to peripherals for premises security monitoring systems, to premises security monitoring systems including such peripherals, and to methods performed by such devices.

Background

[0002] 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, 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. 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 or local management device), generally mains powered, that is coupled to the sensors, detectors, cameras, etc. ("peripherals" or "nodes"), and which processes received notifications and determines a response. The local management device or central unit may be linked to the various peripherals 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 (for example in the event of power loss due to a power cut or actions of an intruder), the peripherals 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 remotely located monitoring station where, typically, human operators manage the responses required by different alarm and notification types. These monitoring stations are often referred to as Central Monitoring Station (CMS) because they may be used to monitor a large number of security monitoring systems distributed around the monitoring station, the CMS located rather like a spider in a web. In such centrally monitored systems, the local management device or central unit at the premises installation typically processes notifications received from the peripherals in the installation, and notifies the Central Monitoring Station of only some of these, depending upon the settings of the system - in particular whether it is fully or only partially armed, 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 peripherals and the Central Monitoring Station. Again, in such installations the central unit may be linked by wires, or wirelessly, to the various peripherals of the installation, and these peripherals will typically be battery rather than mains powered.

[0004] Although we would like to power all alarm peripherals by battery, we also need to achieve battery lives measured in years rather than months, weeks, or less - because if a peripheral loses power, it can no longer serve its intended function. For professionally installed alarm systems, battery replacement frequently involves a site visit by a service engineer or technician - which incurs expense and necessitates scheduling access to the protected premises. Selection of suitable low-power energy designs for transceivers and controllers for alarm peripherals enables many such devices to achieve impressively long battery lives of at least 3 to 5 years using no more than perhaps a few AA alkaline cells. But some peripherals are much more power hungry - at least in some operational modes, and these typically need to be connected to an external power source (because it would be impractical or uneconomic to provide a self-contained power supply of sufficient capacity), generally a mains electricity supply. For example, peripherals that rely on Wi-Fi typically require an external power source because Wi-Fi transceivers (which provide high power and wide bandwidth communication channels) tend to be much more power hungry than the low power narrow bandwidth transceivers used in most peripherals for communication with the alarm system control unit.

[0005] Important examples of such Wi-Fi peripherals are video cameras, typically including or associated with a movement or presence sensor such as a PIR, which use Wi-Fi to transmit images and video to the alarm system control unit - generally when instructed so to do by the control unit. Wi-Fi is needed because of the bandwidth required to transmit large image/video files/streams in a timely fashion, especially for monitored alarm systems there is a need for good quality images/video to be available for review in real time, so that any intervention decided upon can be provided before it is too late to intervene.

[0006] In many countries/regions professionally installed alarms and their main components need to meet certain standards of performance - for example as defined in the relevant European standard EN50131 which must be met for relevant products marketed in the EU. CE For Alarm certified mains devices, a backup battery is required to provide a certain fixed time of operation. For example, a mains-powered control unit of a security monitoring installation is required to have a battery backup with an energy storage capacity sufficient to power the control unit for at least 12 hours in the event that mains power is lost. Mains powered video camera nodes that are provided as part of a professionally installed monitoring system are likewise generally required to include

a battery backup but typically it is the PIR detector that is the certified detector and a low power transceiver (rather than a Wi-Fi transceiver) that is the certified radio channel - so, for example, the camera node may be configured to send a small photo over the certified radio channel when the PIR is triggered, with higher resolution images/video sent using Wi-Fi. But because it is the PIR and certified radio channel that are used to provide alarm notifications, and the camera and Wi-Fi merely to provide confirmation, the battery backup only needs to provide sufficient energy to power the PIR and the transceiver that provides the certified radio channel for several hours operation, rather than needing to store enough energy to support the full functioning of the camera node for hours.

[0007] In an EN certified alarm, any peripheral that handle an alarm signal and that is mains powered will need a backup battery for several hours of operation after loss of mains power. However, a security monitoring system installation could have devices like a CCTV camera or an audio device listening for glass break or other noises, radar, or even a smart plug that controls a light that the system might turn on and these will not require EN certification., and hence are not required to have battery backup. The group of certified alarm sensors is actually quite small.

[0008] Also, many homeowners like to supplement their premises monitoring systems with, for example, one or more video cameras to enable the owner to check in on what is happening at home when they are away - for example, to check to see that their children have arrived home from school as usual, and that there are no strangers in the home. Images and video from such cameras may be accessed on demand by the owner using an app on a smartphone or computer, and may also be stored in the cloud for later review - all potentially independently of the security monitoring system. Such cameras are often referred to as "convenience cameras" because they provide the homeowner with the convenience of being able to check in on their home as and when they like - rather than only providing images/video in the event of s security incident. But such convenience cameras may also be integrated into a security monitoring system, so that images captured during a security incident, for example, may also be shared with the central monitoring station. In this way such "uncertified" cameras may also in effect become peripherals of the security monitoring system. But such uncertified cameras typically do not include battery backup to the mains power supply.

[0009] Another class of device that may operate as mains powered peripherals of a security monitoring system, and which typically do not have any kind of backup power supply are Wi-Fi extenders and Wi-Fi repeaters. Historically, Wi-Fi extenders and Wi-Fi repeaters would not generally be classed as alarm peripherals, but we have realised that there are situations where such a device may usefully function as an alarm peripheral if it includes a (non-Wi-Fi) transceiver for communication with the control unit of the security monitoring system - as we will describe shortly. For example, if the premises protected by the security monitoring system are very extensive (or if the building's construction is such that Wi-Fi signals are significantly attenuated between the central unit and certain Wi-Fi enabled peripherals of the system) it may be necessary to extend the reach of the Wi-Fi network of which the central unit is the access point so that the remote peripheral(s) are able to send data (images, video, etc.) to the central unit over Wi-Fi. If the relevant Wi-Fi extender or repeater is unplugged or otherwise deprived of power, the central unit and hence the central monitoring station 200 will be unaware of the effective loss of the peripherals that are beyond the unextended range of the Wi-Fi network hosted by the central unit 122.

[0010] Peripherals that rely on an external power source, such as a mains electricity supply, cannot be relied upon in the event of an interruption in their power supply - for example as the result of a failure of the power supply network consequent on network failure or storm damage, by a failure of the premises power supply - for example as the result of a circuit breaker being tripped, or as the result of the peripheral being disconnected from the domestic power supply - for example as the result of a premises resident unplugging the device from the socket supplying it with power, perhaps to use the socket to power another device, or as the result of the actions of a villain. While it would conceivably be possible to guard against such problems by including a substantial back up battery in each mains powered peripheral, this is generally neither economic nor practical - in terms of the bulk and capacity of battery required and in terms of the consequent additional cost, at least for non-certified devices such as convenience cameras and Wi-Fi repeaters and extenders. The result is that some mains powered peripherals are not provided with any backup battery power supply, and hence they provide a potential point of failure or weakness in any alarm system that relies on their presence.

[0011] The loss of mains power to a peripheral is likely to reduce the effectiveness of a carefully designed security monitoring system, and can also be the sign of a robbery attempt. As such there exists a need to improve the handling the loss of power to mains powered alarm peripherals. It will be appreciated that a similar problem exists where an alarm peripheral is powered by an external power supply other than mains and is cut off from that external power supply.

[0012] Embodiments of the invention seek to provide at least partial solutions to this problem.

Summary

[0013] According to a first aspect there is provided a peripheral for a home alarm system, the peripheral comprising: a processor operatively connected to a first transceiver that is configured to transmit signals to, and to

receive control signals from, a controller of the alarm system; the peripheral being configured to power the processor, the first transceiver and other power-consuming electronics of the peripheral using electricity supplied from an external energy source; a rechargeable energy store arranged to receive power from the external energy source and to power the second processor and the first transceiver, but not at least some of the other power-consuming electronics, in the event of loss of power from the external energy source; the processor being configured in the event of loss of power from the external energy source to cause the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power, the processor and the first transceiver drawing their power from the energy store.

[0014] Such a peripheral is able to signal loss of power to a controller of a security monitoring system, meaning that the controller, and potentially a remote monitoring station, become aware of the loss of power.

[0015] Optionally, the at least some of the other power-consuming electronics comprises a second transceiver. Optionally, the first transceiver has a relatively narrow bandwidth and a relatively low power consumption, and the second transceiver has a relatively wide bandwidth and a relatively high power consumption.

[0016] Optionally, the second transceiver is a Wi-Fi transceiver. Optionally, the peripheral may be configured as a Wi-Fi extender or a Wi-Fi repeater.

[0017] The peripheral of the first aspect may further comprise a sensor coupled to the processor. The sensor may comprise an image sensor, and optionally the peripheral is a video camera.

[0018] The first transceiver of the peripheral of the first aspect may be configured to operate using a communication protocol other than a communication protocol according to any of the IEEE 802.11 standards, as this may enable the first transceiver to operate with a low power consumption, thereby facilitating the sending of a lost power message using only a little stored energy. Similar transceivers in battery powered peripherals are preferably employed to achieve satisfactory battery life in those other peripherals. Optionally, the first transceiver is configured to operate using single-sideband modulation, Bluetooth low energy, Matter, or a channel in a dedicated ISM band, as all of these may permit very low power operation.

[0019] Optionally, the at least some of the other power-consuming electronics comprises a second processor. This may be a processor that is used to control a second transceiver, such as a Wi-Fi transceiver, or may be a more powerful processor than the first processor (for example a microprocessor as opposed to an MCU used as the first processor) that is used to control extra functionality in the peripheral.

[0020] The energy store of the peripheral may comprise one or more capacitors or super capacitors or a rechargeable battery.

[0021] According to a second aspect there is provided a peripheral for a home alarm system, the peripheral comprising: first and second transceivers, the first transceiver having a relatively narrow bandwidth and a relatively low power consumption, the second transceiver having a relatively wide bandwidth and a relatively high power consumption; the first transceiver being configured to transmit signals to, and to receive control signals from, a controller of the alarm system; and a processor operatively coupled to the first transceiver; the peripheral being configured to power the processor and the two transceivers using electricity supplied from an external energy source; an energy store arranged to receive power from the external energy source and to power the processor and the first transceiver, but not the second transceiver, in the event of loss of power from the external energy source; the processor being configured to cause the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power, the processor and the first transceiver drawing their power from the energy store. Such a peripheral may use the second transceiver for transmission of data that requires a high data rate, but by powering only the less power-hungry first transceiver to report power loss it becomes possible to provide power loss reporting functionality without the need for a large capacity energy store.

[0022] According to a third aspect there is provided a peripheral for a home alarm system, the peripheral comprising: a processor operatively connected to a first transceiver that is configured to transmit signals to, and to receive control signals from, a controller of the alarm system; the peripheral being configured to power the processor and the first transceiver using electricity supplied from an external energy source; a rechargeable energy store arranged to receive power from the external energy source and capable of storing no more power than is sufficient to power the processor and the first transceiver for no more than 5 minutes; the processor being configured in the event of loss of power from the external energy source to cause the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power, the processor and the first transceiver drawing their power from the energy store. Optionally the rechargeable energy store is capable of storing no more power than is sufficient to power the processor and the first transceiver for no more than 4, 3, 2, or 1 minutes or less. In this way it may possible to provide the new power loss reporting functionality with an energy store of small physical dimensions and of low cost.

[0023] According to a fourth aspect there is provided a premises security monitoring system comprising a mains powered controller and multiple peripherals, the controller being configured to receive event notifications from one or more of the peripherals and to report to a remote monitoring station alarm events based on at least some of these event notifications, the multiple peripherals including at least one peripheral as claimed in any one of the preceding claims, the controller being configured to report, unless the controller itself has lost mains

power, to the remote monitoring station any loss of power message received from one or any of the peripherals as claimed in any of the preceding claims.

[0024] According to a fifth aspect there is provided a method performed by a peripheral for a home alarm system, the peripheral comprising: a processor operatively connected to a first transceiver that is configured to transmit signals to, and to receive control signals from, a controller of the alarm system; the peripheral being configured to power the processor, the first transceiver and other power-consuming electronics of the peripheral using electricity supplied from an external energy source; a rechargeable energy store arranged to receive power from the external energy source and to power the second processor and the first transceiver, but not at least some of the other power-consuming electronics, in the event of loss of power from the external energy source; the method comprising in the event of loss of power from the external energy source, causing the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power using power drawn from the energy store.

[0025] According to a sixth aspect there is provided a method performed by a premises security monitoring system, the system comprising a mains powered controller and multiple peripherals, the controller being configured to receive event notifications from one or more of the peripherals and to report to a remote monitoring station alarm events based on at least some of these event notifications, the multiple peripherals including at least one peripheral according to the first aspect, the method comprising reporting, unless the controller itself has lost mains power, to the remote monitoring station any loss of power message received from one or any of the peripherals according to the first aspect.

[0026] The method of the sixth aspect may further comprise the control unit transmitting an instruction to a user interface of the security monitoring system to generate an output to warn occupants of the premises protected by the security monitoring system of the loss of a peripheral for which a loss of power message has been received.

[0027] According to a seventh aspect there is provided a mains powered control unit for a premises security monitoring system that includes multiple alarm peripherals, the control unit being configured to receive event notifications from one or more of the peripherals and to report to a remote monitoring station alarm events based on at least some of these event notifications, the controller being configured to report, unless the controller itself has lost mains power, to the remote monitoring station any loss of power message received from one or any of the alarm peripherals.

[0028] Optionally in the control unit of the seventh aspect the control unit may be further configured to transmit an instruction to a user interface of the security monitoring system to generate an output to warn occupants of the premises protected by the security monitoring system of the loss of a peripheral for which a loss of power message has been received.

Brief description of the drawings

[0029] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic plan of a single floor of premises in which a first security monitoring system has been installed, the system including a plurality of video cameras;

Figure 2 illustrates schematically the main elements of a mains powered peripheral for an alarm system such as that of Figure 1;

Figure 3 illustrates schematically the basics of radio-based presence detection such as Wi-Fi sensing; and

Figure 4 illustrates schematically features of a local management device of the system of Figure 1.

Specific description

[0030] Figure 1 shows schematically a home alarm system or security monitoring system installation 100 in premises comprising a dwelling standing in grounds, not shown. In this example the premises are in the form of a multi-story house, of which only the ground floor is shown. The house has a front door 104, that serves as the main entrance, and which leads into an entrance hall 106. For simplicity and ease of description the various rooms are shown as linked by doorways, but with doors omitted. In practice, of course, most of the doorways would typically be fitted with doors, and some or all of these doors may be fitted with door opening sensors such as that shown on the front door as sensor 107. Typically, these door opening sensors will be battery powered, using a magnet and a sensing element such as a magnetometer or reed switch, and include a radio transceiver for communicating with the local management device, or central unit, 122 of the security monitoring system. The entrance hall leads through to the living room 108, a dining room 110, and thence into a kitchen 112. The kitchen 112 includes the house's back door 114. Like the front door 104, the back door 114 is also provided with the door opening sensor 107. From the kitchen 112 there is an entry to a playroom 118. The playroom leads into a music room 120, and a conservatory 124 which in turn leads back into the entrance hall 106 which in turn leads to a cloakroom 125. Leading off the living room 108 is a library 126, and an office 128 which in turn leads through to a storage room 130. Stairs 131 in the hall lead up to the upper floors of the house.

[0031] Adjacent the front door 104, in the entrance hall, is a control panel 132 by means of which a user may arm and disarm the security monitoring system 100. In par-

ticular, when entering the house through the front door 104 when the system is armed, a user may use the control panel 132 to disarm the monitoring system 100, or to change the armed state from "armed away" - in which the security monitoring system both secures the perimeter of the house, and also monitors the interior of the house with the possibility of an alarm event being triggered upon motion been detected within the house; to "armed at home" state, in which the perimeter is monitored but movement within the house does not give rise to the central unit 122 raising an alarm event. The control panel is preferably mains powered with a backup battery power supply.

[0032] Another similar control panel, including a display, may also be provided adjacent the back door, but in this example a peripheral in the form of a disarm node 134 is provided instead. The disarm node permits arming and disarming of the security monitoring system using a dongle, a suitably programmed smart phone, or the like, and possibly arming and disarming by the entry of a PIN using a physical keypad or touchscreen.

[0033] The central unit 122 of the security monitoring system 100, here located in the library 126, is coupled to an external monitoring station 200 by means of a wired (broadband) connection to the Internet 210 and also by at least one radio network, e.g. a public land mobile network (PLMN). When the security monitoring system 100 is in the armed state, the triggering of an alarm event will cause the central unit 122 to report the alarm event to the external monitoring station 200, where typically a human operator will intervene, involving police and other security personnel as necessary. The premises may also include a router 500 of a broadband connection to the Internet to support a wired data network in the premises and optionally to provide another Wi-Fi network

[0034] The house shown in Figure 1 is provided with a plurality of peripherals in the form of internal video cameras 140, as well as external video cameras 142 to the front and rear of the premises. These video cameras 140 may all be connected to a mains power supply and be without battery backup. The video cameras typically include a first transceiver, with low-power consumption and low bandwidth, for receiving control signals from, and for reporting events to the central unit 122, along with a larger bandwidth and more power-hungry second transceiver, such as a Wi-Fi transceiver, for the transmission of images and video signals to the central unit (typically only done on command from the central unit, often as a result of an intervention from the remote monitoring station 200). The first transceiver is preferably configured to use a protocol, other than one according to any of the IEEE 802.11 standards, to transmit signals to, and to receive control signals from, the controller 122 of the alarm system

[0035] The house is shown without any windows, but of course in practice there would be windows and typically some at least of these windows would be provided with peripherals including sensors to detect opening or attempted opening the windows, again battery-powered and typically coupled to the central unit by means of an internal low bandwidth and low power transceiver.

[0036] If an intruder breaks into the house when the security monitoring system is in the armed away state, typically a window or door sensor peripheral will be triggered, resulting in an alarm event signal being sent by the peripheral to the central unit 122. Upon receiving the alarm event signal, the central unit 122 will typically report this to the remote monitoring station 200. As the intruder moves around the house, there are likely to trigger motion sensors, for example integrated into or associated with one or more of the internal video cameras 140. The relevant motion sensor or camera will then likewise report an alarm event to the central unit 122.

[0037] The central unit or controller 122 may be configured such that, as soon as it determines that there is an alarm event, it requests video (more generally images) from the cameras that have reported being triggered. But it may also be the case that the central unit 122 is configured also (or alternatively) to request video from an as yet untriggered camera - possibly in response to having received a request from the monitoring station 200 so to do: the idea being that the untriggered camera(s) may provide images, for example showing the intruder or enabling the intruder's presence or route to be determined.

[0038] The video cameras 140 may be configured to start to capture images, and possibly video sequences, starting from the triggering of the respective motion sensor, and typically these images and video sequences are initially stored on internal memory of the cameras 140 until they have been sent to the central unit 122, upon its request. The central unit 122 is typically not configured to store the videos received from the video cameras but instead forwards them directly to the remote monitoring station. At the central monitoring station 200 received videos are stored for review by an operative of the CMS.122.

[0039] At the remote monitoring station 200, even if the human operator picks up the alarm event notification from the central unit 122 almost immediately, the operator needs to assess whether the alarm indications suggest that there is a real incident, or whether it is a false alarm. This can be difficult without seeing images, and in particular high resolution video images. The central unit 122 of the security monitoring system 100 will already have started to transmit video files or image files from the cameras that have been triggered. But because in this case there are many rooms with many possible circulation routes between them, it is not immediately evident which camera is likely to provide the most useful images or video. The central unit 122 has limited capacity to receive video, because the capacity of the large bandwidth transceiver that uses to receive video/images from the cameras 140, 142, and therefore the central unit 122 preferably doesn't simultaneously instruct all triggered cameras to transmit their stored videos. Instead, the central unit 122 tend to send serial requests, allowing the

different video cameras to transmit their video/images one after the other. Once an incident is created, the central unit 122 will upload images to the remote monitoring station as they come in, based on the order to detection. If the central unit 122 received a detection notification from camera 1, 3, 4, 2. Images would be received in that order and transferred to a media tab for that incident (on a server, for example) for access by the operator at the remote monitoring station 200. It can be seen therefore that the remote monitoring station may have to wait several minutes, or more, before it receives the video/image data necessary to determine whether an intervention is required, and what type of intervention if any is required.

[0040] But the operator in the remote monitoring station 200 may decide that, based on the information already received, it would be useful to see images from an as yet untriggered camera - and therefore instruct the central unit 122 to signal to the relevant camera to turn on to capture and forward image data.

[0041] But if one or more of the cameras has been disabled, for example by being disconnected from the mains, the central unit and the central monitoring station will be unaware that the relevant cameras are unavailable - so that time can be wasted signalling to, and awaiting responses from, cameras that are effectively disabled. Whereas, had the central unit 122 and remote monitoring station been made aware of the fact that the relevant camera(s) were unavailable, some other course of action - such as requesting images from another untriggered camera that is still connected to power, could have been taken and useful images and information obtained rather than perhaps missed forever.

[0042] This scenario illustrates the very real problem that may arise as the result of a mains powered peripheral losing power.

[0043] Another problem may arise when a Wi-Fi enabled mains powered peripheral loses mains power, and that is due to the loss of Wi-Fi signals from the peripheral - for example where the peripheral is a Wi-Fi extender or repeater. Historically, Wi-Fi extenders and Wi-Fi repeaters would not generally be classed as alarm peripherals, but we have realised that there are situations where such a device may usefully function as an alarm peripheral if it includes a (non-Wi-Fi) transceiver for communication with the control unit 122 of the security monitoring system - as we will describe shortly. For example, if the premises protected by the security monitoring system are very extensive (or if the building's construction is such that Wi-Fi signals are significantly attenuated between the central unit 122 and certain Wi-Fi enabled peripherals of the system) it may be necessary to extend the reach of the Wi-Fi network of which the central unit 122 is the access point so that the remote peripheral(s) are able to send data (images, video, etc.) to the central unit over Wi-Fi. If the relevant Wi-Fi extender or repeater is unplugged or otherwise deprived of power, the central unit 122 and hence the central monitoring station 200 will be unaware of the effective loss of the peripherals that are beyond the unextended range of the Wi-Fi network hosted by the central unit 122 - with possibly even worse consequences than those already outlined.

[0044] We will now introduce a possible solution to this problem, with reference to Figure 2. This shows a generic alarm peripheral 250 which is configured to draw its power from a mains electricity supply 252 (e.g. of 110-120V or 240-250V for example) either via an external low voltage power supply 254, in which case the peripheral receives low voltage (6 to 24 Volts for example) from the power supply 254, or via an internal low voltage power supply (6 to 24 Volts for example) 256 in which case the peripheral receives mains voltage from the supply 252.

[0045] The peripheral includes a processor 258 which is preferably in the form of a microcontroller (MCU) which is configured to control the peripheral 250, and which includes memory (in the form of ROM and RAM), an oscillator, and I/O ports. The use of an MCU is preferred over the use of a conventional microprocessor primarily because MCUs are available that are suitable for the task of managing a peripheral while consuming very low power, which is highly desirable in this application. The processor 258 is coupled to and controls a first transceiver 260. This first transceiver is preferably configured to use a protocol other than one according to any of the IEEE 802.11 standards ("Wi-Fi standards") to transmit signals to, and to receive control signals from, the controller 122. By avoiding the use of any of the IEEE 802.11 standards the first transceiver can be configured for low power consumption device (consuming significantly less power than a Wi-Fi transceiver) with a relatively low transmission power (sufficient for communication with the central unit 122) and low bandwidth which is used to receive control signals from the central unit 122 of the alarm system, as well as to supply data and respond to the central unit 122 - but not for the transmission of, for example, video data or images. Optionally the low power transceiver 260 operates in one or more of the permitted ISM bands - such as around 868 MHz. But other protocols whose transceivers have low energy demands - such as Bluetooth Low Energy, or Matter (formerly Project Connected Home over IP), or the like could be used. Optionally the low power transceiver 260 use single-sideband transmission (either in an ISM band as mentioned above, or in some other band), because single-sideband transmission can help reduce transceiver energy demands. The processor 258 and the low power transceiver may conveniently be in the form of a combined processor/transceiver module.

[0046] Optionally, as shown, the peripheral 250 includes one or more sensors 262. The sensor(s) may comprise, for example a motion sensor (e.g. a PIR sensor), a contact switch for detecting the opening or closing of a door or window, a shock sensor (e.g. including a magnetometer and/or an accelerometer) for detecting shocks applied to doors or windows or their frames, an image sensor (e.g. of a video or still camera), or a microphone. Optionally, the peripheral may include multiple sensors

262- such as an image sensor, a motion/presence sensor, and a microphone - as will often be the case when the peripheral is a camera or video camera.

[0047] Optionally, the peripheral 250 may include a Wi-Fi module 264 including a processor 266 and one or more Wi-Fi transceivers 268 that are controlled by the processor 266. Typically, the power consumption of the Wi-Fi module is many times that of the combination of the processor 258 and the low power transceiver 260 - possibly an order of magnitude greater power consumption, for example. The peripheral may include one or more sensors and at least one Wi-Fi transceiver. For example, a video camera will typically include an image sensor, a motion/presence sensor, and a microphone, and will typically be configured to use the Wi-Fi transceiver to transmit video and audio files to the central unit 122. Each Wi-Fi transceiver has an associated antenna or antenna array, preferably one that supports MIMO as required by 802.11n and 802.11ac, for example.

[0048] As described so far, the internal structure of the peripheral 250 may be considered relatively conventional. However, the peripheral 250 additionally includes an energy storage unit 270, which is charged by electricity received from the mains via the power supply 254 or 256, and which is capable of briefly storing energy to power the processor 258 and the low power transceiver 260 after the loss of externally supplied power from the mains electricity supply 252. The energy storage unit 270 may comprise a capacitor or supercapacitor or a bank of multiple capacitors or supercapacitors (or possible a battery with a small storage capacity) that store sufficient energy to power the MCU and the low power transceiver 260 for long enough that the processor 258 is able to use the low power transceiver 260 to transmit a distress signal (which indicates or signifies that the peripheral has lost mains power - and will hence be unavailable until further notice).

[0049] Such a transmission may be set up and transmitted within a few seconds or less, typically no more than a second or a fraction of a second, but the energy store may be configured to store sufficient energy to power the MCU 258 and the first transceiver 260 for not more than 0.5, 0.7, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, or 19 seconds, optionally for not more than 20 seconds or 30 seconds or not more than a minute, so that the distress signal may be transmitted more than once before power is lost. Optionally, the energy store is configured to store energy sufficient to power the processor and first transceiver 260 for no more than 5 minutes.

[0050] The processor 258 is configured to respond to a loss of power from whichever of power supply 254 or 256 is supplying power by activating the low power transceiver 260 to transmit a message to the central unit 122, using energy from the energy storage unit 270. The message, which is preferably short, includes both a peripheral identifier known to the central unit and a code to signify that the peripheral has lost external power. The message may be pre stored in a memory of the MCU 258. The processor 258 may be configured to interrupt any existing activity of the first transceiver 260 - whether reception of control signals from the central unit 122 or the transmission of data or other signals to the central unit 122 in order to transmit the distress signal. As will be seen later, the central unit 122 of the alarm system preferably includes more than one ISM (or other low power technology such as BLE or Matter) transceiver for the transmission and reception of control signals and messages, one of which may be reserved for reception of messages from peripherals of the alarm system. Typically, messages received from the first transceivers of the peripherals are brief in duration (generally fractions of seconds), so that there should generally be a free window for reception of distress signals from peripherals that have lost power - particularly if the peripheral's energy storage unit stores sufficient power for multiple transmissions of the distress signal. The first transceivers of the peripherals may operate according to a listen before talk protocol, and if such a protocol is implemented it may still be used in the event of a loss of mains power. Typically listen before talk only involves about 5-10ms of RX and we can plan for that in the storage calculation.

[0051] Of course, if the protected premises suffers a power cut -due to a failure of the power transmission network, a main circuit breaker or RCD device for the house being tripped, or as the result of someone manually turning off power to the premises, the central unit will itself lose mains power, and all the mains powered peripherals provided with the distress signalling feature will transmit distress signals. It may be that some of these distress signals are, due to contention (even with the use of a listen before talk protocol), not received by the central unit - but given that the central unit 122 is itself already aware of the loss of power, this is not a problem.

[0052] More significant is if a distress signal is received from one peripheral and then, a little later (seconds or minutes later) a distress signal is received from another peripheral - because that may indicate that someone is deliberately sabotaging or disabling aspects of the alarm system - and the central unit 122 may be configured to respond to such a situation (or even to the loss of just one of the peripherals) both by sensing a warning of a potential incident to the remote monitoring station and by transmitting signals to any camera peripherals of the alarm installation to activate their cameras and to transmit their images to the central unit which can then forward them to the remote monitoring station for analysis and, if necessary, intervention. The central unit may be configured to do this even when the alarm system is disarmed, because although the peripherals might be being disconnected from the mains by a legitimate actor for innocent reasons, the disabling of the peripherals can most easily be done by villains (more generally, actors with a nefarious purpose in mind) when the security monitoring system is disarmed.

[0053] The central unit 122 may additionally or alter-

natively be configured to respond to reception of a distress signal from a mains powered peripheral by transmitting a signal to a user interface of the security monitoring system - such as control panel 132, to cause the control panel to sound a warning, preferably including a voiced announcement to the effect that the relevant peripheral has been disconnected from the mains - e.g. "the security camera (or the Wi-Fi repeater) in the lounge has been disconnected from the mains, please reconnect it". The same or a similar message may also be displayed on the display of the control panel 132. The central unit 122 may also be configured to send a corresponding message to the remote monitoring station 200 and/or to cause a message to be pushed to one or more registered user(s), for example using a cloud -based system that pushes notifications to user(s)'s smartphones or other registered devices. These messages are again (like messages sent to the remote monitoring station) preferably sent whether the security monitoring system is armed or not.

[0054] The alarm peripherals are preferably configured to announce themselves when they come back on line - e.g. when power is restored the peripheral powers up and sends a "hello" message until the central unit responds and the login process kicks off. In this way, the central unit learns when a peripheral has power restored after announcing loss of power.

[0055] As previously mentioned, if the alarm peripheral is a Wi-Fi extender or Wi-Fi repeater, its loss of power can result in the loss of Wi-Fi support for multiple other alarm peripherals - which potentially has serious consequences. Where the peripheral is a Wi-Fi repeater, the Wi-Fi module 264 will generally also include a wireline modem that couples to a wireline modem to provide an ethernet link to receive signals from the central unit 122.

[0056] Another reason why it can be useful to know that a mains-powered peripheral such as a Wi-Fi enabled device has lost power is that such devices may form part of a radio-based presence detection system that provides the security monitoring system with information about the location and movements of humans within a monitored area or areas of the premises protected by the monitoring system. In such a system the central unit 122 may act as an access point of a Wi-Fi network and may also run the radio-based presence detection system using Wi-Fi signals transmitted from Wi-Fi enabled peripherals of the security monitoring system.

[0057] In order to aid the reader's understanding, we here provide a brief introduction to radio-based presence detection, which may for example be based on analysing the signal dynamics and signal statistics of radio signals and/or detecting changes in channel state information (CSI). A radio (or wireless) signal as used herein refers to a signal transmitted from a radio transmitter and received by a radio receiver, wherein the radio transmitter and radio receiver operate according to a standard or protocol. Such standards include, but are not limited to, IEEE 802.11. (which includes the Wi-Fi standards), IEEE 802.15 (which includes Zigbee), Bluetooth SIG, IEEE 802.16, IEEE 802.20, UMTS, GSM 850, GSM 900, GSM 180, GSM 19011, GPM ITU-R 5.13, GPM ITU-R 5.150, ITU-R 5.280, 3GPP 4G (including LTE), 3GPP 5G, 3GPP NR, AND IMT-2000. However, the radio transmitters and receivers may operate in non-telecommunications or Industrial, Scientific and Medical (ISM) spectral regions without departing from the scope of the invention.

[0058] Essentially the idea is to use radio signals to probe a zone or zones of interest, and to analyse and extract statistics from these signals, in particular looking at the physical layer and/or data link layer such as MAC address measurements that expose the frequency response of a radio channel (e.g., CSI or RSSI measurements). These measurements are processed to detect anomalies and variations over time, and in particular to detect changes signifying the entrance of a person and/or movement of a person within a monitored zone. The zone(s) to be monitored need to be covered sufficiently by radio signals, but the sources of the radio signals may either already be present before a monitoring system is established - for example from the plurality of Wi-Fi or Bluetooth capable devices that are now dotted around the typical home or office, or the sources may be added specifically to establish a monitoring system. Often some established (i.e., already located or installed) radio devices are supplemented by some extra devices added as part of establishing a radio-based presence detection system. Among the types of devices (pre-installed or specifically added) that may be used as part of such a detection system are Wi-Fi access points, Wi-Fi routers, smart speakers, Wi-Fi repeaters, as well as video cameras and video doorbells, smart bulbs, etc. Because presence (or intrusion) is detected by detecting a change in the properties or character of radio signals compared to some previous reference signal(s), it is preferred to establish what might be termed the monitoring network between radio devices that are essentially static (i.e., that remain in the same position for extended periods) rather than relying on devices that are repeatedly moved - such as smart phones, headphones, laptops, and tablet devices. It is not strictly speaking essential for all the devices whose signals are used by the monitoring system to be part of the same network - for example, signals from Wi-Fi access points of neighbouring premises could be used as part of a monitoring system in different premises. Again, a primary consideration is the stability of the signals from the signal sources that are used. Wi-Fi access points provided by broadband routers are seldom moved and rarely turned off, consequently they can generally be relied upon as a stable signal source - even if they are in properties neighbouring the property containing the zone or zones to be monitored.

[0059] The idea is illustrated very schematically in Figure 3, here with an installation 300 including just a single source (or illuminator) 302 and just a single receiver 304, for simplicity, although in practice there will typically be multiple sources (illuminators) and sometimes plural re-

ceivers. The installation 300 has been established to monitor a monitored zone 306. In Figure 3A we see that in steady state, and in the absence of a person, radio signals are transmitted from the source 302, spread through the monitored zone 306, and are received by the receiver 304. Of course, in most installations there will be walls, ceilings, floors, and other structures that will tend to reflect, at least in part, signals from the source. Furniture and other objects may block and attenuate the signals, the reflected signals will give rise to multiple paths, and the signals may interfere with each other, and there may be scattering and other behaviours, such as phase shifts, frequency shifts, all leading to complexity in the channels experienced by the radio signals that arrive at the receiver 304. But while the environment is static and unchanging, the receiver will tend to see a consistent pattern of radio signals. And this is true whether or not the source transmits continuously or transmits periodically. But this consistent pattern of received signals is changed by the arrival of an intruder 308, as shown in Figure 3B. From Figure 3B we see that, at the very least, the presence of a person in the monitored zone blocks at least some of the signals from the source, and that affects the pattern of radio signals received by the receiver 304. The changed pattern of signals received by the receiver enables the presence of the intruder to be detected by a presence monitoring algorithm that is supplied with information derived from the received signals. It will be appreciated that the nature and extent of the perturbation of the signals passing from the source 302 to the receiver 304 is likely to change as the intruder 308 enters, passes through, and leaves the monitored area 306, and that this applies also to reflected, refracted, and attenuated signals. These changes may enable the location of a person within the zone, and their speed of movement, to be determined.

[0060] It will be realised that in effect, signals that are received from an illuminator device (or from more than one illuminator device) after having passed through a monitored space (or volume), have in effect been filtered by as a result of the environment to which they have been exposed. We can therefore imagine the monitored volume as a filter having a transfer coefficient, and we can see that a received signal is at least in part defined by the properties, or channel response, of the wireless channel through which it is propagated. If the environment provided by the monitored volume changes, for example by the addition of a person, then the transfer coefficient of the filter, and the channel response or properties, will also change. The changes in the transfer coefficient, and that in the channel response, consequent on the change in the environment of the monitored space, can be detected and quantified by analysing radio signals received by the wireless sensing receiver(s). Both the introduction of an object, e.g. a person, into the monitored space and movement of that object within the monitored space will change the environment and hence change the effective transfer coefficient and the channel response.

[0061] The radio-based sensing system can be trained by establishing a base setting in which the monitored zone is unoccupied, which is then labelled as unoccupied for example by an installer using a smartphone app or the like, and then training occupied states by a person entering, standing, and then walking through each of the zones one by one. Presence at different locations in each of the zones may be captured and labelled in the system in the same way. This process may be repeated with two people, and then optionally with more people. In essence this is a supervised machine learning approach, but other approaches to training may be used.

[0062] The system may need to be retrained for the base setting if bulky furniture (or if a large metal objects) is added to or moved within the monitored space, because these can be expected to change the propagation properties of the relevant zone/space. The data for unoccupied states is preferably retained within a database of "unoccupied" states, even when there are changes to the arrangement of furniture etc. It may not be necessary to retrain for the occupied states, if the system can determine a delta function between the previous base state and the new one, because the delta function may also be applicable in occupied states. But if not, it may be sufficient to retrain only a subset of the occupied states previously learnt. The system may also be configured to self-learn to accommodate changes in the characteristics of the zones when unoccupied, and to add newly determined unoccupied state data to the database.

[0063] Although the Figure 3 example uses just a single source (illuminator) and a single receiver, as already mentioned often multiple sources (illuminators) will be used in order to achieve satisfactory coverage of the zone or zones to be monitored. Multiple zones may be monitored by a single receiver through the use of multiple strategically placed sources, but each zone, or some zones of multiples zones may have a dedicate receiver that does not serve other zones. Likewise, a radio signal source (illuminator) may provide illuminating signals for a single monitored zone or for multiple monitored zones. Also, a presence monitoring system (and a security monitoring system including such a presence monitoring system) may use mesh network arrangement, for example a Wi-Fi mesh network, in which multiple devices act as receivers for illuminating signals - either for a single monitored zone or for multiple monitored zones.

[0064] The reader will now understand that, if a security monitoring system is configured to use radio-based presence detection, it is useful to know if any of the devices (peripherals) used as illuminators is going to be unavailable, because the loss of one or more illuminators will inevitably lead to a change in the pattern of radio signals traversing the monitored space. This in turn can be expected to alter the pattern of signals, and the effects of the presence and positions of people within the monitored space on the signals received by the device that is running the presence detection system (e.g. the central unit 122).

[0065] Whichever device is running the presence detection system - which may be the central unit 122, or some other device such as another access point, may be trained to adapt to the loss of recognised ones of the illuminators of the system - by repeatedly exposing the device to signal patterns for empty premises and premises with one or more people at identified locations with different known illuminators (peripheral) turned off (either individually or in combinations). Then, in the event that one or more distress signals is received by the central unit 122, the central unit (if that is running the presence detection system) can switch to a setting appropriate for the loss of the relevant illuminator. If another device is controlling the presence detection system, the device can be informed by the central unit 122of any distress signals received or otherwise indicate the loss of the relevant identified peripheral(s).

[0066] Figure 4 is a schematic drawing showing in more detail features of the gateway or central unit 122 of Figures 1, as this will assist in understanding what is required of a peripheral for use in a security monitoring system including such a central unit 122. The gateway 122 includes a first transceiver 430 coupled to the first antenna 480, and preferably also a second transceiver 432 coupled to a second antenna 482. The transceivers 430 and 432 can each both transmit and receive, but a transceiver cannot both transmit and receive at the same time. Thus, the transceivers 430, 432 each operate in half duplex. Preferably a transceiver will use the same frequency to transmit and receive (although of course if the two transceivers are to operate simultaneously but in opposite modes, they will operate on different frequencies). The transceivers 430, 432 may be arranged such that one transceiver 430 uses a first frequency for transmit and receive and the second transceiver 432 uses the same first frequency for transmit and receive, i.e. the transceivers are arranged to operate in a diversity-like arrangement. Alternative, the second transceiver may, depending on configuration, be arranged to use a second frequency for transmit and/or receive. The transceivers 430 and 432 are coupled to a controller 450 by a bus. The controller 450 is also connected to a network interface 460 by means of which the controller 450 may be provided with a wired connection to the Internet and hence to the monitoring centre 200. The network interface may also be used to connect the central unit to a wireline modem that is paired with a corresponding wireline modem in a peripheral in the form of a Wi-Fi repeater, the two modems communication using a wireline protocol over a power network that connects the two devices.

[0067] The controller 450 is also coupled to a memory 470 which may store data received from the various peripherals of the installation for example event data, sounds, images and video data. The central unit 122 includes a crystal oscillator 451, which is preferably a temperature controlled or oven-controlled crystal oscillator. This is used for system clocking and also frequency control of the transceivers. The gateway 122 includes a power supply 362 which is coupled to a domestic mains supply, from which the gateway 122 generally derives power, and a backup battery pack 464 which provides power to the gateway in the event of failure of the mains power supply. The central unit 122 also includes a Wi-Fi transceiver 440, and associated antenna arrangement 442, which may be used for communication with any of the peripherals that are Wi-Fi enabled. The Wi-Fi enabled peripheral may be a remote control or control panel that may for example be located close to the main entrance to the building (e.g., control panel 128 or disarm node 130) to enable the occupier to arm or disarm the system from near the main entrance, it may for example be an image-capture device such as a video camera (e.g. camera 126), or as previously mentioned it may be a Wi-Fi repeater or Wi-Fi extender.

[0068] Similarly, an interface enabling bidirectional communication over a Public Land Mobile Network (PLMN), such as GSM or LTE, may optionally be provided. Optionally, a third antenna 484 and associated ISM transceiver 434 may be provided, for example for communication with the monitoring centre 200 over, for example, the European 863MHz to 870MHz frequency band. Optionally, the third transceiver 434 may be a Sigfox transceiver configured to use the Sigfox network to contact the central monitoring station especially in the event that jamming of other radio channels is detected.

[0069] The first 430 and second 432 transceivers are preferably both tuneable ISM devices, operating for example in the European 863MHz to 870MHz frequency band or in the 915MHz band (which may span 902-928MHz or 915-928MHZ depending upon the country). In particular, both of these devices may be tuned, i.e. may be tuneable, to the frequencies within the regulatorily agreed sub-bands within this defined frequency band. Alternatively, the first transceiver and the second transceiver, if present, may have different tuning ranges and optionally there is some overlap between these ranges. Optionally, the first 430 and second 432 transceivers may be BLE or Matter transceivers, or the like.

[0070] The controller 450 may be configured to run a sensing application using a WFS software agent 800, which may be stored in memory 470. The WFS software agent 400 uses WFS radio APIs in the Wi-Fi transceiver 440 to interact with the Wi-Fi radio, the APIs enabling extraction of desired channel environment measurement information and provides the ability to assert any related controls to configure WFS features. The sensing application on the CU will report a presence state change when the appropriate thresholds are triggered, along with the address of the device whose received data triggered the algorithm. The WFS agent provides a monitoring system which enables the security monitoring system to detect presence and movement in a monitored space, without the necessity to use line of sight motion detectors.

[0071] As an alternative to incorporating a radio sensing application into the central unit, this functionality can be provided on an access point, e.g. a Wi-Fi access point,

AP such as router 500, of the premises, with the AP configured to report the result of presence detection to the central unit 122. In another example, a Wi-Fi range extender could instead be used as sensing master for its connected peripherals but would be configured to report to the central unit 122 which would be the overall master in terms of reporting the "alarm".

Claims

1. A peripheral for a home alarm system, the peripheral comprising:

   a processor operatively connected to a first transceiver that is configured to transmit signals to, and to receive control signals from, a controller of the alarm system;
   the peripheral being configured to power the processor, the first transceiver and other power-consuming electronics of the peripheral using electricity supplied from an external energy source;
   a rechargeable energy store arranged to receive power from the external energy source and to power the second processor and the first transceiver, but not at least some of the other power-consuming electronics, in the event of loss of power from the external energy source;
   the processor being configured in the event of loss of power from the external energy source to cause the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power, the processor and the first transceiver drawing their power from the energy store.

2. The peripheral of claim 1, wherein the at least some of the other power-consuming electronics comprises a second transceiver.

3. The peripheral of claim 2, wherein the first transceiver has a relatively narrow bandwidth and a relatively low power consumption, and the second transceiver has a relatively wide bandwidth and a relatively high power consumption.

4. The peripheral of claim 2 or claim 3, wherein the second transceiver is a Wi-Fi transceiver.

5. The peripheral of claim 4, wherein the peripheral is configured as a Wi-Fi extender or a Wi-Fi repeater.

6. The peripheral of any one of claims 1 to 4, wherein the peripheral further comprises a sensor coupled to the processor.

7. The peripheral of claim 6, wherein the sensor comprises an image sensor.

8. The peripheral of claim 7, wherein the peripheral is a video camera.

9. The peripheral of any one of the preceding claims, wherein the first transceiver is configured to operate using a communication protocol other than a communication protocol according to any of the IEEE 802.11 standards.

10. The peripheral of claim 9, wherein the first transceiver is configured to operate using single-sideband modulation, Bluetooth low energy, Matter, or a channel in a dedicated ISM band.

11. The peripheral of any one of the preceding claims, wherein the at least some of the other power-consuming electronics comprises a second processor.

12. The peripheral of any one of the preceding claims, wherein the energy store comprises one or more capacitors or super capacitors or a rechargeable battery.

13. A peripheral for a home alarm system, the peripheral comprising:

   first and second transceivers, the first transceiver having a relatively narrow bandwidth and a relatively low power consumption, the second transceiver having a relatively wide bandwidth and a relatively high power consumption; the first transceiver being configured to transmit signals to, and to receive control signals from, a controller of the alarm system; and
   a processor operatively coupled to the first transceiver;
   the peripheral being configured to power the processor and the two transceivers using electricity supplied from an external energy source;
   an energy store arranged to receive power from the external energy source and to power the processor and the first transceiver, but not the second transceiver, in the event of loss of power from the external energy source;
   the processor being configured to cause the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power, the processor and the first transceiver drawing their power from the energy store.

14. A peripheral for a home alarm system, the peripheral comprising:

   a processor operatively connected to a first transceiver that is configured to transmit signals to, and to receive control signals from, a control-

ler of the alarm system;
the peripheral being configured to power the processor and the first transceiver using electricity supplied from an external energy source;
a rechargeable energy store arranged to receive power from the external energy source and capable of storing no more power than is sufficient to power the processor and the first transceiver for no more than 5 minutes;
the processor being configured in the event of loss of power from the external energy source to cause the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power, the processor and the first transceiver drawing their power from the energy store.

15. A premises security monitoring system comprising a mains powered controller and multiple peripherals, the controller being configured to receive event notifications from one or more of the peripherals and to report to a remote monitoring station alarm events based on at least some of these event notifications, the multiple peripherals including at least one peripheral as claimed in any one of the preceding claims, the controller being configured to report, unless the controller itself has lost mains power, to the remote monitoring station any loss of power message received from one or any of the peripherals as claimed in any of the preceding claims.

16. A method performed by a peripheral for a home alarm system, the peripheral comprising:

a processor operatively connected to a first transceiver that is configured to transmit signals to, and to receive control signals from, a controller of the alarm system;
the peripheral being configured to power the processor, the first transceiver and other power-consuming electronics of the peripheral using electricity supplied from an external energy source;
a rechargeable energy store arranged to receive power from the external energy source and to power the second processor and the first transceiver, but not at least some of the other power-consuming electronics, in the event of loss of power from the external energy source;
the method comprising
in the event of loss of power from the external energy source, causing the first transceiver to transmit a message to inform the controller of the alarm system of the loss of power using power drawn from the energy store.

17. A method performed by a premises security monitoring system, the system comprising a mains powered controller and multiple peripherals, the controller being configured to receive event notifications from one or more of the peripherals and to report to a remote monitoring station alarm events based on at least some of these event notifications, the multiple peripherals including at least one peripheral as claimed in any one of claims 1 to 14, the method comprising reporting, unless the controller itself has lost mains power, to the remote monitoring station any loss of power message received from one or any of the peripherals as claimed in any of claims 1 to 14.

18. The method of claim 17, further comprising the control unit transmitting an instruction to a user interface of the security monitoring system to generate an output to warn occupants of the premises protected by the security monitoring system of the loss of a peripheral for which a loss of power message has been received.

19. A mains powered control unit for a premises security monitoring system that includes multiple alarm peripherals, the control unit being configured to receive event notifications from one or more of the peripherals and to report to a remote monitoring station alarm events based on at least some of these event notifications, the controller being configured to report, unless the controller itself has lost mains power, to the remote monitoring station any loss of power message received from one or any of the alarm peripherals.

20. The control unit of claim 19, wherein the control unit is further configured to transmit an instruction to a user interface of the security monitoring system to generate an output to warn occupants of the premises protected by the security monitoring system of the loss of a peripheral for which a loss of power message has been received.

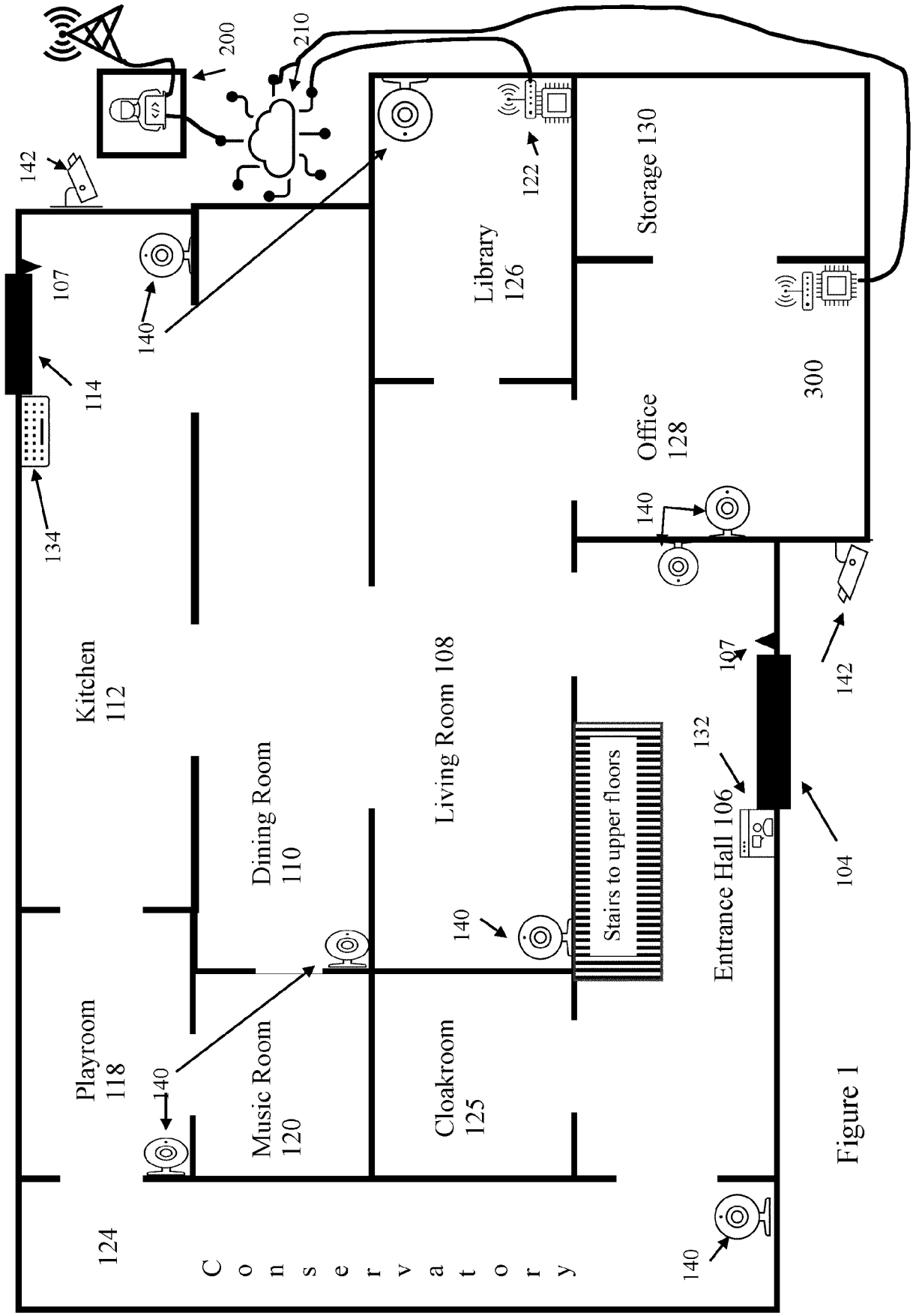
200
210
142
107
140
114
134
122
Storage 130
Library
126
300
Office
128
Kitchen
112
Dining Room
110
Living Room 108
Stairs to upper floors
Playroom
118
Music Room
120
Cloakroom
125
Entrance Hall 106
132
104
124
Conservatory

Figure 1

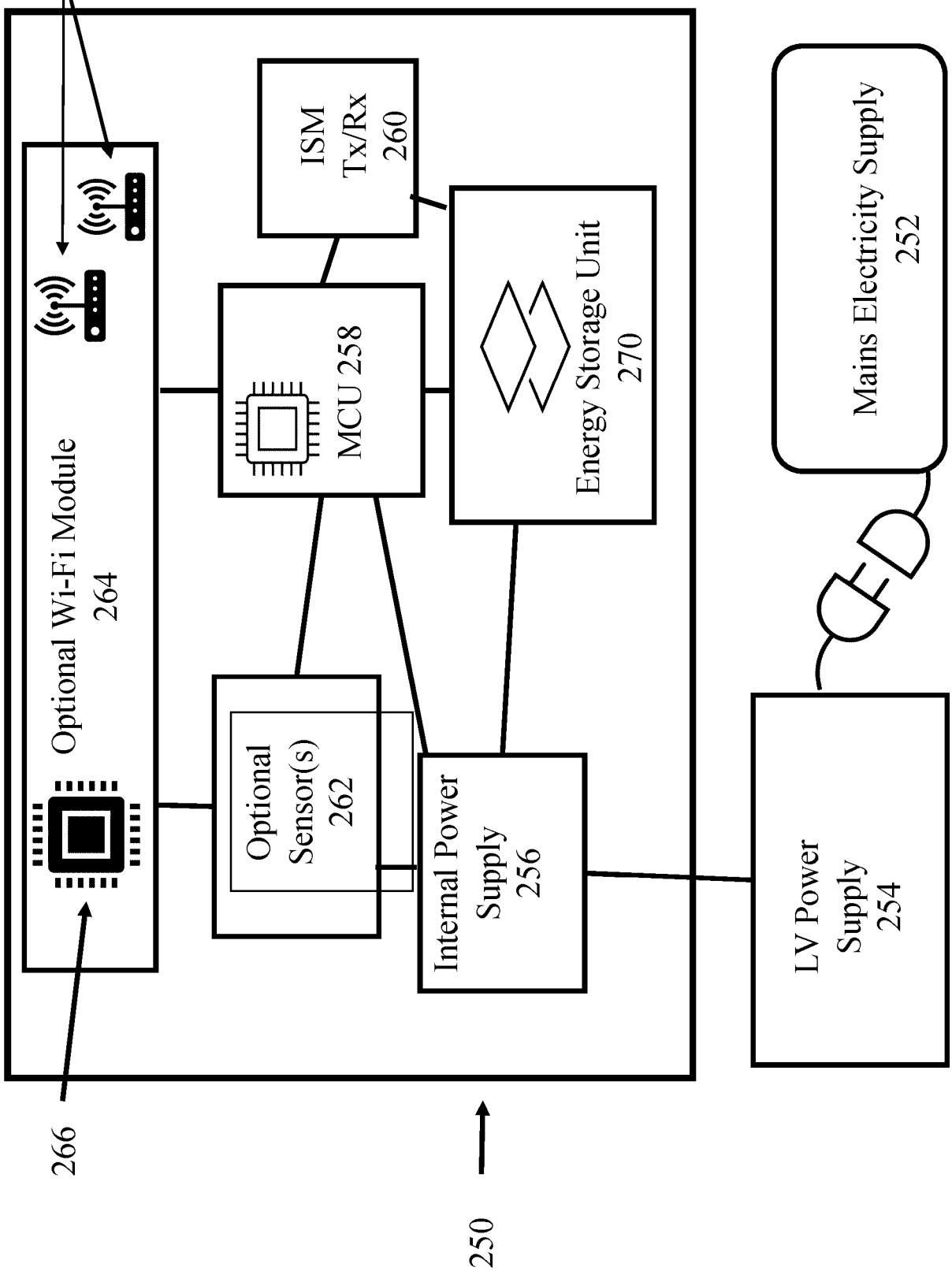
268
Optional Wi-Fi Module
264
ISM
Tx/Rx
260
MCU 258
Energy Storage Unit
270
Mains Electricity Supply
252
Optional
Sensor(s)
262
Internal Power
Supply
256
LV Power
Supply
254
266
250

Fig. 2

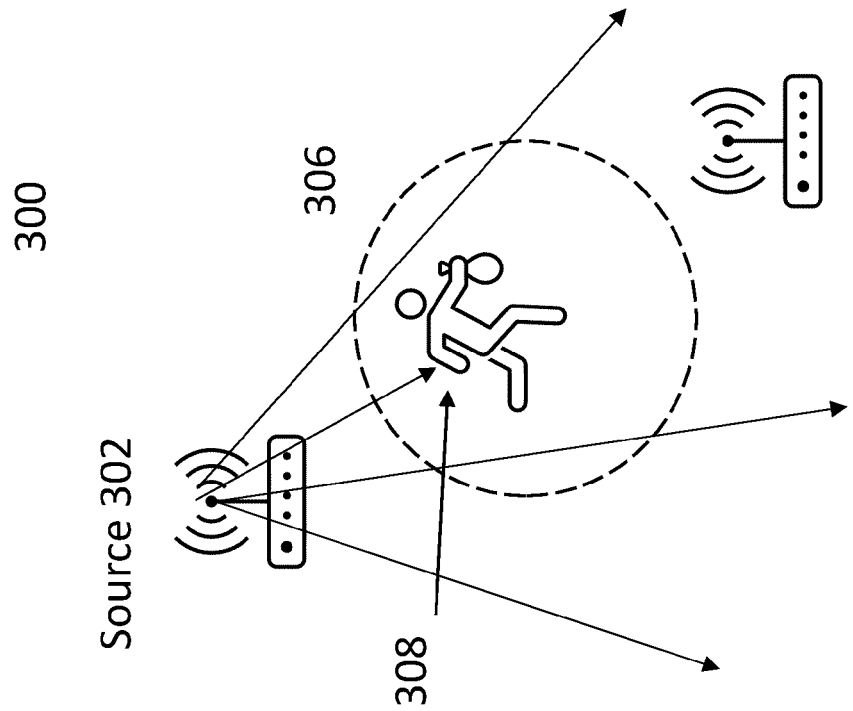

Figure 3B

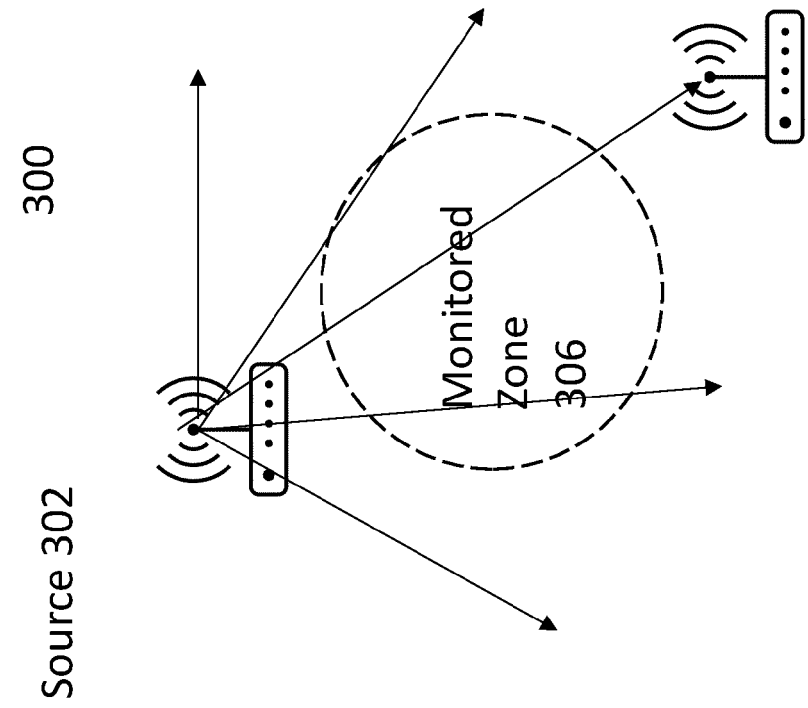

Figure 3A

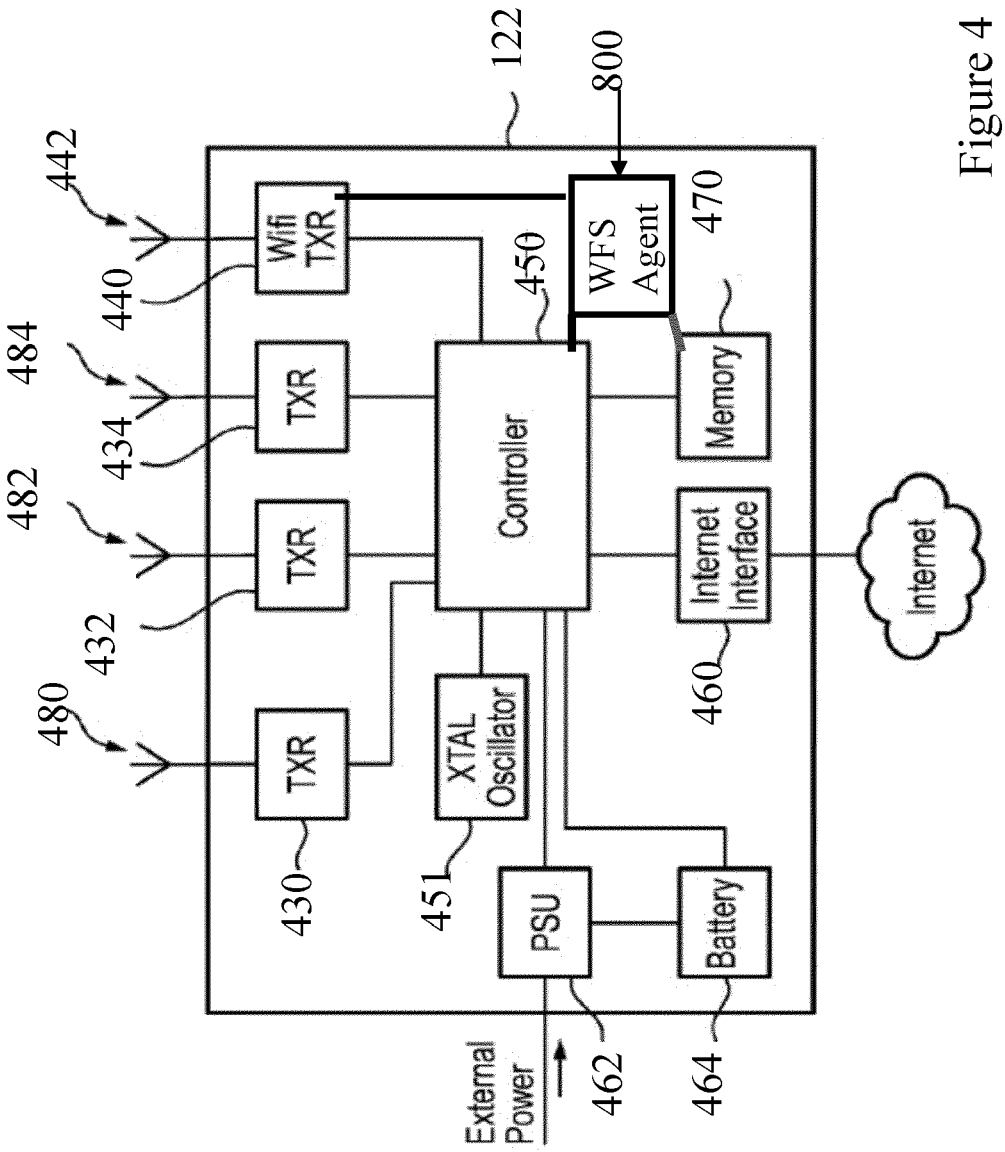
122
800
442
440
484
434
482
432
480
430
451
450
470
460
462
464
Wifi TXR
TXR
TXR
TXR
Controller
WFS Agent
Memory
Internet Interface
Internet
XTAL Oscillator
PSU
Battery
External Power

Figure 4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 22 15 7532

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	US 2014/266767 A1 (HUANG LONGGANG [US] ET AL) 18 September 2014 (2014-09-18) * paragraphs [0001] - [0004], [0007], [0015] - [0051]; figures 1-3 *	1-20	INV. G08B29/18 ADD. G08B13/196
Y	US 7 209 048 B1 (PACE JOSEPH R [US] ET AL) 24 April 2007 (2007-04-24) * column 1, line 23 - column 2, line 10 * * column 2, line 63 - column 3, line 27; figures 1-3 * * column 3, lines 49-56 * * page 4, line 1 - page 5, line 2; figures 5-7 * * claims 1-2 *	1-20	
Y	EP 2 701 132 B1 (NOVAR GMBH [DE]) 4 July 2018 (2018-07-04) * paragraphs [0001], [0003], [0005] - [0008], [0010], [0017], [0021], [0024], [0025], [0028] - [0030], [0032], [0049], [0051], [0085]; figure 1 *	12,14	TECHNICAL FIELDS SEARCHED (IPC) G08B
Y	US 2019/156658 A1 (HESS BRIAN K [US] ET AL) 23 May 2019 (2019-05-23) * paragraphs [0002], [0003], [0011] - [0013], [0019] - [0021], [0034] - [0035], [0040] - [0041], [0045]; figures 1-3 *	12,14	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	9 August 2022	Russo, Michela

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

EPO FORM 1503 03.82 (P04C01)

Europäisches Patentamt
European Patent Office
Office européen des brevets

Application Number
EP 22 15 7532

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing claims for which payment was due.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for those claims for which no payment was due.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☒ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

☐ The present supplementary European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims (Rule 164 (1) EPC).

Europäisches Patentamt
European Patent Office
Office européen des brevets

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 22 15 7532

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-20

all searched claims

1.1. claims: 1-13, 15-20

a peripheral device for a home alarm system, a corresponding control unit and the corresponding method for providing a notification of power loss at the peripheral as well as backup power to essential circuitry only.

1.2. claim: 14

a peripheral device for a home alarm system, comprising a backup battery with very limited energy storage.

Please note that all inventions mentioned under item 1, although not necessarily linked by a common inventive concept, could be searched without effort justifying an additional fee.

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 22 15 7532

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.

09-08-2022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014266767 A1	18-09-2014	CN 104076723 A	01-10-2014
		EP 2779134 A2	17-09-2014
		TW 201503067 A	16-01-2015
		US 2014266767 A1	18-09-2014
US 7209048 B1	24-04-2007	NONE	
EP 2701132 B1	04-07-2018	CN 103778755 A	07-05-2014
		EP 2701132 A1	26-02-2014
US 2019156658 A1	23-05-2019	US 2017316679 A1	02-11-2017
		US 2019156658 A1	23-05-2019
		US 2020342746 A1	29-10-2020

EPO FORM P0459

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