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

(11) **EP 4 506 920 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
12.02.2025 Bulletin 2025/07

(21) Application number: **23382828.4**

(22) Date of filing: **08.08.2023**

(51) International Patent Classification (IPC):
G08B 29/04 *(2006.01)* ***G08B 13/00*** *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G08B 29/046; G08B 13/00; G08B 29/08

(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:
- **NOBLE ECHEVERRIA, Jon**
  28224 Pozuelo de Alarcon (ES)
- **ALFARO, César**
  28224 Pozuelo de Alarcon (ES)
- **OVEJERO, Ivan**
  28224 Pozuelo de Alarcon (ES)

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

(54) ALARM PERIPHERAL

(57) Provided is a method of handling tamper signals from a tamper detecting device, the method comprising: processing a signal received from a tamper detection arrangement of the device, to determine whether, after at least a first change in signal state, the signal meets predetermined stability criteria; determining whether a signal meeting the predetermined stability criteria corresponds to a tamper violation of the alarm peripheral; and causing transmission of a tamper violation signal in response to a determined tamper violation.

Also provided is an alarm peripheral including a tamper detection arrangement, a processor of the peripheral being configured to: process a signal received from the tamper detection arrangement, to determine whether, after at least a first change in signal state, the signal meets predetermined stability criteria; determine whether a signal meeting the predetermined stability criteria corresponds to a tamper violation of the alarm peripheral; and cause transmission of a tamper violation signal in response to a determined tamper violation.

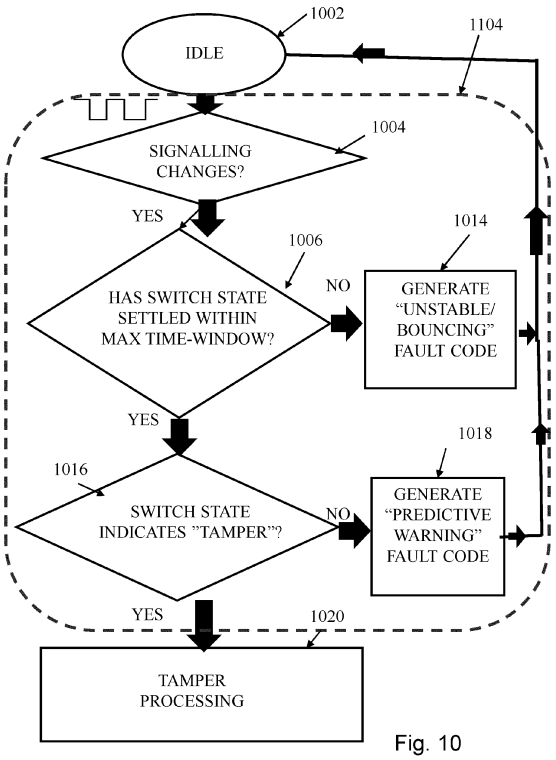

Fig. 10

EP 4 506 920 A1

Description

Technical field

[0001] The present invention relates to alarm peripherals having a tamper detection function, to installations and systems including such peripherals, and to related methods.

Background

[0002] Security installations that are or include security monitoring systems for monitoring premises, often referred to as burglar alarms, 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 alarm peripherals in the form of: 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. 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 Alarm Receiving Centre (ARC) or Central Monitoring Station (CMS) 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] If the operator of a monitored security monitoring system wants to be able to summon police assistance as the result of an automated call to the ARC, the system must generally comply with certain standards or regulations designed to reduce the incidence of false alarms. For example, in Europe, EN standard 50136 on alarm transmission systems requires that security monitoring system peripherals must be tamper protected - meaning that the peripherals must report detected tamper events such as attempts to tamper with the peripheral's power supply, attempts to remove the peripheral from its mounting surface, attempts to obscure or shield motion detectors, etc.

[0005] As with other aspects of security monitoring systems, with tamper detection it is important to avoid false alarms because operators of such systems may be penalised by the police or by industry regulators if more than a given number or percentage of alarm events reported to the police are false alarms. Sanctions may include fines and/or the removal of the right to summon police assistance - which may result in such alarm systems losing the approval of insurance companies, which in turn may jeopardise the operator's business. Additionally, resources devoted to handling false alarms cannot simultaneously be devoted to servicing real alarm events - meaning that either response times for handling real alarm events increase, or that more resources (typically both system resource and head count) must be employed.

[0006] It is therefore important to reduce the incidence of false alarms consequent on detected tamper events.

[0007] WO2019/115505A1 describe a tamper-protected peripheral which is designed to detect any attempt to remove the peripheral from the surface on which it is mounted, or to access a battery compartment of the peripheral. The peripheral comprises a tamper detection element and a housing arranged to be mounted on a surface such as a door or window frame, or a wall, and secured by screw mounting or by means of an adhesive element (such as a tape or pad with adhesive on its two main faces). The tamper detection element is biased towards a first position and arranged to be displaced away from the first position when the housing is mounted on the surface. The peripheral is arranged to generate an alarm signal in response to the detection of the movement of the tamper detection element towards the first position when the peripheral is removed from the surface.

[0008] With tamper-protected peripherals of this kind the speed of installation is often much greater if the peripheral is fixed to its mounting surface using an adhesive rather than screw mounting. Speed of installation is an important consideration for the installers of such equipment and for their employers. This means that frequently adhesive fixing is chosen over screw fixing for reasons of convenience or economy (of course, in some situations, it may either not be possible or not practical to use screw fixing), although not all surfaces

may be suitable for adhesive attachment: dusty or greasy substrates, flaking paint or other friable surfaces, may prove to be unsuitable for adhesive attachment, so that screw attachment may be required.

[0009] The present inventors have appreciated that, over time, the integrity of an adhesive attachment may reduce significantly, especially if elevated temperatures are experienced. This may mean that an adhesively attached peripheral may become less well secured to its mounting surface, which in turn may give rise to the detection of (phantom) tamper events that are not the result of manipulation, but rather the result of an unreliable attachment. The biasing of a tamper detection element may contribute to the failure of an adhesive attachment, but initially the failure may not be visible during routine inspection. This problem may also arise with peripherals that are secured to their mounting surface using screws or other mechanical fasteners, and not just with adhesively secured peripherals.

[0010] The present inventors have appreciated that another problem can arise, perhaps as a result of a tamper-protected peripheral being secured to a less than flat surface, when a tamper-sensing arrangement (such as a bimodal switch arrangement comprising an electrical element) rests at a point near the transition between its two modes. This can result in the tamper-sensing arrangement switching repeatedly between (oscillating or "bouncing") its two modes even when no attempt is being made to manipulate the peripheral. For example, the opening or closing of a door or window, to whose frame the peripheral is attached, may result in a tamper event being triggered as the tamper-sensing arrangement switches repeatedly between its two modes. The same behaviour may also occur as the result of passing road or rail traffic, whether the peripheral is wall mounted or mounted to a door or window. Such a problem may arise whatever the mode of mounting the peripheral to its support surface, and not just with adhesively secured peripherals.

[0011] The present inventors have appreciated that there therefore exists a need to improve alarm peripherals, in particular their tamper-protection capabilities, and security monitoring systems including such peripherals.

[0012] 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.

[0013] Embodiments of the present invention seek to provide enhanced security monitoring systems, and corresponding apps, methods and other implementations that improve the scope of security monitoring systems to address aspects of the problem of phantom tamper detection events, as well as providing new functionality and methods.

Summary

[0014] According to a first aspect there is provided an alarm peripheral including a tamper detection arrangement, a processor of the peripheral being configured to:

process signals received from the tamper detection arrangement to discriminate between genuine tamper events and erroneous tamper events;
generate a tamper fault signal in the event of detecting an erroneous tamper event (also referred to as a tamper fault).

[0015] In an alternative implementation the processing may be performed off-device, that is on something other than the alarm peripheral itself - such as on the controller of a security monitoring installation of which the peripheral forms part, or at a remote monitoring station that supports the security monitoring installation of which the peripheral forms part. These considerations apply equally to the various other aspects of the invention.

[0016] It should also be noted that premises security monitoring installations that include one or more alarm peripherals according to the first aspect may include an on-premises controller which may act as a gateway between the peripherals and a remote monitoring centre, but equally premises security monitoring installations that include one or more alarm peripherals according to the first aspect may be built without an on-premises controller - instead the alarm peripherals, or at least some of them, may be configured to communicate with a remote monitoring centre - for example using hardware/-functionality (e.g., an appropriate transceiver) to support LTE Cat M and/or NB-IoT (NarrowBand-Internet of Things) which are both cellular communication protocols, using (3GPP) licensed frequency spectrum, with potential ranges of up to 10km. These considerations apply equally to the various other aspects of the invention - and hence the other aspects may be used in security monitoring installations with or without the presence of a local controller, with or without on-device processing, and with the alarm peripherals optionally including any or all of the previously described communications technology to support "direct" communication with a remote monitoring station.

[0017] As used herein, the term "tamper fault" means a condition in which there is a lack of reliability of the tamper detection arrangement. This may arise as the result of poor installation or of degradation subsequent to installation. The lack of reliability may stem from the peripheral becoming loose - perhaps through partial or complete failure of an adhesive layer securing the peripheral to a mounting surface, or an unstable fixing arrangement such as a screw that has worked loose in a mounting substrate. Equally, the lack of reliability may arise from the tamper detection arrangement being near its point of transition, possibly as the result of the peripheral being mounted to an uneven surface or the decay or degrada-

tion of a surface with which the tamper detection arrangement co-operates. In addition, lack of reliability may be the result of something coming loose within the peripheral itself - perhaps as the result of a mechanical failure or as the result of vibration. Thus, the term "tamper fault" is to be construed broadly.

[0018] According to a second aspect, optionally in combination with the first aspect, there is provided an alarm peripheral including a tamper detection arrangement, a processor of the peripheral being configured to:

process a signal received from the tamper detection arrangement, to determine whether, after at least a first change in signal state, the signal meets predetermined stability criteria;
determine whether a signal meeting the predetermined stability criteria corresponds to a tamper violation of the alarm peripheral; and
cause transmission of a tamper violation signal in response to a determined tamper violation.

[0019] In an alarm peripheral according to the first or second aspect, the processor may be programmed to determine signal stability based on tamper state values of n of m consecutive signal samples, $m \geq n$, and optionally n is at least 5.

[0020] In an alarm peripheral according to any variant of the first or second aspect, the processor may be programmed to determine signal stability based on tamper state values of n consecutive signal samples, $n>1$, within a predetermined time period, and optionally n is at least 5.

[0021] In an alarm peripheral according to any variant of the first or second aspect, the processor may be signal a fault in the event that the signal does not meet the predetermined stability criteria.

[0022] According to a third aspect, optionally in combination with the first and/or second aspect, there is provided an alarm peripheral including a tamper detection arrangement and an accelerometer, a processor of the peripheral being configured to:

process signals received from the tamper detection arrangement; and
cause the transmission of a tamper violation signal in the event that signals are received from the tamper detection arrangement along with signals from the accelerometer that are indicative of manipulation of the peripheral.

[0023] Optionally, the processor of an alarm peripheral according to the third aspect may be programmed to cause the transmission of a tamper fault signal in the event that signals are received from the tamper detection arrangement without the accelerometer providing signals indicative of manipulation of the peripheral.

[0024] An alarm peripheral according to any variant of the first through third aspects may further comprise an RF transmitter coupled to the processor, the processor being programmed to use the RF transceiver to transmit tamper violation and tamper fault signals to a corresponding RF receiver. Optionally, the RF transmitter may include a transmitter configured to operate on a low power wide area cellular network such as LTE Cat M and NB IoT.

[0025] According to a fourth aspect, optionally in combination with any variant of the first and/or second aspect and/or third aspect, there is provided a security monitoring installation at premises protected by the installation, the installation comprising a controller and a plurality of alarm peripherals configured to transmit event notifications to the controller, the controller being configured to report alarm events to a monitoring station remote from the premises, wherein at least one of the alarm peripherals is as claimed in any one of the preceding claims, the controller having at least one operating mode in which it is programmed to report detected tamper events to the monitoring station.

[0026] According to a fifth aspect, optionally in combination with any variant of the first and/or second aspect and/or third aspect, there is provided a security monitoring installation at premises protected by the installation, the installation comprising a plurality of alarm peripherals configured to transmit event notifications to a monitoring station remote from the premises, wherein at least one of the alarm peripherals is according to any variant of the first through third aspects, said at least one alarm peripheral being programmed to report detected tamper events to the monitoring station.

[0027] According to a sixth aspect, optionally in combination with any variant of the first and/or second aspect and/or third aspect, there is provided a security monitoring installation at premises protected by the installation, the installation comprising a controller and a plurality of alarm peripherals each including a tamper detection arrangement each configured to transmit event notifications to the controller, the controller being configured to report alarm events to a monitoring station remote from the premises, the controller having at least one operating mode in which it is programmed to:

process a signal received from the tamper detection arrangement, to determine whether, after at least a first change in signal state, the signal meets predetermined stability criteria;
determine whether a signal meeting the predetermined stability criteria corresponds to a tamper violation of the alarm peripheral; and
cause transmission of a tamper violation signal in response to a determined tamper violation.

[0028] In a security monitoring installation according to the sixth aspect, the controller may have at least one operating mode in which it is programmed to:

process signals received from the tamper detection arrangement of one of the alarm peripherals and to

discriminate between genuine tamper events and erroneous tamper events;
generate a tamper fault signal in the event of detecting an erroneous tamper event; and report the tamper fault signal to the monitoring station remote from the premises. The controller may be programmed to signal a fault indicative of a need for preventative maintenance in the event that the signal meets the predetermined stability criteria and no tamper violation is determined. The controller may additionally or alternatively be programmed to signal a fault in the event that the signal does not meet the predetermined stability criteria.

[0029] According to a seventh aspect, optionally in combination with any variant of the first and/or second aspect and/or third aspect and/or fourth aspect and/or fifth aspect and/or sixth aspect, there is provided a system that comprises a security monitoring installation at premises protected by the installation and a monitoring station remote from the premises, the security monitoring installation having a controller and a plurality of alarm peripherals configured to transmit event notifications to the controller, the controller being configured to report alarm events to the monitoring station, wherein at least one of the alarm peripherals is according to any variant of the first through third aspects, the controller having at least one operating mode in which it is programmed to report detected tamper events to the monitoring station.

[0030] According to an eighth aspect, optionally in combination with any variant of the first and/or second aspect and/or third aspect and/or fourth aspect and/or fifth aspect and/or sixth aspect and/or seventh aspect, there is provided a system that comprises a security monitoring installation at premises protected by the installation and a monitoring station remote from the premises, the security monitoring installation having a plurality of alarm peripherals configured to transmit event notifications to the monitoring station, wherein at least one of the alarm peripherals is according to any variant of the first through third aspects, said at least one alarm peripheral being programmed to report detected tamper events to the monitoring station.

[0031] In systems according to either the seventh or eighth aspects, said at least one alarm peripheral may include an RF Transmitter arranged to operate on a low power wide area cellular network such as LTE Cat M and NB IoT.

[0032] According to a nineth aspect, optionally in combination with any variant of the first and/or second aspect and/or third aspect and/or fourth aspect and/or fifth aspect and/or sixth aspect and/or seventh aspect and/or eighth aspect there is provided a method of handling tamper signals from a tamper detecting device, the method comprising:

processing a signal received from a tamper detection arrangement of the device, to determine whether, after at least a first change in signal state, the signal meets predetermined stability criteria;
determining whether a signal meeting the predetermined stability criteria corresponds to a tamper violation of the alarm peripheral; and
causing transmission of a tamper violation signal in response to a determined tamper violation.

[0033] The method may comprise determining signal stability based on tamper state values of n of m consecutive signal samples, $m \geq n$, and optionally n is at least 5.

[0034] The method may additionally or alternatively further comprise signalling a fault indicative of a need for preventative maintenance in the event that the signal meets the predetermined stability criteria and no tamper violation is determined.

[0035] The method may additionally or alternatively further comprise signalling a fault in the event that the signal does not meet the predetermined stability criteria.

[0036] In a method according to any variant of the nineth aspect, the processing may be performed by a processor of a control unit of the premises security monitoring system, the peripheral being communicatively coupled to the control unit.

[0037] In a method according to any variant of the nineth aspect, the processing may be performed at a monitoring station remote from the premises, the peripheral being communicatively coupled to the remote monitoring station.

Brief description of figures

[0038] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying figures, in which:

Figure 1 shows, in partial cross-section, a tamper detecting device of a type to which the invention may be applied;
Figures 2, 2A, and 2B show details of exemplary mechanical interface elements of the tamper detection arrangement of the device of Figure 1;
Figure 3 is a partial sectional view through the mechanical interface element of Figure 2;
Figure 4 shows internal detail of part of the device of Figure 1, including an anti-tamper arrangement;
Figure 5 is an enlarged view of part of Figure 4, showing attachment of the anti-tampering arrangement;
Figures 6-7 are enlarged cross-sectional views of the electronic device of Fig. 1 with the mechanical element of the anti-tampering system in second and first positions, respectively;
Figure 8 is an enlarged cross-sectional view of an alternative embodiment of an electronic device comprising a switch with the mechanical element of the anti-tampering system in the second position;
Figure 9 illustrates schematically the main functional

units of a tamper sensing device according to aspects of the invention;

Figure 10 is a flow chart illustrating a method according to a first aspect of the invention; and

Figure 11 is a flow chart illustrating a method according to a second aspect of the invention.

Specific description

[0039] The present inventors have appreciated that the performance of devices that include tamper detection can be improved by applying various kinds of filtering to signals received from the tamper detection system. In some aspects, using signals from an accelerometer within the device may further enhance performance. The inventors' insights may be applied to tamper-sensing devices of current design, with suitable reprogramming or firmware updates, but equally the insights may be applied to new device designs and in particular, but not exclusively, to devices that include at least one accelerometer.

[0040] To provide context for the invention in its various aspects, we will first provide a description of an example of a known tamper-sensing device. Figures 1 to 8 are taken from the applicant's PCT patent application WO2019/115505. Figure 1 shows an electronic device 10, according to an aspect of the invention, prior to installation. The electronic device 10 comprises a housing 12, an electronic circuit 14 arranged within the housing 12, a power source 16 for providing electrical power to the electronic circuit 14, and an anti-tampering arrangement 18. The electronic circuit 14 comprises a processor or microcontroller (not shown) and a printed circuit board, PCB 15. The housing 12 includes a first half 20 configured to support the electronic circuit 14 and the power source 16 thereon. The housing 12 also includes a second half 22 configured to support the anti-tampering arrangement 18 thereon. The anti-tampering arrangement 18 comprises a mechanical element 34 that is arranged to protrude through an aperture 38 when the device 10 is free of the support/mounting surface 24, typically by means of an applied bias. Once the device is installed (e.g. mounted to a surface 24), the mechanical element is pushed into the device (typically closing a tamper switch) ready to emerge from the body of the device, under action of the bias, in the event that the device is removed from its mounting surface 24.

[0041] For example, the electronic device 10 may be a device typically mounted on a support surface 24 such as a wall, a door, a window frame, etc. For example, the electronic device 10 may be sensor device for an anti-burglary system, or a sensor device for a process indicator system such as a level indicator, or a device for private or public use such as smoke sensor, security camera, public phone and so forth. Electronic circuit 14 may comprise a radio unit for communicating, under the control of the processor or microcontroller, with a central unit of an alarm system such as a premises security monitoring system that may in turn report security events to a remote monitoring station. The electronic circuit may also include a vibration sensor, such as an accelerometer, not shown, to sense vibration or shocks. The electronic circuit may also include a magnetic sensor such as a magnetometer or reed relay, for detecting the presence (and proximity) of a magnetic field - for example for use in detecting the position or state of a door or window.

[0042] The second half 22 of the housing 12 includes a surface 36 having an opening 38 configured to allow the portion 34 of the mechanical element 32 to extend therethrough as just described. In an example, the second half 22 of the housing 12 may be a back panel of the housing 12 of electronic device 10 and includes the surface 36 habitually used for mounting the electronic device 10 on the support surface 24. Further, the first half 20 of the housing 12 may be an outer cover of the electronic device 10, and may be removable in order to provide access to the electronic circuit 14 and the power source 16. Moreover, according to an embodiment, the second half 22 also includes at least one hole 40 configured to receive at least one screw (not shown) for mounting the housing 12 on the support surface 24. Alternatively, the second half 22 may include an adhesive element (not shown) arranged on the surface 36 of the housing 12 to enable mounting on the support surface 24. In an example, the electronic device 10 may be screw mounted and require an adequate number of holes 40 to accommodate a sufficient number of screws for mounting. As an alternative, mounting may be done by using the adhesive element, such as a two-sided tape, or a layer of glue, arranged on the surface 36 of the housing 12. It will be appreciated that the adhesive element would be placed so as not to interfere with the opening 38 on the surface 36 of the housing 12.

[0043] Various anti-tampering arrangements 18 are illustrated in Figs 2 to 2B. The anti-tampering arrangement 18 comprises an electrical element 30, and a mechanical element 32 coupled to the electrical element 30. A portion 34 of the mechanical element 32 extends from a surface 36 of the housing 12 (as shown in Fig. 1).

[0044] Fig. 2A shows an alternative anti-tampering arrangement 18 in which the mechanical element 30 comprises a first spring S 1, a second spring S2 and a plate 33. A first end of first spring S1 and second spring S2 are firmly attached to the plate 33. A second end of first spring S 1 is attached to the second half 22 of the housing 12. The spring constant of first spring S 1 is smaller than the spring constant of second spring S2. The first spring S 1 may be coaxial with second spring S2. Fig. 2B illustrates an embodiment in which the first spring S1 is replaced by two springs arranged one on either side of second spring S2. The total spring constant of the two springs S1 is smaller than spring constant of second spring S2.

[0045] With reference to Fig. 3, a cross-section of the anti-tampering arrangement 18 of Fig. 2 is illustrated

according to one embodiment. As shown, the mechanical element 32 of the anti-tampering arrangement 18 includes a shaft 42 having a first end portion 44 coupled to the electrical element 30 and a second end portion (i.e. the portion 34 of the mechanical element 32) opposite to the first end portion 44 and configured to extend from the surface 36 of the housing 12, as shown in Fig. 1. The mechanical element 32 also includes a lateral flange 46 extending from the first end portion 44 of the shaft 42 and a longitudinal flange 48 coupled to the lateral flange 46 and extending along the shaft 42. The mechanical element 32 also includes a pair of connecting pieces 50 coupled to the longitudinal flange 48. The pair of connecting pieces 50 is configured to engage with connecting tabs 52 configured within the housing 12 (shown in Figs. 4 and 5).

[0046] With reference to Figs. 4 and 5, illustrated are the second half 22 of the housing 12 attached with the anti-tampering arrangement 18. Fig. 5 clearly illustrates that the pair of connecting pieces 50 engages with the connecting tabs 52, configured on the second half 22 of the housing 12. This allows the anti-tampering arrangement 18 to be held securely with the second half 22, when the portion 34 of the mechanical element 32 protrudes out of the surface 36 of the housing 12. Further, the longitudinal flange 48 along with the connecting pieces 50 prevents any undesirable movement of the anti-tampering arrangement 18 with respect to the housing 12.

[0047] With reference to Figs. 6 and 7, operation of the anti-tampering arrangement 18 for the electronic device 10 is illustrated. In operation, the mechanical element 32 is configured to attain a first position (shown in Fig. 6) from a second position (shown in Fig. 7) when the surface 36 of the housing 12 is mounted on the use-surface 24 (shown in Fig. 1). Further, in the first position the electrical element 30 contacts the electronic circuit 14 for closing an electrical connection to avoid generation of an alarm signal. Moreover, in the second position the electrical element 30 moves away from the electronic circuit 14 for opening the electrical connection to generate the alarm signal.

[0048] In operation, the shaft 42 can be configured to actuate with the help of the lateral flange 46 to allow the mechanical element 32 to attain the first position and the second position with the mounting and removal of the housing 12, respectively, as shown in Figs. 6 and 7. For example, the lateral flange 46 may be in the form of a flexible bellow, which allows a longitudinal movement of the shaft 42 with respect to the housing 12. The flexible bellow 46 will return to second position when unloaded. As mentioned above, the mechanical element 32 is composed of silicon, and different parts of the mechanical element 32 are configured to have different properties. For example, the longitudinal flange 48 is configured to be rigid in nature to prevent unnecessary movement of the mechanical element 32, whereas the shaft 42 and the lateral flange 46 are configured to be flexible in nature to accommodate longitudinal movement of the shaft 42 and to push electrical element 30 and shaft 42 to the second position when unloaded. Lateral flange 46, specifically when formed as a bellow, will provide a high resilience. A flexible character of shaft 42 and lateral flange 46 will result in a high resilience and a low pressure on the adhesive during installation. The high resilience will also lower the force exerted on the adhesive when the device is mounted.

[0049] With reference to Fig. 6, the electronic device 10 is illustrated in a mounted state (i.e. when the mechanical element 32 is in the first position). Upon mounting the housing 12 on the use-surface 24, pressure applied by the use-surface 24 against the shaft 42 pushes the lateral flange 46 towards the electronic circuit 14. This causes the electrical element 30 to be pressed against the electronic circuit 14. Therefore, when the electronic device 10 is fully mounted on the use-surface 24, either using screws or adhesive element, the portion 34 of the mechanical element 32 of the anti-tampering arrangement 18 is pressed. This results in the electrical element 30 closing electrical connection for the electronic circuit 14. It may be appreciated that a force, acts on the portion 34 of the mechanical element 32, which contradicts an adhesive force offered by an adhesive means used for mounting the electronic device 10 on the use-surface 24. However, such force acting on the portion 34 should be as small as possible to prevent weakening of the adhesive force, which allows mounting of the electronic device 10 on the use-surface 24. For example, if the electrical element 30 is a conductive carbon pill, the carbon pill is pressed against conductive pads on the electronic circuit 14 when the housing 12 is mounted on the use-surface 24 (i.e. the mechanical element 32 attains the first position), thus closing the electrical connection and providing a no-alarm condition. In another example, if the electrical element 30 is a microswitch 35, c.f. Fig. 8, mounted on the electronic circuit 14, the shaft 42 of the mechanical element 32 activates the microswitch upon being compressed by the use-surface 24.

[0050] With reference to Fig. 7, the electronic device 10 is illustrated in an un-mounted state (i.e. when the mechanical element 32 is in the second position). In this state, the lateral flange 46 pushes the shaft 42 arranged with the electrical element 30 away from the electronic circuit 14. Accordingly, the mechanical element 32 of the anti-tampering arrangement 18 attains the second position from the first position, i.e. the portion 34 of the mechanical element 32 protrudes or extends out from the opening 38 (shown in Fig. 1) of the surface 36 of the housing 12. Consequently, tampering of the electronic device 10 will result in the mechanical element 32 of the anti-tampering arrangement 18 reverting to the second position, thus causing a tamper alarm signal. For example, if the electronic device 10 is forcefully removed from the use-surface 24 (shown in Fig. 6), the shaft 42 will decompress and the lateral flange 46 will move to its unloaded position, thus breaking contact of the electrical element 30 with the electronic circuit 14 and giving the

tamper alarm signal. Similarly, if the first half 20 of the housing 12 is removed for repair or maintenance work, contact of the electronic circuit 14 with the electrical element 30 is lost, thus giving the tamper alarm signal.

[0051] With reference to Fig. 8, the electronic device 10 is illustrated in an un-mounted state (i.e. when the mechanical element 32 is in the second position). In this state, the lateral flange 46 pushes the shaft 42 arranged with the electrical element 30 away from a switch or micro switch 35 of the electronic circuit 14. Accordingly, the mechanical element 32 of the anti-tampering arrangement 18 attains the second position from the first position, i.e. the portion 34 of the mechanical element 32 protrudes or extends out from the opening 38 (shown in Fig. 1) of the surface 36 of the housing 12. Consequently, tampering of the electronic device 10 will result in the mechanical element 32 of the anti-tampering arrangement 18 reverting to the second position, thus causing a tamper alarm signal.

[0052] Upon mounting the housing 12 of the embodiment of the electronic device shown in Fig. 8 on the use-surface 24, pressure applied by the use-surface 24 against the shaft 42 pushes the lateral flange 46 towards the electronic circuit 14. This causes the shaft 42 to be pressed against the micro switch 35 of the electronic circuit 14. Therefore, when the electronic device 10 is fully mounted on the use-surface 24, either using screws or adhesive element, the portion 34 of the mechanical element 32 of the anti-tampering arrangement 18 is pressed. This results in the switch 35 closing electrical connection for the electronic circuit 14.

[0053] It should be appreciated that the foregoing description is merely exemplary of tamper sensing devices in which a mechanical tamper detecting element cooperates with an electrical arrangement to detect tampering. Figure 9 illustrates schematically the main functional units of a tamper sensing device 900 according to aspects of the invention. A processor 902, which may be a microcontroller, is coupled to a power supply 904. In many applications, the power supply 904 will be an autonomous power supply, for example based on battery technology. A tamper detection arrangement 906, for example as previously described, is also coupled to the processor 902 to provide the processor with signals in the event that the tamper detection arrangement 906 is disturbed. Preferably, the processor 902 is coupled to an RF transceiver (or separate transmitter and receiver) for communication with a controller of a security monitoring system (or potentially for direct communication with a remote monitoring station) for the reporting of detected tamper events. The device 900 further comprises a sensor 910, such as a magnetic contact switch (which may be embodied as a magnetometer, a reed relay, a Hall sensor, or the like) for detecting the state of a door or window, that is also coupled to the processor 902 (such a device may itself be referred to as a "magnetic contact switch"). In the case that the sensor 910 is triggered or otherwise detects an event, signals from the sensor may be processed by the processor 902 and an event reported via the RF transceiver 908 to the controller of the security monitoring system (for potential onward transmission to a remote monitoring station) or directly to the remote monitoring station.

[0054] In addition, the device 900 may include an accelerometer or other vibration sensor 912 (which may be in addition to or instead of sensor 910) to detect shock (e.g.as the result of blows from an object, such as a hammer, occasioned during an attempted break in) and/or movement (such as movement of a door or window as it is opened or closed, or broken down) and to provide appropriate signals to the processor 902 to which it is coupled.

[0055] Having set the scene, we will now describe a method 1000 according to a first aspect of the invention will be described with reference to Figure 10 which is a flow chart illustrating the method. The method starts at 1002 with the tamper detection system in an idle state ready to respond to any tamper detection signals. Upon receiving a signal 1004 indicating a change of state of the tamper detection arrangement, the processor starts a timer during which it monitors signals received from the tamper detection arrangement to determine whether there is evidence of "tamper bouncing". The inventors have realised that sometimes an installation results in the tamper detection arrangement being positioned, or dislodging over time, so that it is very close to the transition point (e.g. with the tamper switch closed but only just so, so that vibration or shock, may cause the tamper switch to open - perhaps momentarily). Under these circumstances the tamper detection arrangement may fluctuate or oscillate between open and closed states, even though no attempt is being made to manipulate the device - that is, in the absence of real tamper. Upon detecting a change of state 1004, the processor waits at step 1006 to determine whether the tamper detection arrangement settles to a steady state, within a maximum time (e.g. time-out) window determined by the timer. For example, the duration may be not more than about 120ms, optionally not more than about 100ms, optionally not more than about 90ms, optionally not more than about 80ms.

[0056] A variety of techniques and/or conditions may be used to determine whether a state of the tamper arrangement has settled. The processor may be arranged to sample the state of the tamper detection arrangement repeatedly during the duration of the timer. The sample values may be binary values corresponding to the state of the tamper detection arrangement, or non-binary values. Step 1006 may comprise processing the sampled values to determine whether the values are substantially consistent, for example, at least "n" of "m" consecutive values being consistent (e.g. equal, in the case of binary values), where "n" and "m" are integers. The value "m" defines a number of consecutive samples considered, at least within a sliding processing window. The proportion "n/m" allows for a tolerance to determine substantial consistency within this processing window.

For example, the value "m" may be at least 8, at least 9, at least 10, at least 11, or at least 12 samples. The value "n" may be equal to "m", or it may be smaller than "m" by, for example, a value of 1, or 2, or 3 or more. When "n" and "m" are equal to each other, step 1006 comprises detecting "m" consecutive consistent samples (e.g. without any deviation in the case of binary values) to determine that the tamper arrangement state has settled.

[0057] The duration of the timer may correspond to the time taken to sample the "m" samples, or the duration may be longer. When the duration is longer, step 1006 may optionally determine that the tamper arrangement state has settled before expiry of the timer, if the condition for substantially consistent (or consistent) sample values is detected sooner. Allowing step 1006 to terminate earlier, when a stable tamper arrangement state is detected, may avoid delaying processing of a tamper signal any longer than is needed to verify the stable state. The timer duration may then be regarded as a maximum permitted duration, or time-out, for the state of the tamper detection arrangement to settle. Providing a longer time duration allows more flexibility in time for the processing in step 1006 to determine an effective state of a tamper detection arrangement, even in the case of some fluctuation or bounce, within certain limits of acceptable performance.

[0058] If step 1006 concludes without detecting a stable state of the tamper detection arrangement within the permitted time duration, the processor determines that tamper bounce is occurring, and sends 1014 an appropriate fault code to indicate "tamper bouncing". This fault code may be transmitted to the controller of the security monitoring installation, for onward transmission to a remote monitoring station or back end system, or the fault code may be transmitted directly to the remote monitoring station or back end system using for example an appropriate cellular IoT protocol. (e.g. LTE-M, EC-GSM-IoT, or NB-IoT).

[0059] But if step 1006 detects that the tamper detection arrangement has settled (either before expiry of the timer, or at expiry of the timer) the processor may be programmed:

in the case that the signal does not indicate tamper, to send 1018 a predictive maintenance fault report, to indicate that the device experienced a hardware glitch for a while - indicating the need for the device to be inspected;

in the case that the signal does indicate tamper, either to send a tamper alert (e.g. as described with reference to the tamper bouncing fault report), or to apply a further method 1020 to determine whether the detected tamper was accompanied by the detection of movement (using the accelerometer or other vibration sensor).

[0060] Thus, the processor may be programmed to apply an anti-bounce and/or stabilization algorithm. One such algorithm may look for n consecutive consistent and/or same-value of tamper (yes or no, active or inactive, 1 or 0) to occur within a certain max-timeout time window. If there are n or m (e.g. 10) consecutive tamper = 1 readings within the timeout window, the processor determines a real (debounced) tamper=1, which is processed accordingly.

[0061] If instead n (e.g. 10) consecutive consistent and/or same-tamper values of tamper=0 occur in the max-timeout window, then this may indicate a developing fault (code XX), because the method ran only due to the tamper having changed value. This may indicate that the tamper is becoming unstable somehow, although not completely unreliable. The filtering seems to be able to handle the instability, and identify a real (debounced) value that has reset to tamper=0. It could also happen if the tamper pin is manually pushed back in.

[0062] If the max-timeout window expires without having obtained n (e.g. 10) consecutive consistent and/or same-values in that window, then this may indicate a more significant fault (code YY) due to instability. The method ran only due to the tamper having changed value, and the filtering is unable to identify a real (debounced) value. The processor may be programmed to repeat the method so that it repeatedly sends the same error code, or it may be programmed to continue to monitor the situation but only to send error codes only occasionally or to report if the system improves.

[0063] The further method, referenced as 1020 in Figure 10, will now be described with reference to Figure 11.

[0064] The method 1100 may be applied in conjunction with the method 1000 illustrated in Figure 10, but may be applied instead of that earlier method. In the latter case, the method starts at 1102 with the tamper detection system in an idle state. If tamper violation is detected 1106 (optionally as the result of applying 1104 the method 1000), the processor determines 1108 whether signals from the accelerometer indicate any movement such as a change in orientation (which is indicative of manipulation of the peripheral device). The processor may consider all signals received from the accelerometer in a period overlapping with the occurrence of any signals received from the tamper detection arrangement: there may be time-stamping of received signals at the processor, the accelerometer may also time stamp signals that it sends, as may the tamper detection arrangement - although the processor itself may handle such timestamping.

[0065] The processor may be programmed to distinguish between the signatures of different types of movement - for example using a technique such as that described in the applicant's WO2019/238256 (the contents of which are hereby incorporated by reference), this may involve a trained neural network or some kind of machine learning (all relevant training may be done on pre-production devices or other suitable training devices, and a suitably trained neural network or other system may be loaded to devices prior to deployment). In particular, the processor may apply a classifier to distinguish between, on the one hand, patterns of vibration or movement that

characterise the passage of traffic, trains, aeroplanes, and on the other hand patterns of movement characteristic of manipulation of the device (which are likely to differ according to the device type and its place of installation). If the device is a door/window sensor, the processor is preferably programmed to recognise signals indicative of movement consistent with door or window opening, and also to recognise signals indicative of shock patterns characteristic of someone attempting to force open or to destroy a door or window. If the device is configured to operate as a shock sensor in its own right, high impact attacks will probably result in the device signalling an alarm event (to the controller of the security monitoring system, or to a remote monitoring station directly or indirectly). Sneaky or surreptitious attacks are more likely to be associated with attempts to tamper with the device, and hence the processor is preferably configured to react to receiving a tamper signal and certain accelerometer signals (indicative of stealthy or surreptitious attacks) by sending an alarm signal (which may be termed a tamper violation signal) at 1110. If the processor subsequently receives signals 1112 from the tamper detection arrangement that indicate that there is no longer a tamper condition, the processor send a "tamper restored" message 1114.

[0066] Conversely, if no relevant motion is reported by the accelerometer, the processor may be programmed to determine that any detected tamper violation is a false alarm, possibly as a result of the device coming loose and being able to move (possibly as the result of failure or weakening of an adhesive bond, or perhaps of failure or loosening of a retaining screw). In consequence, the processor at 1116 sends a fault report "tamper without movement" which may indicate failure of a glued attachment, but which is also indicative of the need for preventative maintenance. If the processor subsequently receives signals 1118 from the tamper detection arrangement that indicate that there is no longer a tamper condition, the processor send a "tamper restored" fault message 1120 which again suggest the need for a site inspection to perform preventative maintenance.

[0067] As mentioned previously, the inventors have realised that the failure of glued attachments may give rise to characteristic patterns of tamper faults. Hence it is useful for the processor to apply a classifier trained to recognise accelerometer signals indicative of failure modes of adhesive bonding - in particular gradual release/sag/slide of adhesive - the detection of which should lead to some kind of "tamper without movement" fault report. That is, depending upon the number of classes of movement the processor is able to distinguish, there may be more than one "tamper without movement" fault report.

[0068] In the present embodiment, tamper detection events can be validated by using another sensor 912 of the alarm peripheral, for example, an accelerometer. The sensor 912 may be dedicated to assisting validation of tamper detection, or it may have another function independent of tamper detection. In the latter case, the ability to use the sensor 912 also for tamper detection provides additional advantages using existing hardware components and/or without the cost of additional hardware components.

Claims

1. An alarm peripheral including a tamper detection arrangement, a processor of the peripheral being configured to:

   process a signal received from the tamper detection arrangement, to determine whether, after at least a first change in signal state, the signal meets predetermined stability criteria;
   determine whether a signal meeting the predetermined stability criteria corresponds to a tamper violation of the alarm peripheral; and
   cause transmission of a tamper violation signal in response to a determined tamper violation.

2. An alarm peripheral as claimed in claim 1, wherein the processor is programmed to signal a fault indicative of a need for preventative maintenance in the event that the signal meets the predetermined stability criteria and no tamper violation is determined.

3. An alarm peripheral as claimed in claim 1 or claim 2, wherein the processor is programmed to determine signal stability based on tamper state values of n of m consecutive signal samples, $m \geq n$, and optionally n is at least 5.

4. An alarm peripheral as claimed in claim 1 or claim 2, wherein the processor is programmed to determine signal stability based on tamper state values of n consecutive signal samples, $n>1$, within a predetermined time period, and optionally n is at least 5.

5. An alarm peripheral as claimed in any one of claims 2 to 4, wherein the processor is programmed to signal a fault in the event that the signal does not meet the predetermined stability criteria.

6. An alarm peripheral as claimed in any one of the preceding claims, further comprising an RF transmitter coupled to the processor, the processor being programmed to use the RF transceiver to transmit tamper violation and tamper fault signals to a corresponding RF receiver, and optionally
   wherein the RF transmitter includes a transmitter configured to operate on a low power wide area cellular network such as LTE Cat M and NB IoT.

7. A security monitoring installation at premises protected by the installation, the installation comprising

a controller and a plurality of alarm peripherals configured to transmit event notifications to the controller, the controller being configured to report alarm events to a monitoring station remote from the premises, wherein at least one of the alarm peripherals is as claimed in any one of the preceding claims, the controller having at least one operating mode in which it is programmed to report detected tamper events to the monitoring station.

8. A security monitoring installation at premises protected by the installation, the installation comprising a plurality of alarm peripherals configured to transmit event notifications to a monitoring station remote from the premises, wherein at least one of the alarm peripherals is as claimed in any one of claims 1 to 6, said at least one alarm peripheral being programmed to report detected tamper events to the monitoring station.

9. A security monitoring installation at premises protected by the installation, the installation comprising a controller and a plurality of alarm peripherals each including a tamper detection arrangement each configured to transmit event notifications to the controller, the controller being configured to report alarm events to a monitoring station remote from the premises, the controller having at least one operating mode in which it is programmed to:

process a signal received from the tamper detection arrangement, to determine whether, after at least a first change in signal state, the signal meets predetermined stability criteria;
determine whether a signal meeting the predetermined stability criteria corresponds to a tamper violation of the alarm peripheral; and
cause transmission of a tamper violation signal in response to a determined tamper violation.

10. A security monitoring installation as claimed in claim 9, wherein the controller has at least one operating mode in which it is programmed to:

process signals received from the tamper detection arrangement of one of the alarm peripherals and to discriminate between genuine tamper events and erroneous tamper events;
generate a tamper fault signal in the event of detecting an erroneous tamper event; and
report the tamper fault signal to the monitoring station remote from the premises.

11. A security monitoring installation as claimed in claim 10, wherein the controller is programmed to signal a fault indicative of a need for preventative maintenance in the event that the signal meets the predetermined stability criteria and no tamper violation is determined.

12. A security monitoring installation as claimed in claim 10 or claim 11, wherein the controller is programmed to signal a fault in the event that the signal does not meet the predetermined stability criteria.

13. A system that comprises a security monitoring installation at premises protected by the installation and a monitoring station remote from the premises, the security monitoring installation having a controller and a plurality of alarm peripherals configured to transmit event notifications to the controller, the controller being configured to report alarm events to the monitoring station, wherein at least one of the alarm peripherals is as claimed in any one of claims 1 to 6, the controller having at least one operating mode in which it is programmed to report detected tamper events to the monitoring station.

14. A system that comprises a security monitoring installation at premises protected by the installation and a monitoring station remote from the premises, the security monitoring installation having a plurality of alarm peripherals configured to transmit event notifications to the monitoring station, wherein at least one of the alarm peripherals is as claimed in any one of claims 1 to 6, said at least one alarm peripheral being programmed to report detected tamper events to the monitoring station.

15. A method of handling tamper signals from a tamper detecting device, the method comprising:

processing a signal received from a tamper detection arrangement of the device, to determine whether, after at least a first change in signal state, the signal meets predetermined stability criteria;
determining whether a signal meeting the predetermined stability criteria corresponds to a tamper violation of the alarm peripheral; and
causing transmission of a tamper violation signal in response to a determined tamper violation.

16. A method as claimed in claim 15, the method comprising determining signal stability based on tamper state values of n of m consecutive signal samples, $m \geq n$, and optionally n is at least 5.

17. A method as claimed in claim 15, the method comprising determining signal stability based on tamper state values of n consecutive signal samples, $n>1$, within a predetermined time period, and optionally n is at least 5.

18. A method as claimed in any one of claims 15 to 17,

the method further comprising signalling a fault indicative of a need for preventative maintenance in the event that the signal meets the predetermined stability criteria and no tamper violation is determined.

19. A method as claimed in any one of claims 15 to 18, the method further comprising signalling a fault in the event that the signal does not meet the predetermined stability criteria.

20. A method as claimed in any one of claims 15 to 19, wherein the processing is performed by a processor of a control unit of the premises security monitoring system, the peripheral being communicatively coupled to the control unit.

21. A method as claimed in any one of claims 15 to 20, wherein the processing is performed at a monitoring station remote from the premises, the peripheral being communicatively coupled to the remote monitoring station.

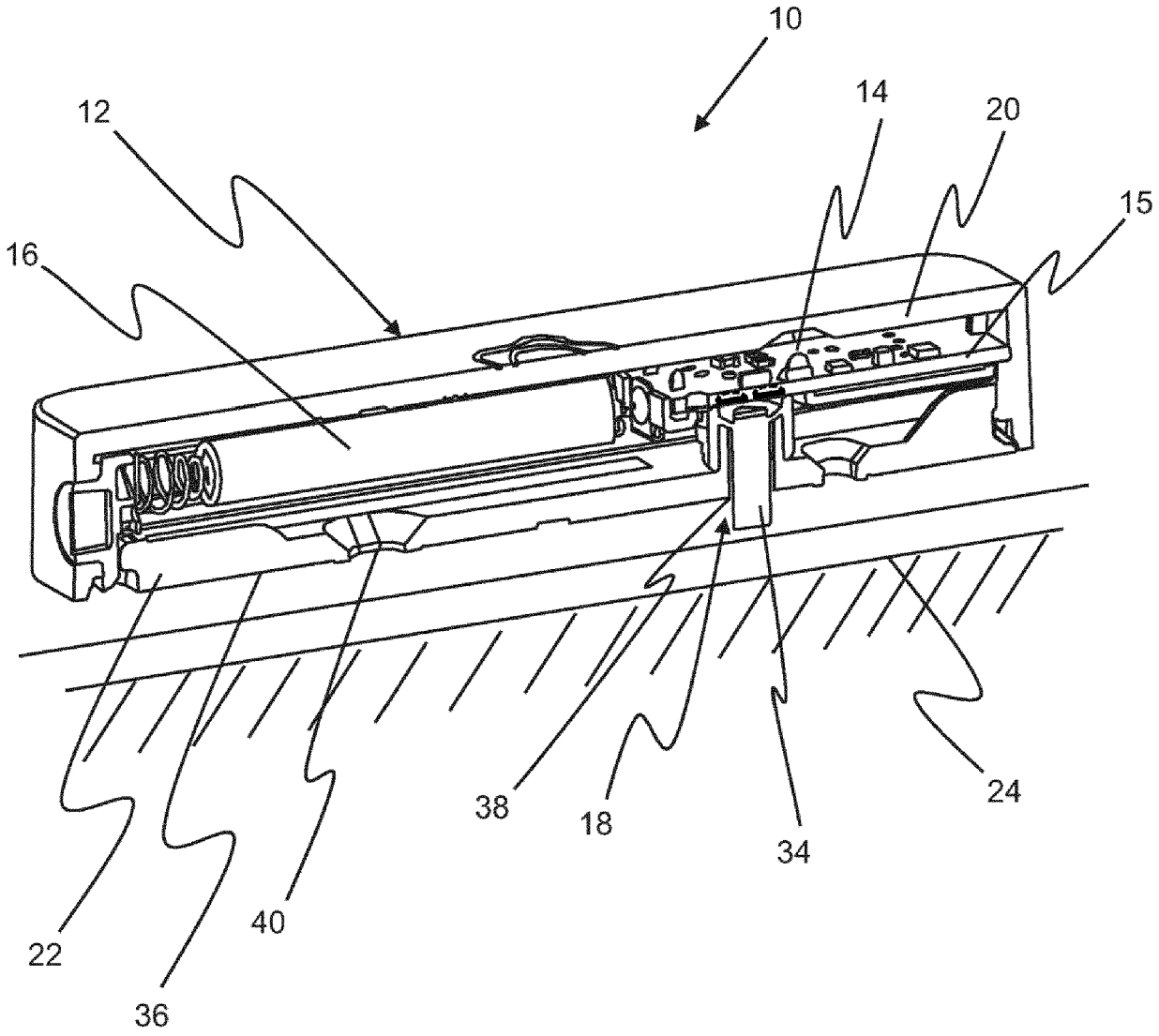

Fig. 1

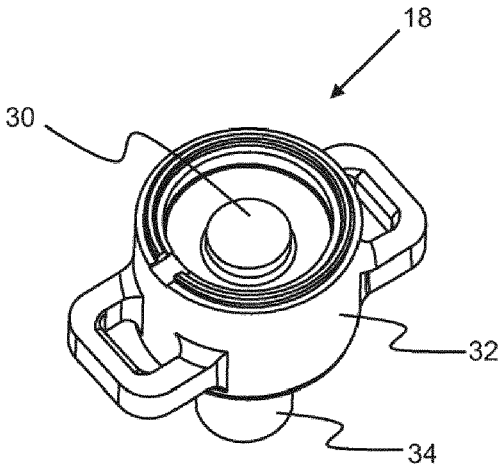

Fig. 2

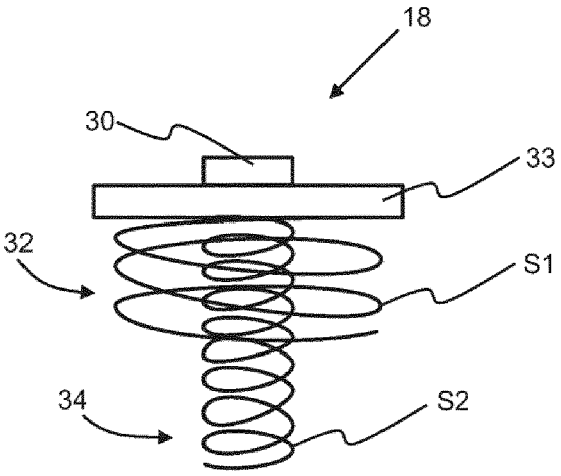

Fig. 2A

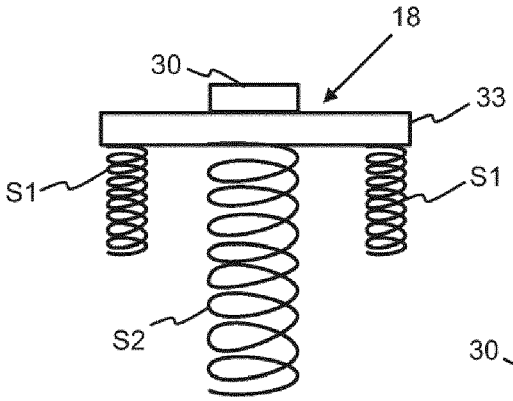

Fig. 2B

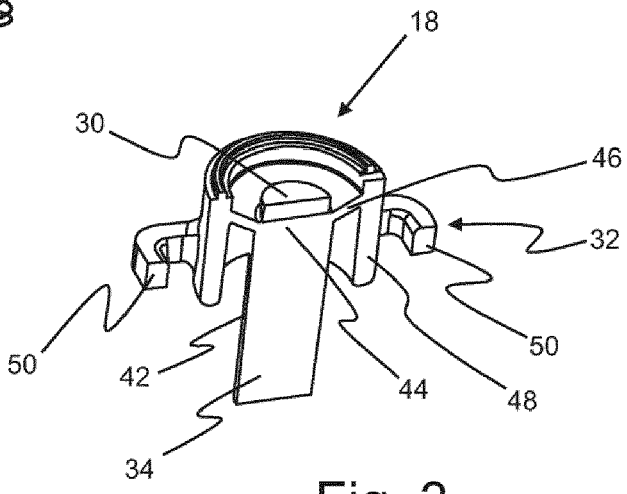

Fig. 3

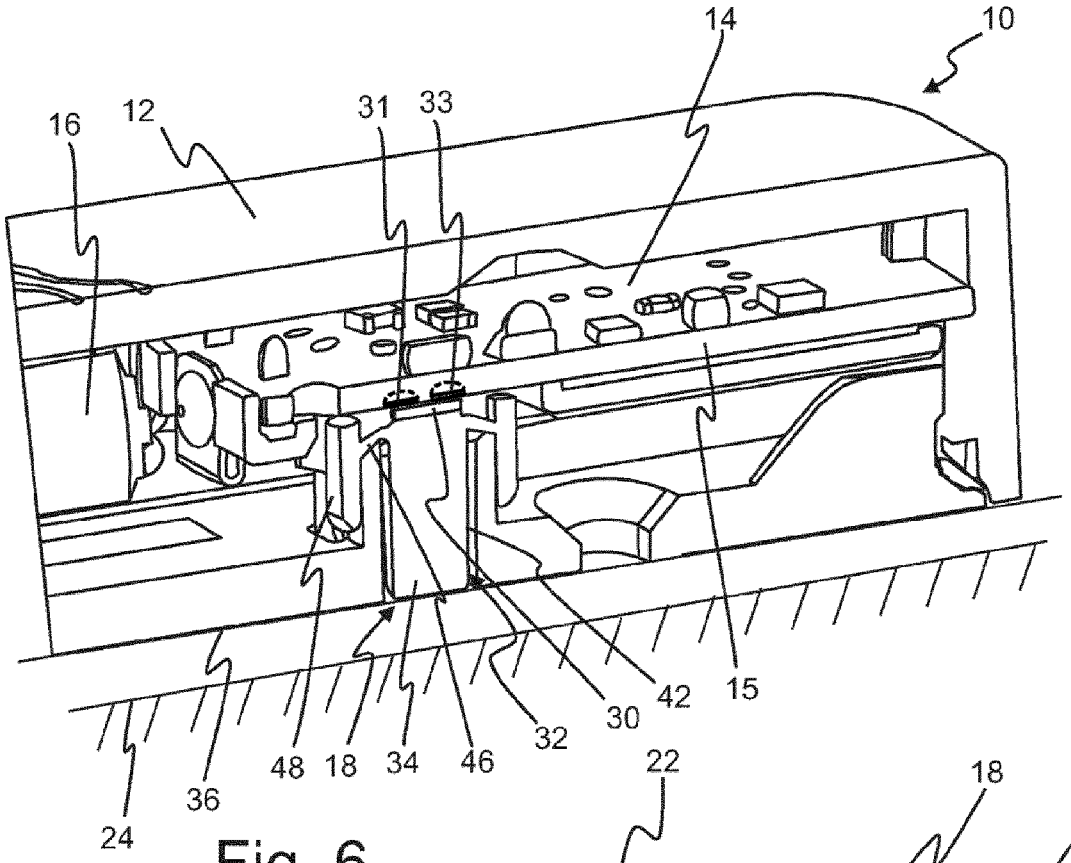

Fig. 6

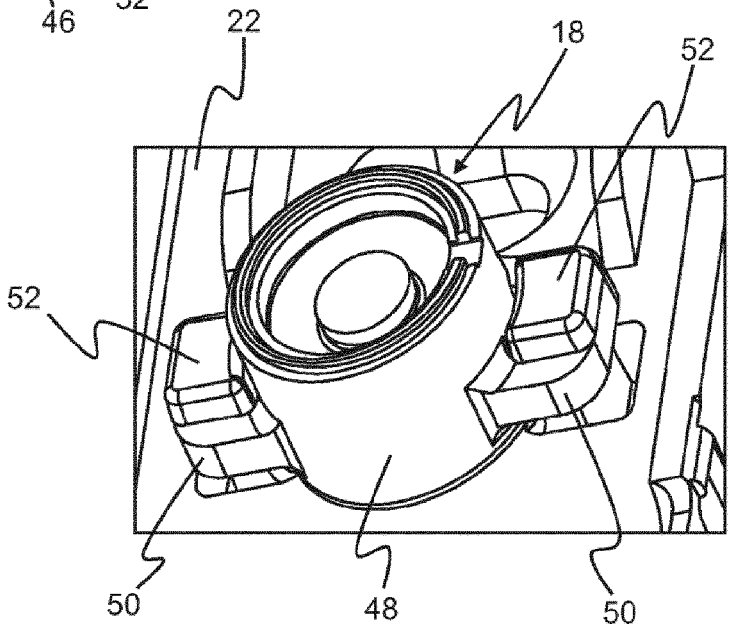

Fig. 5

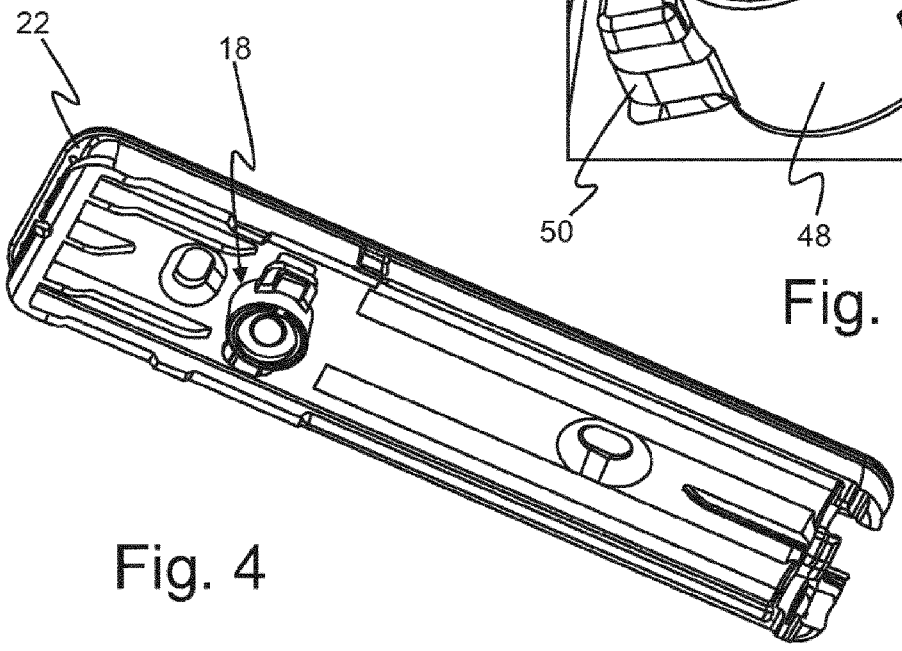

Fig. 4

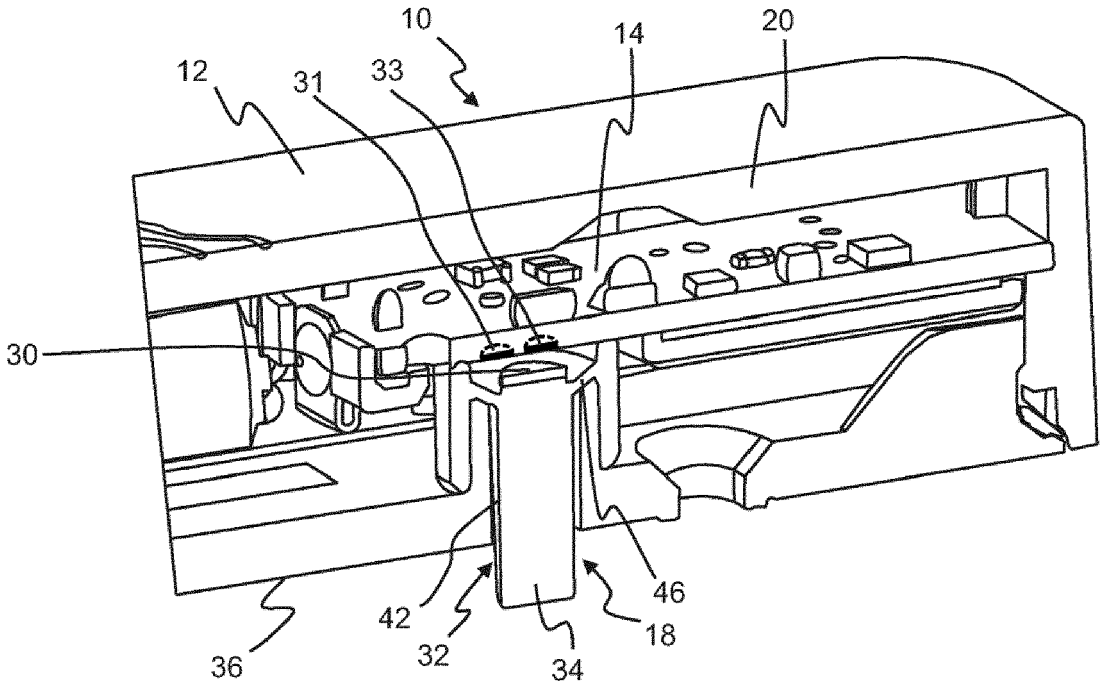

Fig. 7

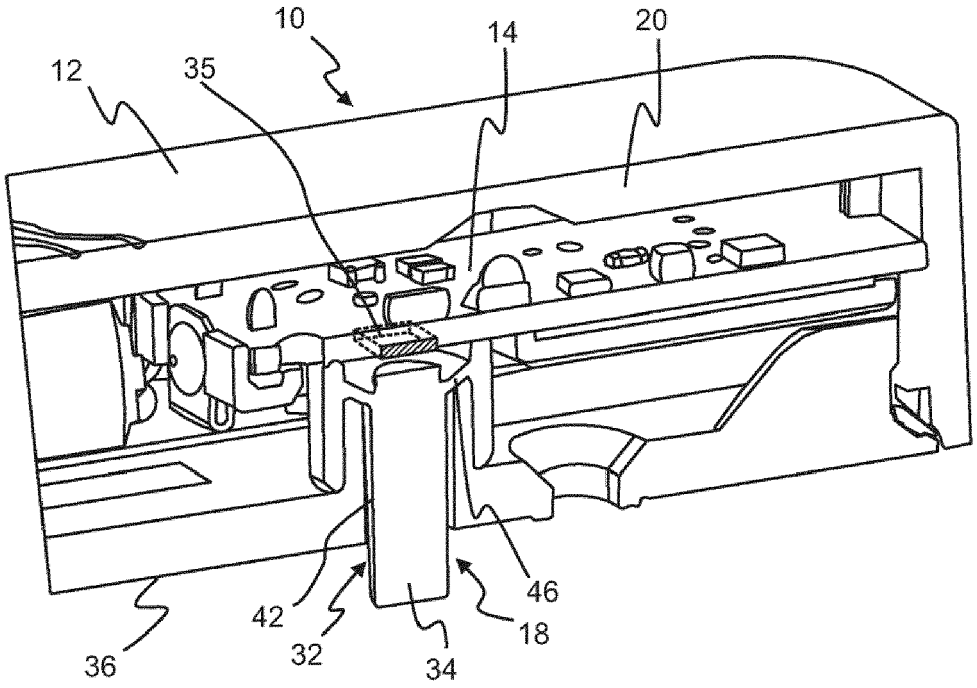

Fig. 8

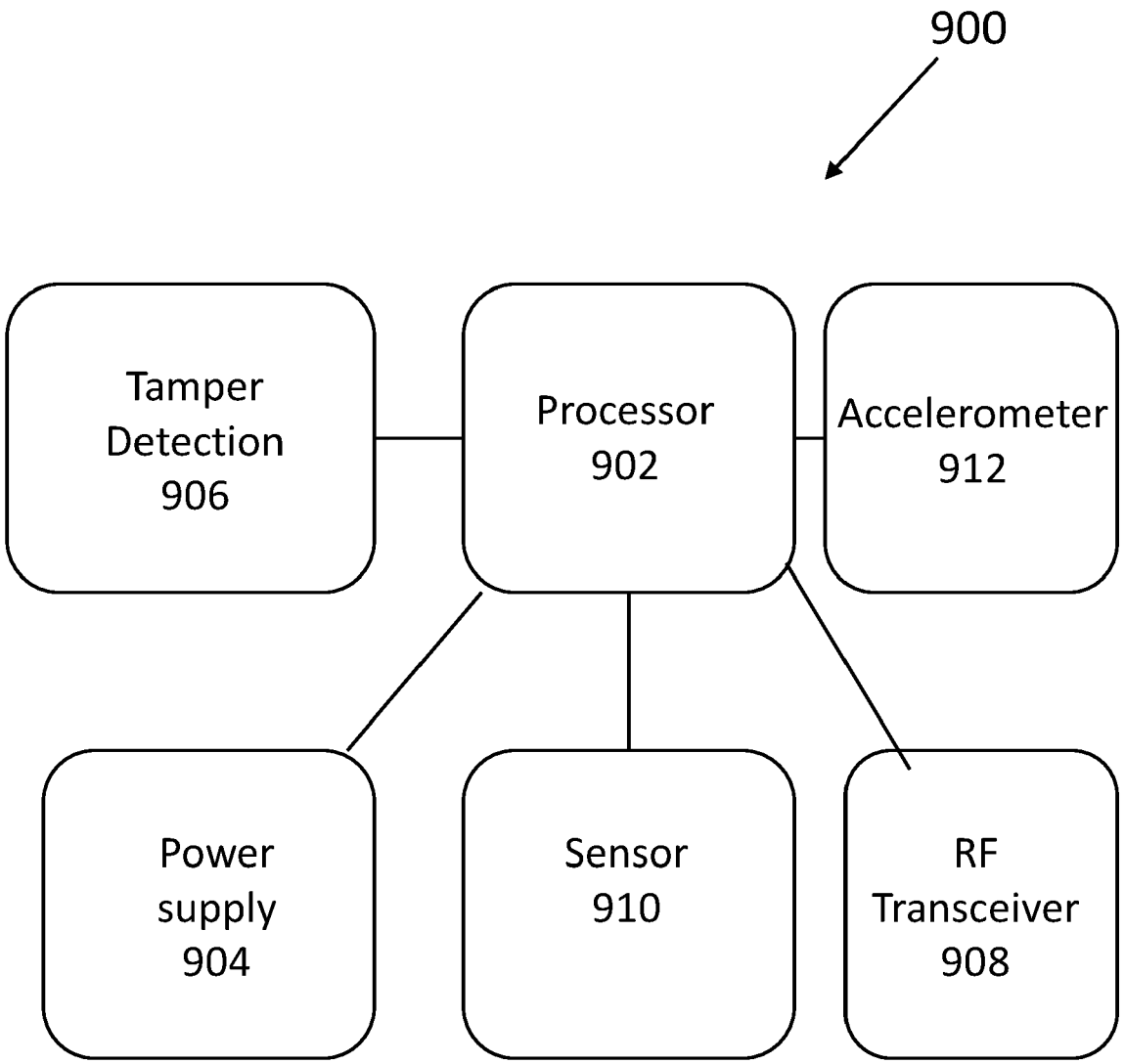
900
Tamper Detection 906
Processor 902
Accelerometer 912
Power supply 904
Sensor 910
RF Transceiver 908

Fig. 9

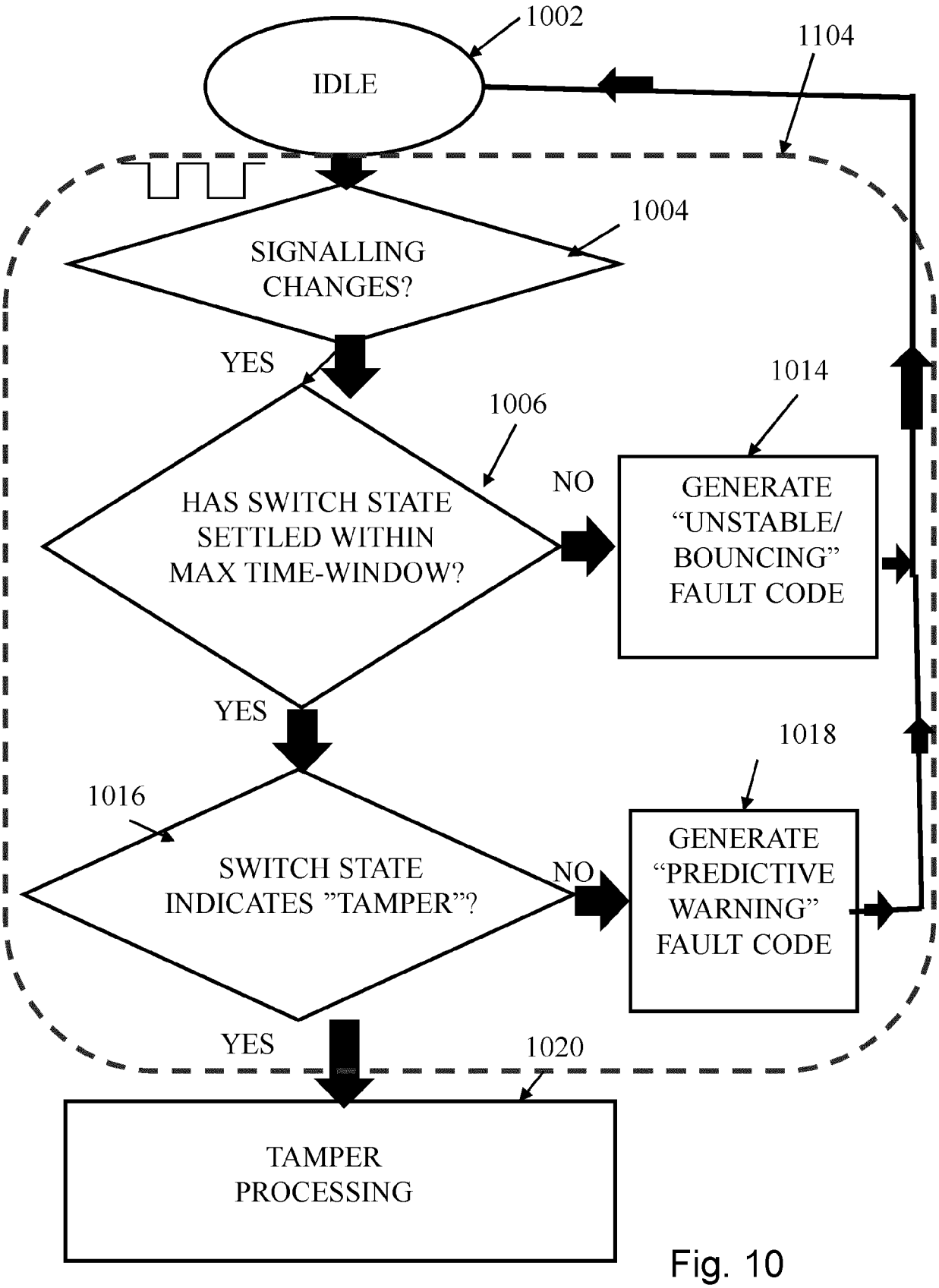
1002
IDLE
1104
1004
SIGNALLING CHANGES?
YES
1006
HAS SWITCH STATE SETTLED WITHIN MAX TIME-WINDOW?
NO
1014
GENERATE "UNSTABLE/ BOUNCING" FAULT CODE
YES
1016
SWITCH STATE INDICATES "TAMPER"?
NO
1018
GENERATE "PREDICTIVE WARNING" FAULT CODE
YES
1020
TAMPER PROCESSING

Fig. 10

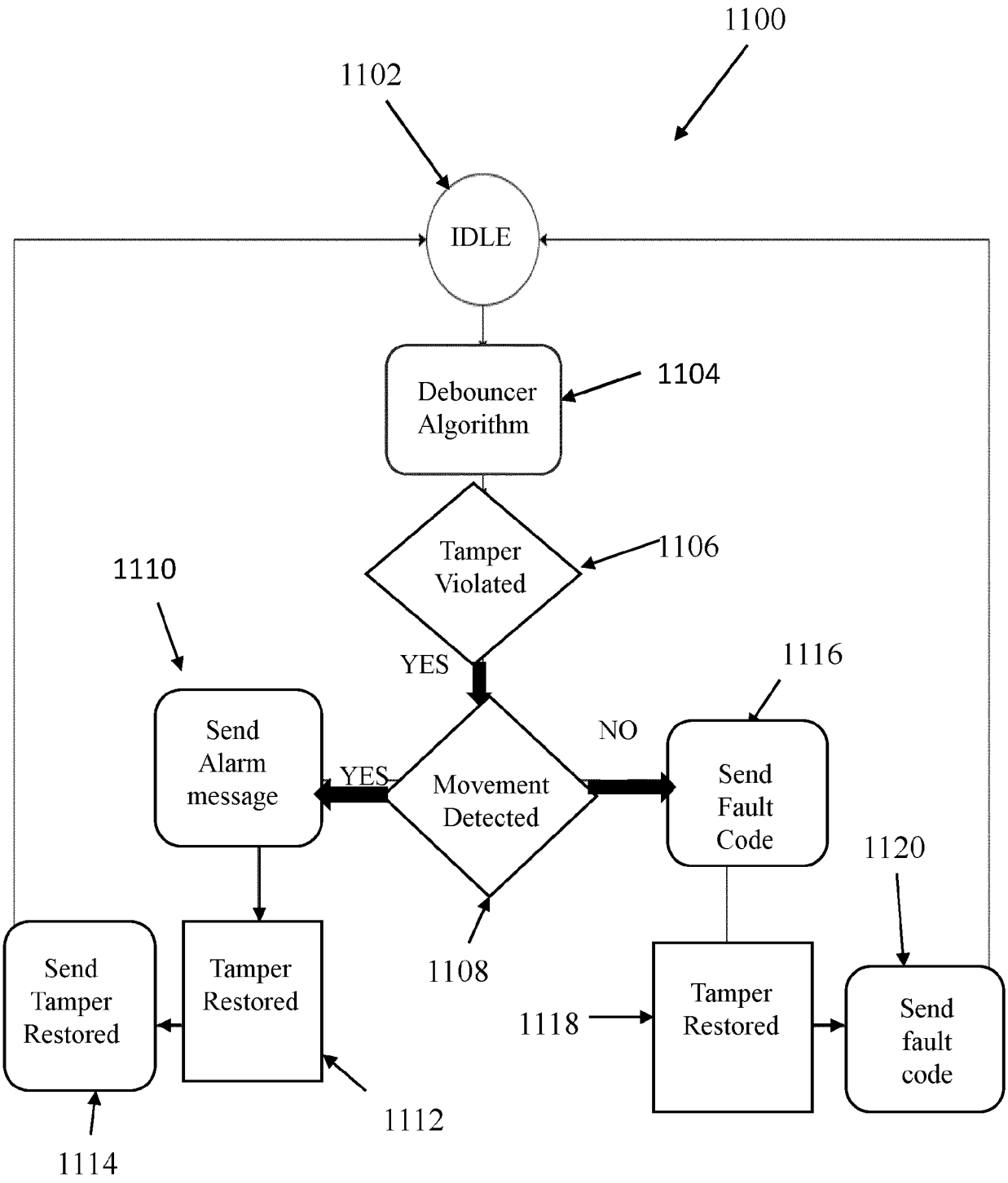
1100
1102
IDLE
Debouncer Algorithm
1104
Tamper Violated
1106
1110
YES
1116
Send Alarm message
YES
Movement Detected
NO
Send Fault Code
1120
1108
Send Tamper Restored
Tamper Restored
1118
Tamper Restored
Send fault code
1112
1114

Fig. 11

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 38 2828

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	EP 3 923 257 A1 (ESSENCE SECURITY INT E S I LTD [IL]) 15 December 2021 (2021-12-15) * abstract * * column 0008 - column 0009 * * column 0012 - column 0018 * * paragraph [0087] - paragraph [0097]; figure 2 * * paragraph [0101] - paragraph [0105]; figure 3 * * paragraph [0126] - paragraph [0177]; figures 7A,7B * * paragraph [0215] - paragraph [0225]; figure 9 *	1-21	INV. G08B29/04 G08B13/00
A,D	WO 2019/115505 A1 (VERISURE SARL [CH]) 20 June 2019 (2019-06-20) * abstract *	1,9,15	

TECHNICAL FIELDS SEARCHED (IPC)

G08B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	12 January 2024	Heß, Rüdiger

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)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 23 38 2828

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.

12-01-2024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 3923257 A1	15-12-2021	NONE	
WO 2019115505 A1	20-06-2019	EP 3499479 A1	19-06-2019
		ES 2875477 T3	10-11-2021
		PT 3499479 T	18-06-2021
		WO 2019115505 A1	20-06-2019

EPO FORM P0459

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

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- WO 2019115505 A1 **[0007]**
- WO 2019115505 A **[0040]**
- WO 2019238256 A **[0065]**