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

(11) **EP 3 644 210 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
30.11.2022 Bulletin 2022/48

(21) Application number: **19205466.6**

(22) Date of filing: **25.10.2019**

(51) International Patent Classification (IPC):
G06F 21/86 *(2013.01)*

(52) Cooperative Patent Classification (CPC):
G06F 21/86; G06F 2221/2143

(54) TAMPER DETECTION AND RESPONSE DEACTIVATION TECHNIQUE

MANIPULATIONSDETEKTIONS- UND -REAKTIONSDEAKTIVIERUNGSTECHNIK

DÉTECTION DE FRAUDES ET TECHNIQUE DE DÉSACTIVATION DE RÉPONSES

(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

(30) Priority: **26.10.2018 US 201816172320**

(43) Date of publication of application:
29.04.2020 Bulletin 2020/18

(60) Divisional application:
21203379.9 / 3 961 466

(73) Proprietor: **Hamilton Sundstrand Corporation**
Charlotte, NC 28217-4578 (US)

(72) Inventors:
- **LILLESTOLEN, Kirk A.**
  East Hartland, CT Connecticut 06027 (US)
- **VILLANO, William E.**
  Canton, CT Connecticut 06019 (US)

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

(56) References cited:
US-A1- 2017 116 440
US-A1- 2017 354 027
US-A1- 2018 032 761

EP 3 644 210 B1

Description

BACKGROUND

[0001] The present disclosure relates to tamper detection systems, and more particularly, to a self-powering tamper detection and response system architecture for electronic circuitry.

[0002] The protection of critical information contained on printed circuit boards from unwanted access is necessary to ensure the integrity of components and systems in which those circuits can reside. For example, sensitive program data that can be stored in circuitry must not be accessed by unauthorized persons, competitors, or adversaries. In some situations, the unauthorized tampering of program data can affect the proper functioning of a component. In other situations, the unauthorized access of program data can pose a risk to competitive advantage and/or national security. Multiple levels of security can often be used to prevent the unauthorized access to program data, but as a final measure of security, an electronic component may have a means of detecting when unauthorized tampering is occurring. When a tampering event is triggered, an electronic component is instructed to erase or disrupt the stored program data so that the data cannot be accessed by an unauthorized party.

[0003] Several anti-tamper systems have been developed to achieve the goal of detecting and responding to a tampering event. For example, U.S. Patent No. 9,798,902, to Ludlow, discloses anti-tamper sensors involving transducers. Tamper detection systems involving transducers are known in the art, whereby a transducer utilizes the conversion of one form of energy into another to achieve a response. For example, U.S. Patent No. 8,499,173, to Caci, discloses a light emitter, a light receiver, and a reflector for detecting tampering on a circuit board. Tamper detections have also been developed to detect tampering on consumer electronics products, which can be useful for products that are under a manufacturer's warranty. For example, U.S. Patent No. 8,736,286, to Johnson, discloses a means of detecting consumer abuse without having to rely upon the explanatory statements of the user who may be returning a unit that is no longer working according to the original specification of the manufacturer. The tamper systems disclosed in documents US 2017/116440 and US 2017/354027 also form part of the background art.

SUMMARY

[0004] A self-powering tamper detection system architecture is provided as defined by claim 1.

[0005] A method of suppressing a tamper response in a self-powering tamper system architecture is provided as defined by claim 7.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006]

FIG. 1 is a block diagram of a tamper system of the prior art.
FIG. 2 is a block diagram of a self-powering tamper system.
FIG. 3A is a side view of an embodiment of a tamper detection embedded transformer.
FIG. 3B is a top view of an embodiment of a tamper detection embedded transformer.
FIG. 4A is a side view of a second embodiment of a tamper detection embedded transformer.
FIG. 4B is a top view of a second embodiment of a tamper detection embedded transformer.
FIG. 5A is a side view of a third embodiment of a tamper detection embedded transformer.
FIG. 5B is a top view of a third embodiment of a tamper detection embedded transformer.
FIG. 6A is a schematic diagram of the embedded transformer of FIG. 3A in a normal equipment configuration.
FIG. 6B is a schematic diagram of the embedded transformer of FIG. 3A in an abnormal equipment configuration.
FIG. 7 is a block diagram of an embodiment of a tamper system utilizing the embedded transformer of FIG. 3A.
FIG. 8 is an exemplary electrical schematic diagram of the tamper system of FIG. 5.
FIG. 9A is an electrical schematic diagram of an embodiment of a tamper switch.
FIG. 9B is an electrical schematic diagram of a second embodiment of a tamper switch.
FIG. 10A is a perspective view of an embodiment of the tamper switch.
FIG. 10B is a perspective view of a second embodiment of the tamper switch.
FIG. 10C is a perspective view of a third embodiment of the tamper switch.
FIG. 10D is a perspective view of a fourth embodiment of the tamper switch.
FIG. 11 is side view of an embodiment of the tamper switch in the self-powering tamper detection and response system.
FIG. 12 is an electrical block diagram showing the tamper switch in the self-powering tamper detection and response system.
FIG. 13 is an electrical schematic diagram of an embodiment of the tamper deactivation circuit.
FIG. 14 is an electrical block diagram of a second embodiment of the tamper deactivation circuit.

DETAILED DESCRIPTION

[0007] FIG. 1 is a block diagram of a representative tamper system architecture of the prior art. Shown in FIG.

1 are tamper system architecture 10, power source 12, tamper detection transducer 14, tamper switch 16, tamper controller 18, and program memory 20. Power source 12 can be a power supply, such as a power supply that powers the equipment (not shown) in which tamper system architecture 10 resides. During operation, tamper detection transducer 14 monitors for a tampering condition. In a particular embodiment, tamper detection transducer 14 can be a piezoelectric transducer, which transforms a pressure force from tampering into an electrical signal to represent tampering. In another particular embodiment, tamper detection transducer 14 can be an optical transmitter and optical receiver that convert electrical energy into optical energy, and optical energy into electrical energy, respectively. Accordingly, a change in the optical transmission path could be representative of a tamper condition. When a tamper event occurs, tamper switch 16 receives a tamper signal from tamper detection transducer 14 and provides a signal to tamper controller 18 representative of the tamper event. Tamper controller 18 can also be referred to as a tamper logic and controller circuit. Tamper controller 18 evaluates one or more signals received from tamper switch 16 to evaluate the tamper condition and determine the tamper response. If tamper controller 18 determines that the tamper event warrants destruction of stored program data, tamper controller 18 provides instructions to program memory 20 that disrupt and/or erase the stored program data from program memory 20 thereby preventing the unauthorized access to stored program data.

[0008] FIG. 2 is a block diagram of the self-powering tamper system architecture of the present disclosure. Shown in FIG. 2 are tamper system architecture 100, power source 112, tamper detector 114, tamper switch 116, tamper controller 118, program memory 120, and tamper system 130. In the illustrated embodiment, power source 112 is a long-life source of electrical power that is available for a prolonged duration of time. In an embodiment, power source 112 can be a lithium battery that stores usable energy for 5 - 20 years. In another embodiment, power source 112 can be a super-capacitor that stores usable energy for 2 - 10 months. Super-capacitors can be available under various trademarks (e.g., CAP-ATTERY™ capacitor manufactured by Evans Capacitor Company). In some embodiments, power source 112 receives a charging voltage from another power supply (not shown) during operation of the equipment (not shown) in which tamper system architecture 100 resides, and then power source 112 remains charged for 2 - 10 years following the shutdown of the equipment. In other embodiments, power source 112 can be a long-life energy cell that stores electrical energy for an indefinite duration of time. In some embodiments, power source 112 can store energy for more than 20 years. In other embodiments, power source 112 can store energy for more than 50 years. It can be beneficial for power source 112 to store energy for a duration of time that is equivalent to the expected service life of the equipment in which tamper system architecture 100 resides. Tamper system architecture 100 can also be referred to as a tamper detection system architecture.

[0009] Referring again to FIG. 2, tamper detector 114 is a transducerless device that can be actuated when a tampering event occurs. The present disclosure is predicated on the storing of program data in program memory 120 which is contained within a physical enclosure (not shown). Therefore, tamper detector 114 senses a tampering event as a result of the actuation of at least one component of the physical enclosure. Specific embodiments of the tamper detector will be described in FIGS. 3A - 3B, 8A - 8D, and 9. During a tampering event, tamper detector 114 actuates tamper switch 116, thereby causing electrical power to be delivered from power source 112 via tamper switch 116 to tamper controller 118. Tamper switch 116 can be a mechanical, electromechanical, or electronic switch. Together, tamper detector 114 and tamper switch 116 can be referred to as tamper system 130.

[0010] In the illustrated embodiment, tamper detector 114 also provides a tamper signal directly to tamper controller 118 when a tamper event occurs. Tamper controller 118 can also be referred to as a tamper logic and controller circuit. Tamper controller 118 evaluates one or more signals received from tamper switch 116 and/or tamper detector 114 to evaluate the tamper condition and determine the tamper response. If tamper controller 118 determines that the tamper event warrants destruction of stored program data, tamper controller 118 provides instructions to program memory 120 that disrupt and/or erase the stored program data from program memory 120 thereby preventing the unauthorized access to stored program data. In some embodiments, program memory 120 can be non-transitory machine-readable media including without limitation a field-programmable gate array (FPGA), flash memory, random access memory (RAM), programmable read-only memory (PROM), and erasable programmable read-only memory (EPROM). In some of these embodiments, program memory 120 can utilize semiconductor, magnetic, optical, electrostatic, and/or atomic storage. All forms of data storage on program memory 120 are within the scope of the present disclosure.

[0011] FIG. 3A is a side view of an embodiment of a tamper system 130 that utilizes an embedded transformer, and FIG. 3B is a top view of the tamper detection embedded transformer. Shown in FIGS. 3A - 3B are chassis 250, chassis cover 252, printed circuit board 254, aperture 255, chassis strut 258, cover screw 260, shaft 262, embedded transformer 264, primary winding 266, first secondary winding 268, and second secondary winding 270. Chassis 250 encloses program memory 120 in which program data are stored. During normal operation chassis cover 252 is in place as shown in FIG. 3A, providing a physical boundary preventing access to various electronic circuitry that includes program memory 120. In the illustrated embodiment, cover screw 260 secures

chassis cover 252 to chassis 250, thereby preventing chassis cover 252 from being removed. For an unauthorized person to gain access to program memory 120, cover screw 260 must first be removed. Cover screw 260 includes shaft 262 which is held in place by chassis strut 258, thereby securing chassis cover 252 to chassis 250. Chassis strut 258 also holds printed circuit board 254 in place. Printed circuit board 254 is a multilayer printed circuit board (PCB). Multilayer PCBs are known to those who are skilled in the electronics arts as being useful in providing dense circuit architecture, for example, those that utilize integrated circuit chips. Multilayer PCBs have one or more embedded layers containing circuit traces in addition to top and/or bottom surface circuit traces. Printed circuit board 254 includes aperture 255, through which shaft 262 can pass. Accordingly, primary winding 266, first secondary winding 268, and second secondary winding 270 each encircle aperture 255. In the illustrated embodiment, chassis strut 258 is a non-ferromagnetic material and shaft 262 is a ferromagnetic material.

[0012] First secondary (S1) winding 268 and second secondary (S2) winding 270 are connected in series, which can have one or more beneficial effects. This increases the voltage amplitude at the combined secondary output of embedded transformer 264, and it can also assist in providing common mode noise rejection. In other embodiments, first secondary (S1) winding 268 and second secondary (S2) winding 270 can be connected in other configurations. Moreover, in some embodiments, first secondary (S1) winding 268 and/or second secondary (S2) winding 270 can include more than one turn. An advantage to a multi-turn first secondary (S1) winding 268 and/or second secondary (S2) winding 270 can be to provide an output voltage having a greater amplitude than is provided by a single turn. In some of these embodiments, embedded transformer 264 can include secondary winding(s) formed on multiple layers of printed circuit board 254. For example, one or more loops can be formed on the top and/or bottom surfaces of printed circuit board 254. In other embodiments, first secondary (S1) winding 268 and/or second secondary (S2) winding 270 can include a multi-loop planar circuit trace formed as a spiral and/or by connected concentric circular traces. In yet other embodiments, second secondary winding 270 can be omitted and embedded transformer 264 can include only primary winding 266 and first secondary winding 268. In these other embodiments, first secondary winding 268 can be called the secondary winding, and the secondary winding can have one or more turns. For example, in some of these other embodiments, the secondary winding can have multiple turns that are formed on a single layer of printed circuit board 254.

[0013] Referring again to FIGS. 3A - 3B, printed circuit board 254 contains embedded transformer 264, which is an electrical transformer that includes primary (P) winding 266, first secondary (S1) winding 268, and second secondary (S2) winding 270. In the illustrated embodiment, primary winding 266, first secondary winding 268, and second secondary winding 270 are each a circuit trace on different layers of printed circuit board 254 in close proximity to each other, encircling aperture 255. Primary winding 266, first secondary winding 268, and second secondary winding 270 are each approximately circular and are stacked vertically with respect to the axis of chassis strut 258, each having two connection terminals as shown in FIG. 3B. Accordingly, in some embodiments, primary winding 266, first secondary winding 268, and second secondary winding 270 are each approximately one loop, thereby each having a single turn of wire, with "turns" being used to characterize the windings of electrical transformers.

[0014] It is to be appreciated that primary winding 266, first secondary winding 268, and second secondary winding 270 are connected to associated components by wires and/or conductive traces on printed circuit board 254, and that interlayer conductors (i.e., "vias") are used to provide electrical connections to embedded layers (including primary winding 266, first secondary winding 268, and second secondary winding 270) on printed circuit board 254. The associated methods for interconnecting the various layers and components on printed circuit boards are known to those in the electrical arts. Accordingly, the supporting traces and vias are not shown on printed circuit board 254 in FIGS. 3A - 3B for illustration clarity. In the illustrated embodiment, primary winding 266, first secondary winding 268, and second secondary winding 270 each are about 0.9 turns as a result of the via connectors (not labeled). In other embodiments, primary winding 266, first secondary winding 268, and second secondary winding 270 can each form at least 0.75 turns. In some embodiments, particularly where printed circuit board 254 has more than three layers of circuit traces, it can be beneficial for primary winding 266, first secondary winding 268, and second secondary winding 270 to be located on three adjacent layers which can help maximize the magnetic flux coupling between primary winding 266, first secondary winding 268, and second secondary winding 270. As used in this disclosure, "magnetic flux coupling" can be referred to a "magnetic coupling" with regard to the transformer action between primary winding 266, first secondary winding 268, and second secondary winding 270.

[0015] FIG. 4A is a side view of a second embodiment of a tamper detection embedded transformer, and FIG. 4B is a top view of a second embodiment of a tamper detection embedded transformer. The features shown in FIGS. 4A - 4B follow the same numbering as those described above with respect to FIGS. 3A - 3B, with the addition of the letter "A" following each number. The description of FIGS. 4A - 4B is similar to that provided above with respect to FIGS. 3A - 3B, with the following exceptions. Primary winding 266A, first secondary winding 268A, and second secondary winding 270A do not surround chassis strut 258A (as shown in FIG. 4A). Instead, embedded transformer 264A in printed circuit board 254A is vertically aligned with chassis strut 258A and

adjacent to shaft 262A as shown in FIG. 4A. In the illustrated embodiment, magnetic flux coupling between primary winding 266, first secondary winding 268, and second secondary winding 270, when in the vicinity of shaft 262A, is greater than in an equivalent configuration shown in FIGS. 3A - 3B. Accordingly, in the illustrated embodiment, the induced voltages in first secondary winding 268A and/or second secondary winding 270A, when in the vicinity of shaft 262A, is greater than in an equivalent configuration shown in FIG. 3A.

[0016] FIG. 5A is a side view of a third embodiment of a tamper detection embedded transformer, and FIG. 5B is a top view of a third embodiment of a tamper detection embedded transformer. The features shown in FIGS. 5A - 5B follow the same numbering as those described above with respect to FIGS. 3A - 3B, with the addition of the letter "B" following each number. The description of FIGS. 5A - 5B is similar to that provided above with respect to FIGS. 4A - 4B, with the following exceptions. A first ring 256B is directly above embedded transformer 264B and axially aligned with chassis strut 258B, with respect to the orientation shown in FIG. 5A. Similarly, a second ring 256B is directly below embedded transformer 264B and axially aligned with chassis strut 258B, with respect to the orientation shown in FIG. 5A. In the illustrated embodiment, rings 256B are ferromagnetic material and therefore assist in providing magnetic flux coupling between primary winding 266, first secondary winding 268, and second secondary winding 270 when shaft 262B is in position in embedded transformer 264B, as shown in FIG. 5A. Accordingly, in the illustrated embodiment, the induced voltages in first secondary winding 268B and/or second secondary winding 270B, when in the vicinity of shaft 262B, is greater than in an equivalent configuration shown in FIGS. 4A. An electrical schematic diagram (not shown) for embedded transformer 264 could depict a variably-coupled transformer depending on the axial position on shaft 262B.

[0017] FIG. 6A is a schematic diagram of embedded transformer 264 shown in FIG. 3A when cover screw 260 is installed to hold chassis cover 252 in place on chassis 250. FIG. 6B is a schematic diagram of embedded transformer 264' when cover screw 260 is removed. Shown in FIGS. 6A - 6B are shaft 262, embedded transformer 264, primary winding 266, first secondary winding 268, and second secondary winding 270. It is to be appreciated that a standard schematic symbol for a transformer is shown in FIGS. 6A - 6B, despite primary winding 266, first secondary winding 268, and second secondary winding 270 each being a single conductive loop. Moreover, the schematic symbol shown in FIG. 6B depicts as air core transformer when shaft 262 is removed because chassis strut 258 is non-ferromagnetic in the illustrated embodiment. In other embodiments, ferromagnetic materials other than shaft 262 can be located near embedded transformer 264. Referring again to FIG. 6A, shaft 262 acts as the ferromagnetic core of embedded transformer 264, assisting in magnetic flux coupling (i.e., magnetic coupling) between primary winding 266, first secondary winding 268, and second secondary winding 270.

[0018] During the operation of embedded transformer 264, an alternating voltage (i.e., time-varying voltage from an alternating current waveform) is applied across the terminals of primary winding 266, thereby inducing a voltage in each of first secondary winding 268 and second secondary winding 270 by magnetic flux coupling between primary winding 266, first secondary winding 268, and second secondary winding 270 as a result of shaft 262 forming the mutual inductive coupling as a result of the ferromagnetic nature of shaft 262. In other words, shaft 262 is the ferromagnetic core of embedded transformer 264. Accordingly, if shaft 262 is removed from embedded transformer 264 as a result of removing cover screw 260, the magnetic flux coupling between primary winding 266, first secondary winding 268, and second secondary winding 270 will be reduced. Therefore, the voltage induced in first secondary winding 268 and second secondary winding 270 in response to a time-varying alternating voltage applied across the terminals of primary winding 266 will be reduced. FIG. 6B represents the equivalent schematic diagram of embedded transformer 264' when cover screw 260 is removed, in which the magnetic flux coupling between primary winding 266, first secondary winding 268, and second secondary winding 270 is significantly reduced. Accordingly, the voltage induced in first secondary winding 268 and second secondary winding 270 in response to a time-varying alternating voltage applied across the terminals of primary winding 266 will be significantly reduced. In some embodiments, there can be no discernable voltage induced in first secondary winding 268 and/or second secondary winding 270.

[0019] FIG. 7 is a block diagram of an embodiment of the tamper system utilizing the embedded transformer of FIG. 3A. Shown in FIG. 7 are tamper system 230, oscillator driver 232, signal conditioner 234, decoder 236, timer 238, and embedded transformer 264. FIG. 7 depicts a representative circuit block diagram that can be used with embedded transformer 264, and will be described in general terms as follows. Oscillator driver 232 receives electrical power from a power supply (not shown), producing a time-varying waveform having a frequency that can vary between 50 Hz - 1 MHz. The output of oscillator driver 232 is applied to signal conditioner 234, producing an alternating voltage that is applied across the primary of embedded transformer 264, thereby inducing voltage across the combined secondary of embedded transformer 264. Decoder 236 senses the secondary voltage across embedded transformer 264, providing a periodic signal to timer 238 representative of the induced voltage at the secondary of embedded transformer 264. Timer 238 is configured to require a periodic signal input from decoder 236 as a representation of normal operation.

[0020] During a tamper event in which an unauthorized user removes cover screw 260 to gain access within chassis 250 (as shown in FIG. 3A), shaft 262 is removed

from embedded transformer 264, thereby reducing the magnetic flux coupling between primary winding 266, first secondary winding 268, and second secondary winding 270. As oscillator driver 232 and signal conditioner 234 continue to provide a time-varying alternating voltage across the primary of embedded transformer 264, the voltage potential at the secondary of embedded transformer 264 is reduced as a result of the reduced magnetic flux coupling. Accordingly, decoder 236 stops producing periodic signals and timer 238 responds to the absence of periodic signals, thereby providing an input to tamper controller 118 indicating that a tamper event has occurred.

[0021] FIG. 8 is an exemplary electrical schematic diagram of tamper system 230 described above with respect to FIG. 7. Shown in FIG. 8 are tamper system 230, oscillator driver 232, signal conditioner 234, decoder 236, timer 238, and embedded transformer 264. The electronic components shown in FIG. 6 create a representative electronic circuit that performs the functionality of tamper system 230. In the illustrated embodiment, oscillator driver 232 includes an operational amplifier (i.e., Op Amp), and timer 238 includes a monostable pulse generator (i.e., one shot). It is to be appreciated that a detailed description of each electronic component is unnecessary. Instead, major sections of tamper system 230 are denoted as oscillator driver 232, signal conditioner 234, decoder 236, timer 238, and embedded transformer 264, each having an operation that is similar to the blocks described above with respect to FIG. 7. In some embodiments a different circuit can be used to sense the removal of cover screw 260, thereby altering the magnetic flux coupling in embedded transformer 264 and providing an indication that a tamper event has occurred.

[0022] FIG. 9A is an electrical schematic diagram of an embodiment of tamper switch 116 shown in FIG. 2. Switch device 140 shown in FIG. 9A is a double-pole double-throw (DPDT) switch having two sets of contacts (i.e., two poles) and two positions (i.e., two throws). Switch device 140 is an electromechanical component which responds to a mechanical actuation. Switch device 140 is shown in a "normal" position with regard to an electrical schematic diagram. Switch device 140 is held in the normal position by the force of a mechanical spring (not shown). When switch device is actuated by an external force, the mechanical spring is compressed, aligning switch device 140 in an anti-normal position. It is to be appreciated that in spring-return switches, "normally open (NO)" and "normally closed (NC)" refer to the alignment of electrical contacts when the spring-return switch is in a relaxed (i.e., not compressed) condition.

[0023] FIG. 9B is an electrical schematic diagram of a second embodiment of tamper switch 116. Switch device 140A shown in FIG. 9B is a single-pole double-throw (SPDT) switch. The description of switch device 140A is similar to that provided for switch device 140 provided above with respect to FIG. 9A, except that switch device 140A has only one set of contacts (i.e., one pole).

[0024] Tamper switches 140, 140A depicted above in FIGS. 9A - 9B are non-limiting exemplary embodiments of tamper switch 116, and many other switch contact configurations can be used in different embodiments. For example, in some embodiments a double-pole single-throw (DPST) switch can be used. In a particular embodiment, a single-pole single-throw (SPST) switch can be used. In other embodiments, electrical switches having multiple poles and/or multiple positions (i.e., more than two poles and/or more than two positions) can be used.

[0025] FIG. 10A is a perspective view of switch device 140 shown in FIG. 9A, depicting switch device 140 in a normal position (i.e., not compressed). FIG. 10B is a perspective view of switch device 140A shown in FIG. 9B, depicting switch device 140A in a normal position (i.e., not compressed). FIG. 10C is a perspective view of switch device 140C, and FIG. 10D is a perspective view of switch device 140D, depicting additional exemplary embodiments of tamper switch 116. Collectively, FIGS. 9A - 9B and 10A - 10D show non-limiting examples of tamper switch 116 depicted in FIG. 2. It is to be appreciated that a vast variety of electrical switches are commercially available, thereby representing a vast number of options that are available to implement tamper switch 116 in a particular embodiment. Various terms can be used to describe tamper switch 116, with non-limiting examples being "micro-switch", "limit switch", and "interlock switch". Moreover, micro-switches can be available under various trademarks (e.g., CHERRY™ Switch manufactured by Cherry GmbH (formerly Cherry Corporation).

[0026] FIG. 11 is side view of an embodiment of tamper switch 116 in an exemplary embodiment. Shown in FIG. 11 are switch device 140, chassis 150, chassis cover 152, and printed circuit boards 154, 156. Switch device 140 is a representative electrical switch, as described above with respect to FIGS. 9A and 10A. Chassis 150 encloses program memory 120 in which program data are stored. During normal operation, chassis cover 152 is in place as shown. Program data are stored on program memory 120 (not shown in FIG. 7), which can be located on printed circuit boards 154, 156. Chassis cover 152 is closed during routine system operation, as depicted in FIG. 11. Switch device 140 is mounted on printed circuit board 154 and is configured to be actuated (i.e., depressed) by chassis cover 152 when chassis cover 152 is closed. Accordingly, in the illustrated embodiment, the mechanical spring of switch device 140 is compressed during routine system operation, thereby holding switch device 140 in the anti-normal position as described above in respect to FIG. 9A. Accordingly, the anti-normal position of switch device 140 exists during routine system operation (i.e., tampering is not occurring). For tampering to occur, chassis cover 152 must be opened for an unauthorized person to gain access to program memory. The opening of chassis cover 152 allows switch device 140 to switch electrical position, move from the "anti-normal" position to the "normal" position. As will be seen in FIG. 12, the switching of switch device 140 can be indic-

ative of a tamper event.

[0027] FIG. 12 is an electrical block diagram showing switch device 140 of FIG. 9A in an exemplary embodiment. Shown in FIG. 12 are tamper system architecture 200, power source 112, tamper controller 118, program memory 120, and switch device 140. In the illustrated embodiment, power source 112, tamper controller 118, and program memory 120 are as described above with respect to FIG. 2, and switch device 140 is described as above with respect to FIG. 9A. Switch 140 functions as a tamper system, for example, as tamper system 130 shown in FIG. 2. When a tamper event occurs, switch device 140 is actuated, connecting electrical power from power source 112 to tamper controller 118, whereby tamper controller 118 provides instructions to program memory 120 that disrupt and/or erase the stored program data from program memory 120, thereby preventing the unauthorized access to stored program data.

[0028] In the embodiments described above, for example, with respect to FIGS. 2, 7, and 11 - 12, it can be important to determine when a tamper condition exists so that sensitive stored program data can be destroyed (i.e., removed, erased, wiped, disrupted). Non-limiting examples of sensitive program data can include software control code, software algorithms, hardware algorithms, reconnaissance information, intelligence data, and cryptographic keys. The destruction of program data is deemed to be necessary when it has been determined that tampering is occurring, meaning there is a possibility that an unauthorized person is attempting to access sensitive program data. The present disclosure is directed at a transducerless means of determining when a chassis cover is being removed as an identifiable indication of tampering. However, there can be situations when an authorized person may need to remove a chassis cover where it can be desirable for program data to not be destroyed. For example, a particular component that is protected by tamper system architecture 200 can require periodic inspection and/or maintenance by an authorized technician in an authorized test facility. In this exemplary situation, a tamper response deactivation technique is needed.

[0029] FIG. 13 is an electrical schematic diagram of an embodiment of a tamper deactivation circuit. Shown in FIG. 13 are tamper deactivation circuit 300, tamper power source 312, tamper controller 318, tamper unlock circuit 360, bias resistor 362, unlock signal line 364, first pin 366, second pin 368, and external plug 370. Tamper deactivation circuit 300 can be included with tamper system architecture 100 as shown in FIG. 2. When activated by an authorized user, tamper unlock circuit 360 provides unlock signal 364 to tamper controller 318. In the illustrated embodiment, unlock signal 364 is provided continuously to tamper controller 318 during the duration of the maintenance period. Tamper controller 318 is configured to ignore a tamper signal from a tamper system (e.g., tamper system 130 as shown in FIG. 2) while unlock signal 364 is present at tamper controller 318. During the normal operation of the tamper system architecture (not shown), meaning that tamper system architecture is providing protection against a tampering event, tamper deactivation circuit 300 does not deactivate the tamper response. Accordingly, in this normal condition, tamper unlock circuit 360 is not engaged, and the voltage of tamper power source 312 is present at unlock signal 364 as a result of bias resistor 362. Tamper controller 318 is configured so that when a sufficient voltage potential exists at unlock signal 364, tamper controller 318 will function normally (i.e., respond to a tamper event by destroying program data stored in program memory 120). However, during authorized maintenance, a technician can install external plug 370 on tamper unlock circuit 360, electrically connecting first pin 366 to second pin 368 and thereby shunting unlock signal line to ground. Tamper controller 318 is configured to ignore a tamper signal when a ground potential exists at unlock signal 364, thereby deactivating the tamper system architecture. After installing external plug 370, the technician can proceed with opening chassis cover 152 to perform the authorized inspection and/or maintenance.

[0030] In an embodiment, external plug 370 can be configured to help prevent a technician from failing to remove external plug 370 form tamper unlock circuit 360 after the completion of the inspection and/or maintenance. For example, in a particular embodiment, external plug 370 can be configured with an encumbering device that is conspicuous and/or prevents normal system operation. In another embodiment, first pin 366 and secondpin 368 can be configured to be masked and/or concealed to prevent their identification by an unauthorized user. For example, in a particular embodiment, first pin 366 and/or second pin 368 and/or external plug 370 can be mechanically keyed so that only a particular design of external plug 370 can be used. In another embodiment, first pin 366 and/or second pin 368 can be secluded among other similar-looking pins, whereby only an authorized user is aware of the identity of secluded first pin 366 and/or second pin 368.

[0031] FIG. 13 is an electrical block diagram of a second embodiment of the tamper deactivation circuit in which the tamper deactivation is accessed through an embedded control. Shown in FIG. 14 are tamper deactivation circuit 500, tamper controller 518, tamper unlock circuit 560, power input resistor 562, tamper power source 564, equipment power source 566, power OR circuit 568, non-volatile memory 570, address bus 572, data bus 574, processing system 580, RD/WR input 582, internal data bus 584, communications bus 586, and test interface 588. In the illustrated embodiment, tamper controller 518 can be substantially similar to tamper controller 118 and tamper power source 564 can be substantially similar to power source 112 as described above in respect to FIG. 2. Accordingly, tamper power source 564 is a long-life source of electrical power. In the illustrated embodiment, equipment power source 566 can be a power supply that energizes the equipment (not shown) being

protected by tamper system architecture 100.

[0032] Prior to accessing protected equipment by opening the chassis cover (not shown in FIG. 13), an authorized user will access non-volatile memory 570 of tamper unlock circuit 560 by issuing a write command on read/write (RD/WR) input 582 to non-volatile memory 570 via a memory mapped location in processing system 580 to deactivate an indication of a tamper event. An authorized user can access processing system 580 by providing the proper memory mapped location at communications bus 586 from test interface 588. Communications bus 586 can be called a test communications bus, and test interface 588 can be called a test facility test interface, because access by an authorized user can typically occur at an authorized test facility. Processing system 580 can also be called an embedded control processing system because it is embedded within the system architecture. The identity of the memory mapped location within processing system is necessary to provide the tamper deactivation, but the location remains concealed even if the chassis cover is opened to provide access to processing system 580. Therefore, tamper unlock circuit 560 cannot be activated or the memory mapped location determined after the chassis cover has been opened.

[0033] Tamper power source 564 and equipment power source 566 provide electrical power to tamper unlock circuit 560 via power OR circuit 568, thereby providing electrical power to tamper power circuit 560 so long as tamper power source 564 or equipment power source 566 (or both) are energized. In the illustrated embodiment, a lock/unlock signal on data bus 574 is only activated when a tamper event is detected. In these embodiments, electrical power is drawn only when a tamper event occurs, thereby energizing tamper power source 564 to supply power to tamper unlock circuit 560, in turn providing an unlock signal to tamper controller 518. Accordingly, power is drawn only when a tamper event occurs, thereby helping to prolong the duration of tamper power source 564. Non-volatile memory 570 is separate from processor system 580 to reduce the power drawn from tamper power source 564 when equipment power source 566 is de-energized. Accordingly, non-volatile memory 570 maintains the desired lock/unlock signal on data bus 574 after processing system 580 is de-energized. Non-volatile memory 570 is configured to always output the proper lock/unlock signal at data bus 574. The condition of non-volatile memory 570 can only be changed when properly over-written by processing system 580 upon the receipt of an authorized signal from test interface 588 at communications bus 586.

[0034] In other embodiments, tamper power circuit 560 can remain powered after equipment power source 566 is de-energized by receiving electrical power from tamper power source 564 via power OR circuit 568.

Discussion of Possible Embodiments

[0035] The following are non-exclusive descriptions of possible embodiments of the present invention.

[0036] A self-powering tamper detection system architecture, comprising: a power source; a tamper detector, configured to mechanically actuate a tamper switch when a tamper event occurs; a tamper switch, electrically connected to the power source and mechanically connected to the tamper detector; a tamper unlock system, configured to provide a tamper unlock signal when an authorized maintenance condition exists; a tamper controller, configured: to produce a tamper response when the tamper event is identified; and to not produce the tamper response when the tamper unlock signal is provided; and program memory, configured to store program data; wherein the tamper response comprises a disruption of the program data.

[0037] The self-powering tamper detection system architecture of the preceding paragraph can optionally include, additionally and/or alternatively, any one or more of the following features, configurations and/or additional components:

[0038] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the power source stores electrical energy for at least 5 years.

[0039] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the power source stores electrical energy for at least 20 years.

[0040] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the power source comprises a chemical battery, electrical capacitor, and/or super-capacitor.

[0041] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the program memory comprises a field-programmable gate array (FPGA), flash memory, random access memory (RAM), programmable read-only memory (PROM), and/or erasable programmable read-only memory (EPROM).

[0042] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the program data comprises software control code, software algorithms, hardware algorithms, reconnaissance information, intelligence data, and/or cryptographic keys.

[0043] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the authorized maintenance condition comprises inspection and/or maintenance by an authorized technician in an authorized test facility.

[0044] A further embodiment of the foregoing self-powering tamper detection system architecture, further comprising: a chassis defining an interior and exterior; and two electrical pins; wherein: the program memory is located in the interior of the chassis; and the two electrical pins are disposed on the exterior of the chassis.

[0045] A further embodiment of the foregoing self-pow-

ering tamper detection system architecture, further comprising an external plug configured to electrically connect the two electrical pins when an authorized maintenance condition exists; wherein: the tamper unlock system is configured to generate a tamper inhibit condition when the two electrical pins are electrically connected; the tamper controller is configured to ignore the tamper event when the tamper inhibit condition is present; and the tamper controller is configured to respond to a tamper condition when the tamper inhibit condition is not present.

[0046] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the two electrical pins are disposed on the exterior of the chassis.

[0047] A further embodiment of the foregoing self-powering tamper detection system architecture, further comprising a plurality of pins, wherein the two electrical pins are concealed within the plurality of pins.

[0048] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein: the two electrical pins are disposed on a connector; and the external plug is mechanically keyed to the connector, defining a keyed external plug, thereby preventing the two electrical pins from being electrically connected without the keyed external plug.

[0049] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the tamper unlock system comprises: a test interface; a test communications bus, configured to receive a tamper inhibit signal from the test interface; an embedded control processing system, configured to receive the tamper inhibit signal from the communications bus; non-volatile memory, configured to store a lock-unlock signal; and a data bus, configured to provide the lock-unlock signal to the tamper controller; wherein: the tamper unlock system is configured to generate a tamper inhibit condition when the tamper inhibit signal is received from the test interface; and the tamper controller is configured to ignore the tamper event when the tamper inhibit condition is present.

[0050] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein: the memory-mapped location is concealed within the non-volatile memory; and the tamper inhibit signal is written to the memory-mapped location by an authorized technician.

[0051] A further embodiment of the foregoing self-powering tamper detection system architecture, wherein the power source comprises a power OR circuit configured to supply electrical power to the tamper unlock system when: the power source is providing electrical power; an equipment power supply is providing electrical power; or the power source is providing electrical power and the equipment power supply is providing electrical power.

[0052] A method of suppressing a tamper response in a self-powering tamper system architecture comprising a power source, a tamper detector configured to mechanically actuate a tamper switch when a tamper event occurs, a tamper switch electrically connected to the power source and mechanically connected to the tamper detector, a tamper unlock system configured to provide a tamper unlock signal when an authorized maintenance condition exists, a tamper controller configured to produce a tamper response when the tamper event is identified and to not produce the tamper response when the tamper unlock signal is provided, and program memory configured to store program data, the method comprising the steps of: inputting, to the tamper unlock system, a signal indicative of an authorized maintenance condition; and deactivating, by the tamper unlock system, the tamper response; wherein the tamper response comprises a disruption of the program data,

[0053] The method of the preceding paragraph can optionally include, additionally and/or alternatively, any one or more of the following features, configurations and/or additional components:

[0054] A further embodiment of the foregoing method, further comprising writing, by an authorized technician, a tamper inhibit signal to a memory-mapped mapped location, wherein the memory-mapped location is concealed within the non-volatile memory.

[0055] A further embodiment of the foregoing method, further comprising inputting a tamper inhibit signal to a test interface when the authorized maintenance condition exists.

[0056] A further embodiment of the foregoing method, wherein the power source comprises a power OR circuit configured to supply electrical power to the tamper unlock system when: the power source is providing electrical power; an equipment power supply is providing electrical power; or the power source is providing electrical power and the equipment power supply is providing electrical power.

[0057] A further embodiment of the foregoing method, wherein electrical power is supplied to the self-powering tamper system architecture only when a tamper event occurs.

[0058] While the invention has been described with reference to an exemplary embodiment(s), it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted for elements thereof without departing from the scope of the invention as defined by the claims. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the invention without departing from the scope thereof. Therefore, it is intended that the invention not be limited to the particular embodiment(s) disclosed, but that the invention will include all embodiments falling within the scope of the appended claims.

Claims

1. A self-powering tamper detection system architecture, comprising:

a power source (112);
a tamper detector (114), configured to mechanically actuate a tamper switch when a tamper event occurs;
a tamper switch (116), electrically connected to the power source and mechanically connected to the tamper detector;
a tamper unlock system (360), configured to provide a tamper unlock signal when an authorized maintenance condition exists;
a tamper controller (118), configured:

to produce a tamper response when the tamper event is identified; and
to not produce the tamper response when the tamper unlock signal is provided; and

program memory (120), configured to store program data;
wherein the tamper response comprises a disruption of the program data; and

further comprising:

a test interface (588) ;
a test communications bus (586), configured to receive a tamper inhibit signal from the test interface;
an embedded control processing system (580), configured to receive the tamper inhibit signal from the communications bus;
non-volatile memory (570), configured to store a lock-unlock signal; and
a data bus (574), configured to provide the lock-unlock signal to the tamper controller; and
a memory-mapped location
wherein:

the tamper unlock system is configured to generate a tamper inhibit condition when the tamper inhibit signal is received from the test interface;
the tamper controller is configured to ignore the tamper event when the tamper inhibit condition is present;

the memory-mapped location is concealed within the non-volatile memory; and
the tamper inhibit signal is written to the memory-mapped location by an authorized technician.

2. The self-powering tamper detection system architecture of claim 1, wherein the power source (42) stores electrical energy for at least 5 years, or wherein the power source stores electrical energy for at least 20 years.

3. The self-powering tamper detection system architecture of claim 1 or 2, wherein the power source (112) comprises a chemical battery, electrical capacitor, or super-capacitor.

4. The self-powering tamper detection system architecture of any preceding claim, wherein the program memory (120) comprises a field-programmable gate array (FPGA), flash memory, random access memory (RAM), programmable read-only memory (PROM), or erasable programmable read-only memory (EPROM).

5. The self-powering tamper detection system architecture of any preceding claim, wherein the program data comprises software control code, software algorithms, hardware algorithms, reconnaissance information, intelligence data, or cryptographic keys.

6. The self-powering tamper detection system architecture of any preceding claim, wherein the authorized maintenance condition comprises inspection and/or maintenance by an authorized technician in an authorized test facility.

7. A method of suppressing a tamper response in a self-powering tamper system architecture comprising a power source, a tamper detector configured to mechanically actuate a tamper switch when a tamper event occurs, a tamper switch electrically connected to the power source and mechanically connected to the tamper detector, a tamper unlock system configured to provide a tamper unlock signal when an authorized maintenance condition exists, a tamper controller configured to produce a tamper response when the tamper event is identified and to not produce the tamper response when the tamper unlock signal is provided, and program memory configured to store program data, the method comprising the steps of:

inputting, to the tamper unlock system, a tamper inhibit signal indicative of an authorized maintenance condition; and
deactivating, by the tamper unlock system, the tamper response;
wherein inputting, to the tamper unlock system comprises:
writing, by an authorized technician, the tamper inhibit signal to a memory-mapped location, wherein the memory-mapped location is concealed within the non-volatile memory;
wherein the tamper response comprises a disruption of the program data.

8. The method of claim 7, further comprising inputting the tamper inhibit signal to a test interface when the authorized maintenance condition exists.

9. The method of claim 8, wherein the power source comprises a power OR circuit configured to supply electrical power to the tamper unlock system when:

the power source is providing electrical power; an equipment power supply is providing electrical power; or
the power source is providing electrical power and the equipment power supply is providing electrical power, and preferably wherein electrical power is supplied to the self-powering tamper system architecture only when a tamper event occurs.

Patentansprüche

1. Selbstversorgende Manipulationsdetektionssystemarchitektur, umfassend:

eine Stromquelle (112);
einen Manipulationsdetektor (114), der dazu konfiguriert ist, einen Manipulationsschalter mechanisch zu betätigen, wenn ein Manipulationsereignis auftritt;
einen Manipulationsschalter (116), der elektrisch mit der Stromquelle verbunden ist und mechanisch mit dem Manipulationsdetektor verbunden ist;
ein Manipulationsentriegelungssystem (360), das dazu konfiguriert ist, ein Manipulationsentriegelungssignal bereitzustellen, wenn ein autorisierter Wartungszustand besteht;
eine Manipulationssteuerung (118), konfiguriert:

um eine Manipulationsreaktion zu erzeugen, wenn das Manipulationsereignis identifiziert wird; und
keine Manipulationsreaktion zu erzeugen, wenn das Manipulationsentriegelungssignal bereitgestellt wird; und
Programmspeicher (120), der zum Speichern von Programmdaten konfiguriert ist;
wobei die Manipulationsreaktion eine Unterbrechung der Programmdaten umfasst; und ferner umfassend:

eine Testschnittstelle (588);
einen Testkommunikationsbus (586), der dazu konfiguriert ist, ein Manipulationssperrsignal von der Testschnittstelle zu empfangen;
ein eingebettetes Steuerungsverarbeitungssystem (580), das dazu konfiguriert ist, das Manipulationssperrsignal von dem Kommunikationsbus zu empfangen;
nichtflüchtiger Speicher (570), konfiguriert, um ein Verriegelungs-Entriegelungs-Signals zu speichern; und
einen Datenbus (574), der dazu konfiguriert ist, das Verriegelungs-Entriegelungs-Signal an die Manipulationssteuerung zu liefern; und
ein speicherabgebildeter Ort,
wobei:

das Manipulationsentriegelungssystem dazu konfiguriert ist, eine Manipulationssperrbedingung zu erzeugen, wenn das Manipulationssperrsignal von der Testschnittstelle empfangen wird;
die Manipulationssteuerung dazu konfiguriert ist, das Manipulationsereignis zu ignorieren, wenn die Manipulationssperrbedingung vorhanden ist;
der speicherabgebildete Ort innerhalb des nichtflüchtigen Speichers verborgen ist; und
das Manipulationssperrsignal von einem autorisierten Techniker an den speicherabgebildeten Ort geschrieben wird.

2. Selbstversorgende Manipulationsdetektionssystemarchitektur nach Anspruch 1, wobei die Stromquelle (42) elektrische Energie für mindestens 5 Jahre speichert oder wobei die Stromquelle elektrische Energie für mindestens 20 Jahre speichert.

3. Selbstversorgende Manipulationsdetektionssystemarchitektur nach Anspruch 1 oder 2, wobei die Stromquelle (112) eine chemische Batterie, einen elektrischen Kondensator oder einen Superkondensator umfasst.

4. Selbstversorgende Manipulationsdetektionssystemarchitektur nach einem der vorhergehenden Ansprüche, wobei der Programmspeicher (120) ein feldprogrammierbares Gate-Array (field-programmable gate array, FPGA), einen Flash-Speicher, einen Direktzugriffsspeicher (random access memory, RAM), einen programmierbaren Nur-Lese-Speicher (programmable read-only memory, PROM) oder einen löschbaren programmierbaren Nur-Lese-Speicher (erasable programmable read-only memory, EPROM) umfasst.

5. Selbstversorgende Manipulationsdetektionssystemarchitektur nach einem der vorhergehenden Ansprüche, wobei die Programmdaten Softwaresteuercode, Softwarealgorithmen, Hardwarealgorithmen, Aufklärungsinformationen, Geheimdienstda-

ten oder kryptografische Schlüssel umfassen.

6. Selbstversorgende Manipulationsdetektionssystemarchitektur nach einem der vorhergehenden Ansprüche, wobei der autorisierte Wartungszustand eine Inspektion und/oder Wartung durch einen autorisierten Techniker in einer autorisierten Prüfeinrichtung umfasst.

7. Verfahren zum Unterdrücken einer Manipulationsreaktion in einer selbstversorgenden Manipulationssystemarchitektur, umfassend eine Stromquelle, einen Manipulationsdetektor, der dazu konfiguriert ist, einen Manipulationsschalter mechanisch zu betätigen, wenn ein Manipulationsereignis auftritt, einen Manipulationsschalter, der elektrisch mit der Stromquelle verbunden ist und mechanisch mit dem Manipulationsdetektor verbunden ist, ein Manipulationsentriegelungssystem, das dazu konfiguriert ist, ein Manipulationsentriegelungssignal bereitzustellen, wenn ein autorisierter Wartungszustand besteht, eine Manipulationssteuerung, die dazu konfiguriert ist, eine Manipulationsreaktion zu erzeugen, wenn das Manipulationsereignis identifiziert wird, und die Manipulationsreaktion nicht zu erzeugen, wenn das Manipulationsentriegelungssignal bereitgestellt wird, und Programmspeicher, der zum Speichern von Programmdaten konfiguriert ist, wobei das Verfahren die folgenden Schritte umfasst:

Eingeben eines Manipulationssperrsignals, das einen autorisierten Wartungszustand anzeigt, in das Manipulationsentriegelungssystem; und
Deaktivieren der Manipulationsreaktion durch das Manipulationsentriegelungssystem;
wobei das Eingeben in das Manipulationsentriegelungssystem umfasst:

Schreiben des Manipulationssperrsignals durch einen autorisierten Techniker an einen speicherabgebildeten Ort, wobei der speicherabgebildete Ort innerhalb des nichtflüchtigen Speichers verborgen ist;
wobei die Manipulationsreaktion eine Unterbrechung der Programmdaten umfasst.

8. Verfahren nach Anspruch 7, ferner umfassend das Eingeben des Manipulationssperrsignals in eine Testschnittstelle, wenn der autorisierte Wartungszustand besteht.

9. Verfahren nach Anspruch 8, wobei die Stromquelle eine Strom-ODER-Schaltung umfasst, die dazu konfiguriert ist, dem Manipulationsentriegelungssystem elektrische Energie zuzuführen, wenn:

die Stromquelle elektrischen Strom liefert;
eine Ausrüstungsstromversorgung elektrischen Strom liefert; oder
die Energiequelle elektrische Energie bereitstellt und die Ausrüstungsstromversorgung elektrische Energie bereitstellt, und wobei elektrische Energie vorzugsweise nur dann an die selbstversorgende Manipulationssystemarchitektur geliefert wird, wenn ein Manipulationsereignis auftritt.

Revendications

1. Architecture de système de détection de fraudes auto-alimenté, comprenant :

une source d'alimentation (112) ;
un détecteur de fraudes (114), configuré pour actionner mécaniquement un commutateur de fraudes lorsqu'un événement de fraudes se produit ;
un commutateur de fraudes (116), connecté électriquement à la source d'alimentation et connecté mécaniquement au détecteur de fraudes ;
un système de déverrouillage de fraudes (360), configuré pour fournir un signal de déverrouillage de fraudes lorsqu'une condition de maintenance autorisée existe ;
un dispositif de contrôle de fraudes (118), configuré :

pour produire une réponse de fraudes lorsque l'événement de fraudes est identifié ; et
pour ne pas produire la réponse de fraudes lorsque le signal de déverrouillage de fraudes est fourni ; et
une mémoire de programme (120), configurée pour stocker des données de programme ;
dans laquelle la réponse de fraudes comprend une interruption des données de programme ; et comprenant en outre :

une interface de test (588) ;
un bus de communication de test (586), configuré pour recevoir un signal d'inhibition de fraudes de l'interface de test ;
un système de traitement de contrôle intégré (580), configuré pour recevoir le signal d'inhibition de fraudes du bus de communication ;
une mémoire non volatile (570), configurée pour stocker un signal de verrouillage-déverrouillage ; et
un bus de données (574), configuré pour fournir le signal de verrouillage-déverrouillage au dispositif de contrôle

de fraudes ; et
un emplacement mappé en mémoire dans laquelle :

le système de déverrouillage de fraudes est configuré pour générer une condition d'inhibition de fraudes lorsque le signal d'inhibition de fraudes est reçu de l'interface de test ;
le dispositif de contrôle de fraudes est configuré pour ignorer l'événement de fraudes lorsque la condition d'inhibition de fraudes est présente ;
l'emplacement mappé en mémoire est caché dans la mémoire non volatile ; et
le signal d'inhibition de fraudes est écrit dans l'emplacement mappé en mémoire par un technicien agréé.

2. Architecture de système de détection de fraudes auto-alimenté selon la revendication 1, dans lequel la source d'alimentation (42) stocke de l'énergie électrique pendant au moins 5 ans, ou dans laquelle la source d'alimentation stocke de l'énergie électrique pendant au moins 20 ans.

3. Architecture de système de détection de fraudes auto-alimenté selon la revendication 1 ou 2, dans laquelle la source d'alimentation (112) comprend une batterie chimique, un condensateur électrique ou un supercondensateur.

4. Architecture de système de détection de fraudes auto-alimenté selon une quelconque revendication précédente, dans laquelle la mémoire de programme (120) comprend un réseau de portes programmables in situ (FPGA), une mémoire flash, une mémoire vive (RAM), une mémoire morte programmable (PROM), ou mémoire morte programmable effaçable (EPROM).

5. Architecture de système de détection de fraudes auto-alimenté selon une quelconque revendication précédente, dans laquelle les données de programme comprennent un code de contrôle logiciel, des algorithmes logiciels, des algorithmes matériels, des informations de reconnaissance, des données de renseignement ou des clés cryptographiques.

6. Architecture de système de détection de fraudes auto-alimenté selon une quelconque revendication précédente, dans laquelle la condition de maintenance autorisée comprend une inspection et/ou maintenance par un technicien agréé dans une installation d'essai agréée.

7. Procédé de suppression d'une réponse de fraudes dans une architecture de système de fraudes auto-alimenté comprenant une source d'alimentation, un détecteur de fraudes configuré pour actionner mécaniquement un commutateur de fraudes lorsqu'un événement de fraudes se produit, un commutateur de fraudes connecté électriquement à la source d'alimentation et connecté mécaniquement au détecteur de fraudes, un système de déverrouillage de fraudes configuré pour fournir un signal de déverrouillage de fraudes lorsqu'une condition de maintenance autorisée existe, un dispositif de contrôle de fraudes configuré pour produire une réponse de fraudes lorsque l'événement de fraudes est identifié et pour ne pas produire la réponse de fraudes lorsque le signal de déverrouillage de fraudes est fourni, et une mémoire de programme configurée pour stocker des données de programme, le procédé comprenant les étapes de :

entrée, dans le système de déverrouillage de fraudes, d'un signal d'inhibition de fraudes indicatif d'une condition de maintenance autorisée ; et
désactivation, par le système de déverrouillage de fraudes, de la réponse de fraudes ;
dans lequel la saisie dans le système de déverrouillage de fraudes comprend :

l'écriture, par un technicien agréé, du signal d'inhibition de fraudes dans un emplacement mappé en mémoire, dans lequel l'emplacement mappé en mémoire est caché dans la mémoire non volatile ;
dans lequel la réponse de fraudes comprend une interruption des données de programme.

8. Procédé selon la revendication 7, comprenant en outre l'entrée du signal d'inhibition de fraudes dans une interface de test lorsque la condition de maintenance autorisée existe.

9. Procédé selon la revendication 8, dans lequel la source d'alimentation comprend un circuit OU une alimentation configuré(e) pour fournir de l'énergie électrique au système de déverrouillage de fraudes lorsque :

la source d'alimentation fournit de l'énergie électrique ;
une alimentation électrique de l'équipement fournit de l'énergie électrique ; ou
la source d'alimentation fournit de l'énergie électrique et l'alimentation électrique de l'équipement fournit de l'énergie électrique, et de préfé-

rence dans lequel l'énergie électrique est fournie à l'architecture de système de fraudes autoalimenté uniquement lorsqu'un événement de fraudes se produit.

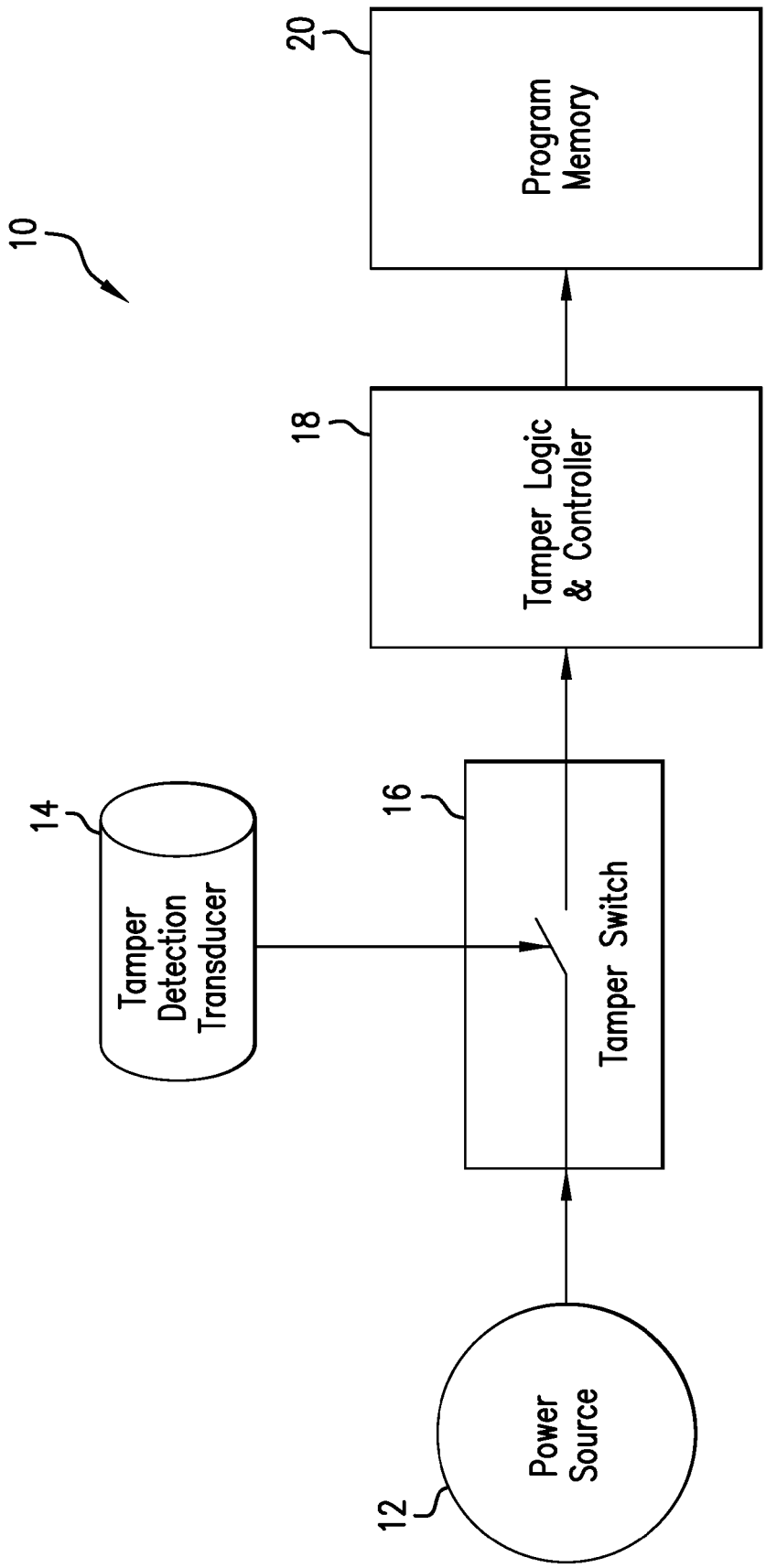

FIG. 1
(PRIOR ART)

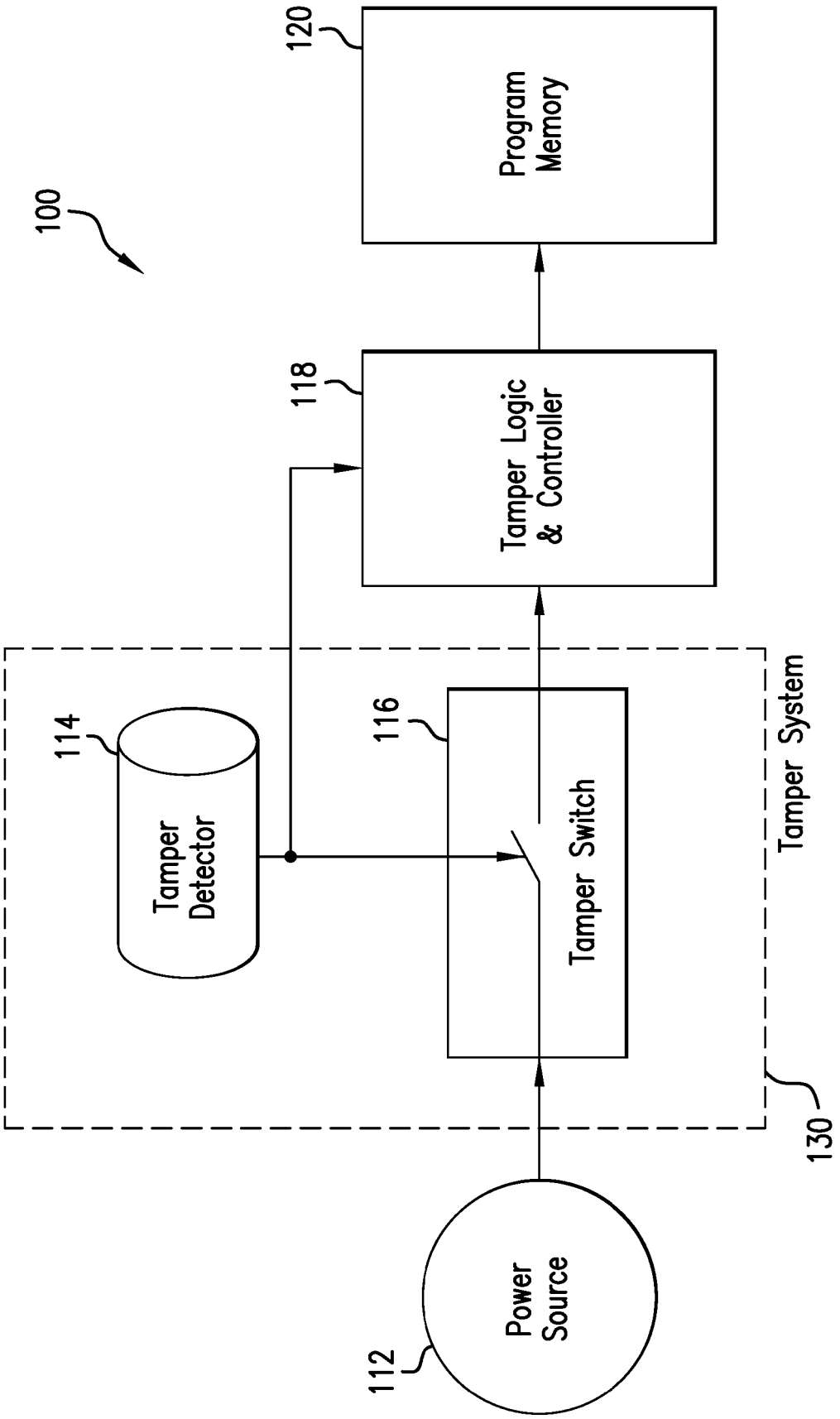
100
120
Program Memory
118
Tamper Logic & Controller
114
Tamper Detector
116
Tamper Switch
Tamper System
130
112
Power Source

FIG.2

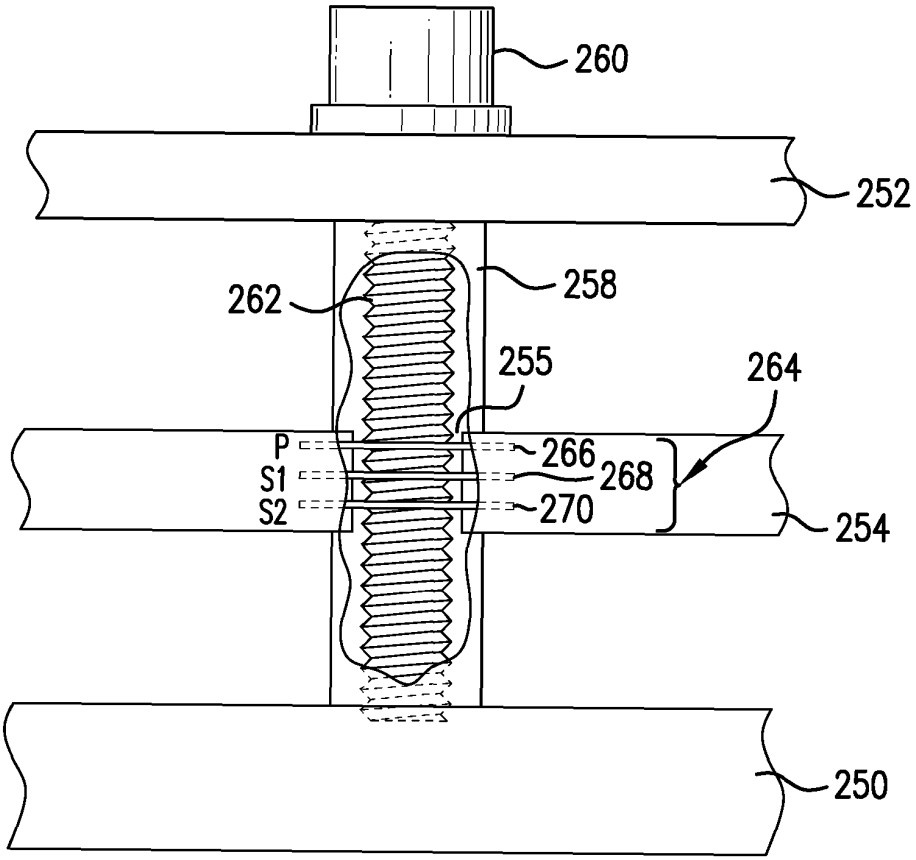
260
252
262
258
255
264
P
S1
S2
266
268
270
254
250

FIG.3A

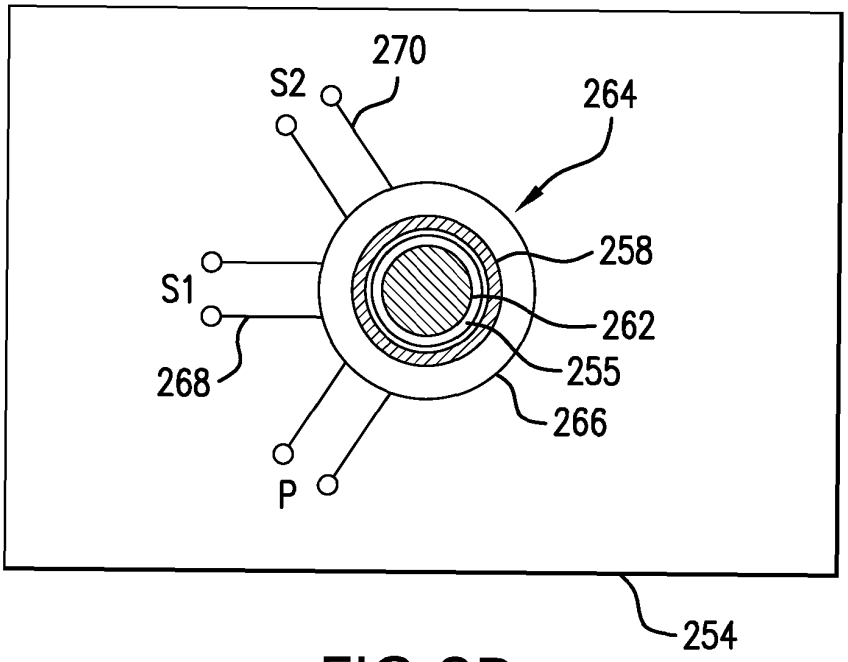
270
S2
264
258
S1
262
268
255
266
P
254

FIG.3B

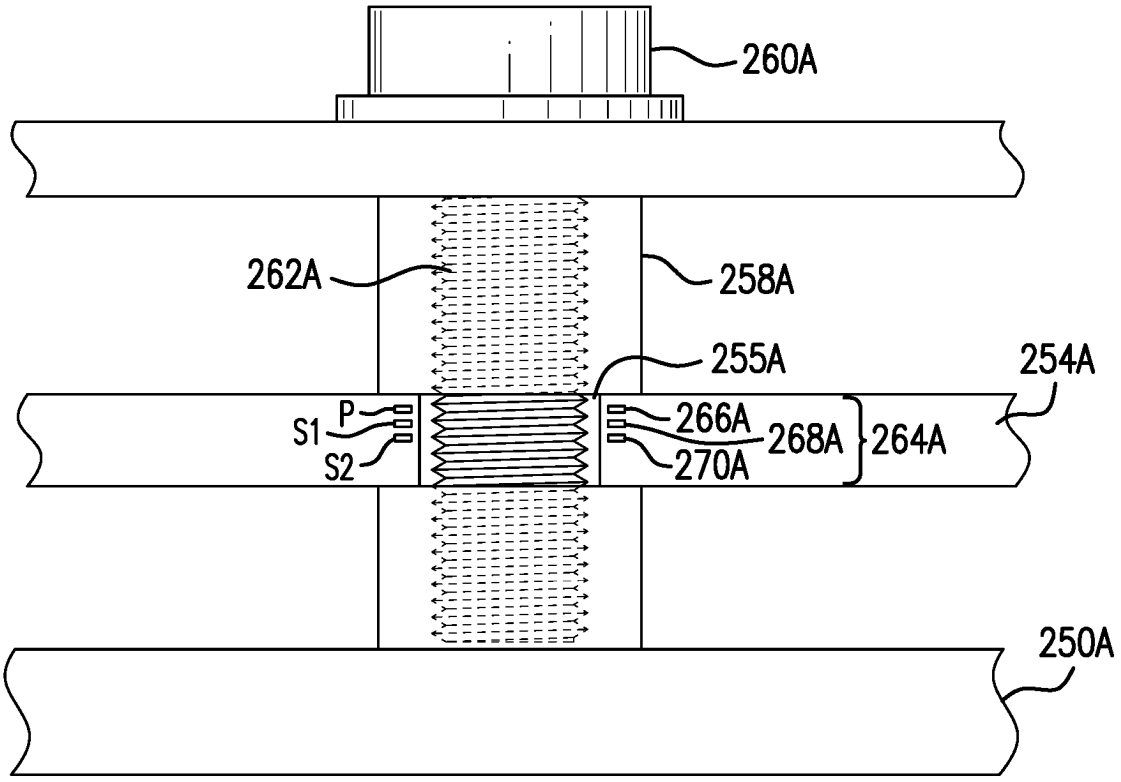
260A
262A
258A
255A
254A
P
S1
S2
266A
268A
270A
264A
250A

FIG.4A

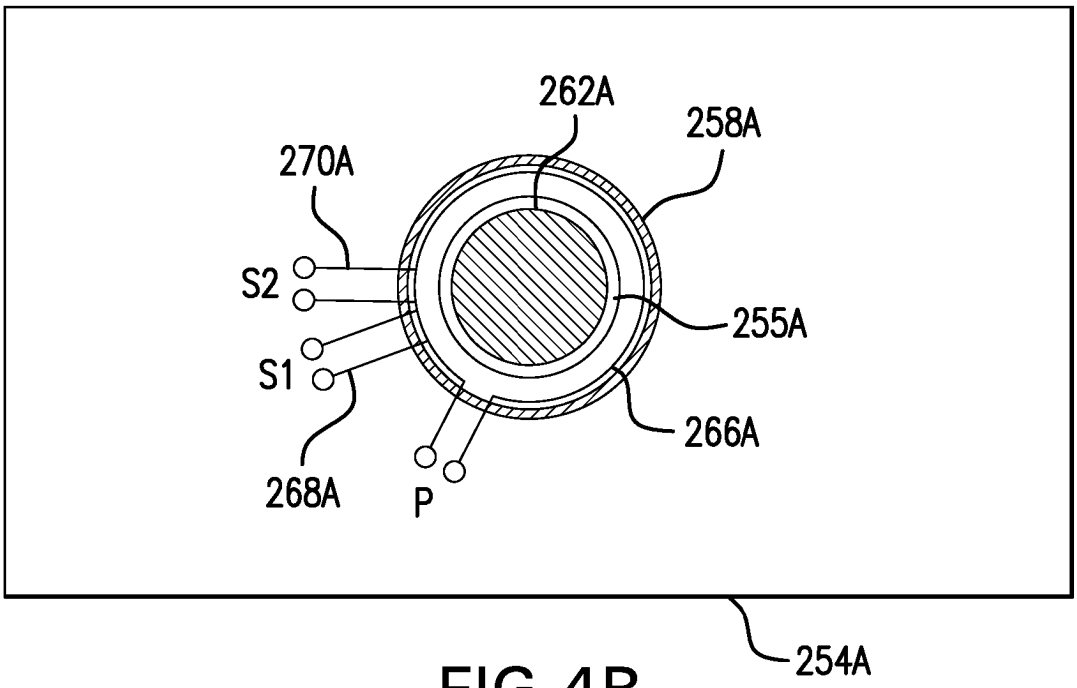
262A
258A
270A
S2
255A
S1
266A
268A
P
254A

FIG.4B

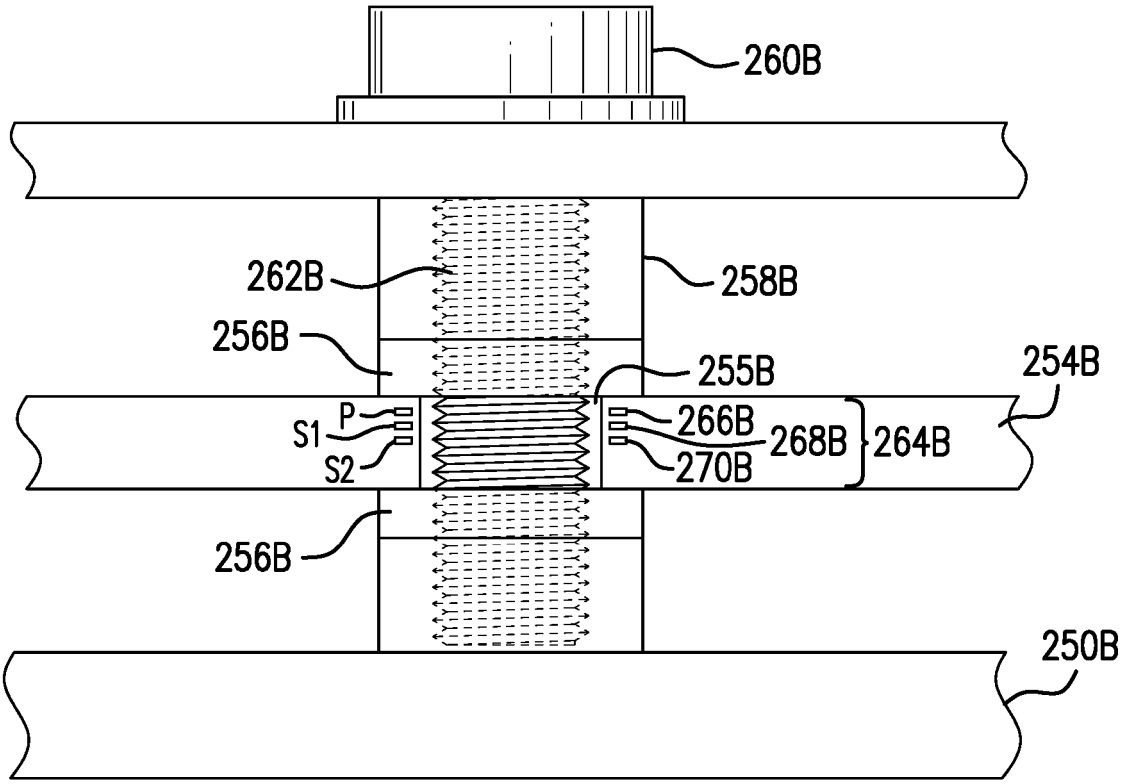
260B
262B
258B
256B
255B
254B
P
S1
S2
266B
268B
270B
264B
256B
250B

FIG.5A

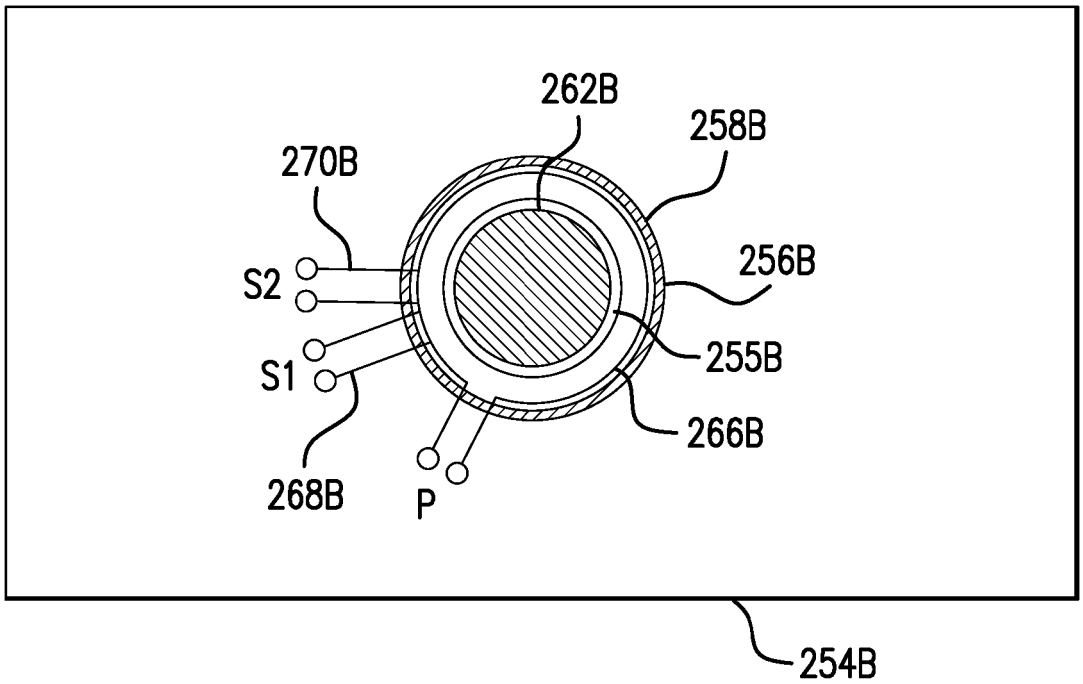
262B
258B
270B
256B
S2
255B
S1
266B
268B
P
254B

FIG.5B

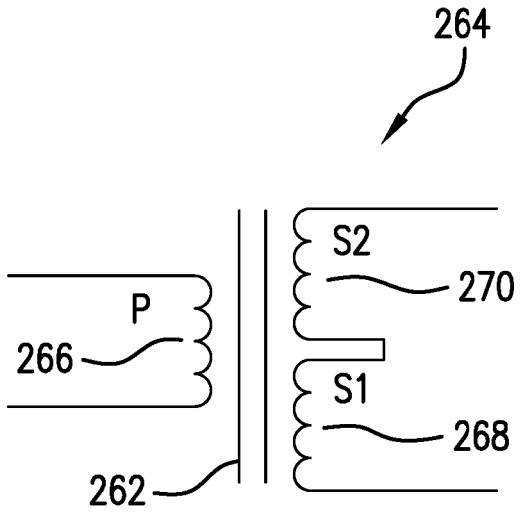

FIG.6A

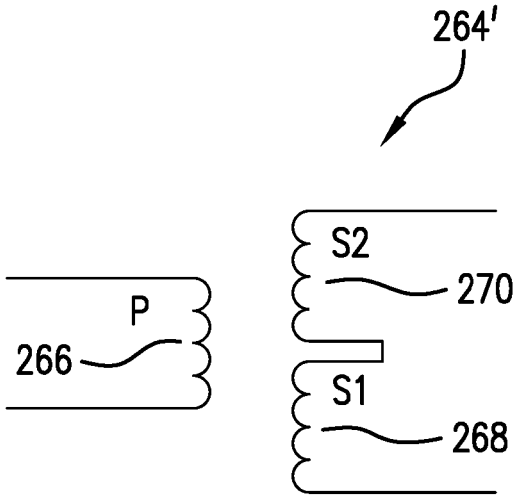

FIG.6B

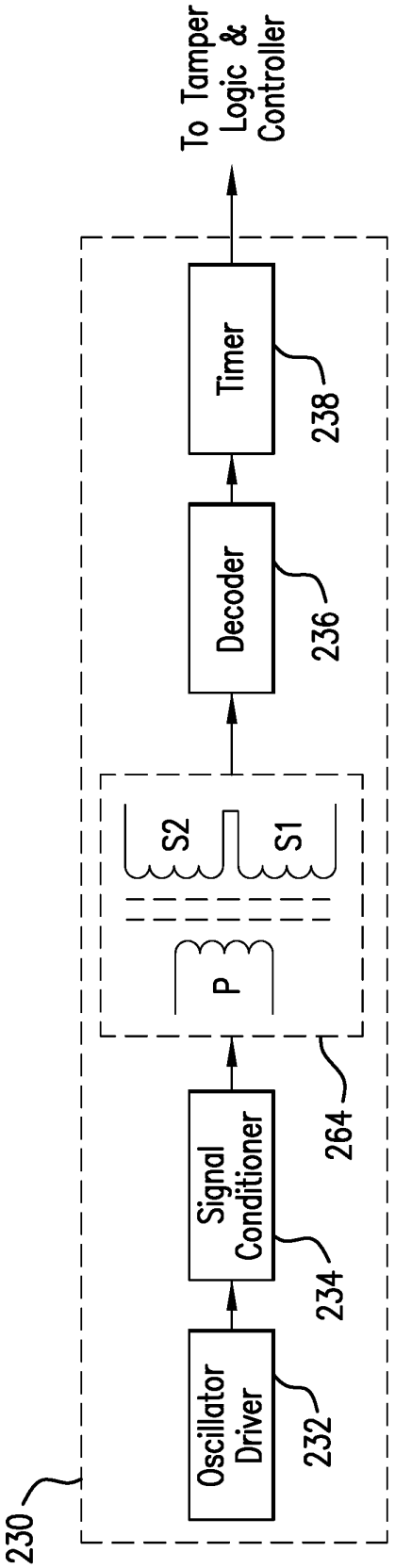
To Tamper Logic & Controller
Timer
238
Decoder
236
S2
S1
P
264
Signal Conditioner
234
Oscillator Driver
232
230

FIG.7

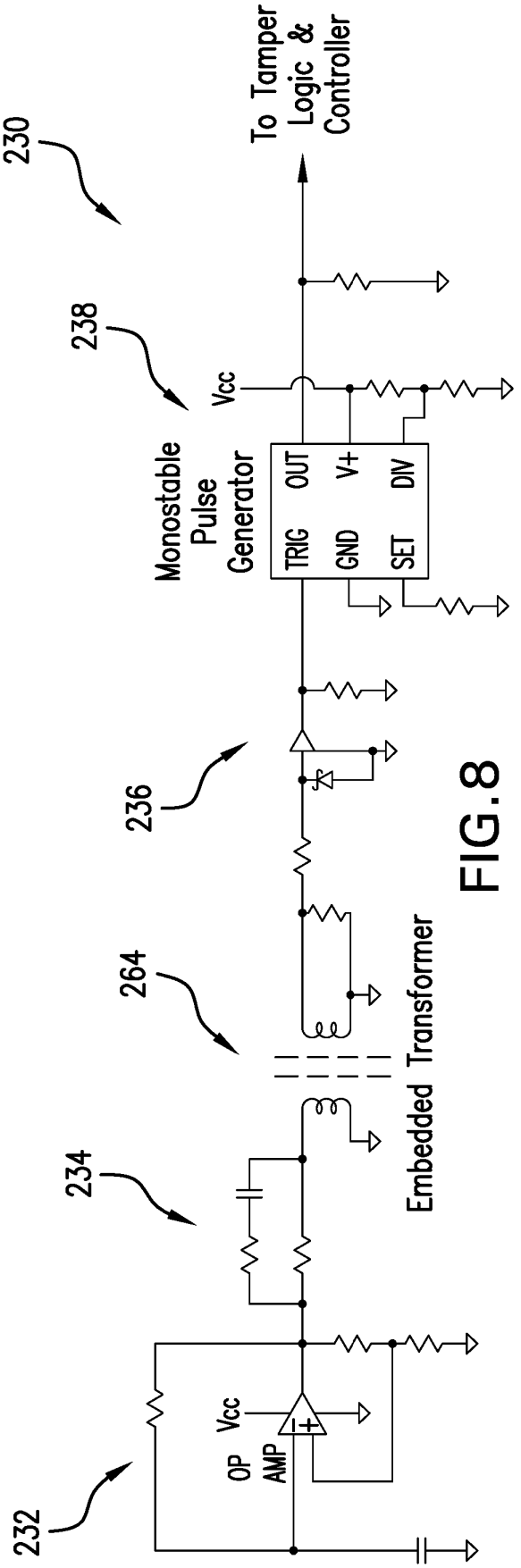
230
To Tamper Logic & Controller
238
Vcc
Monostable Pulse Generator
TRIG
OUT
V+
DIV
GND
SET
236
264
Embedded Transformer
234
Vcc
OP AMP
232

FIG.8

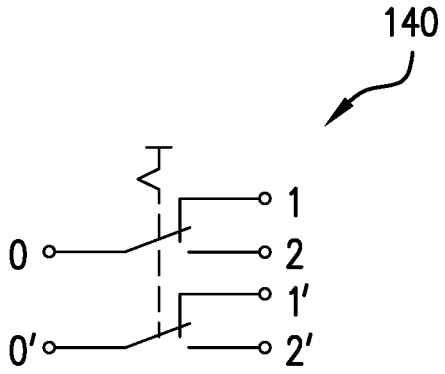

FIG.9A

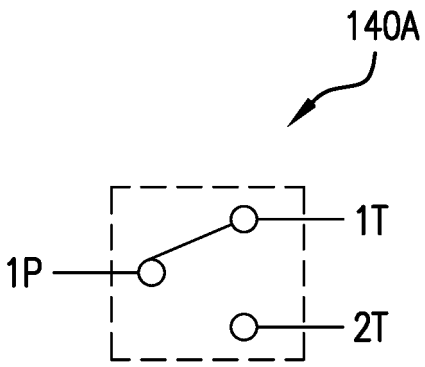

FIG.9B

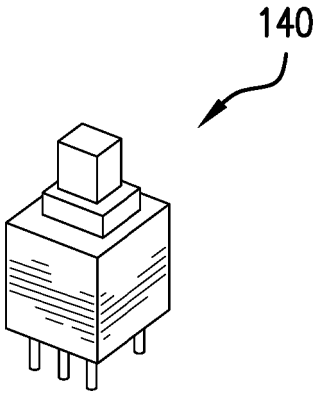

FIG.10A

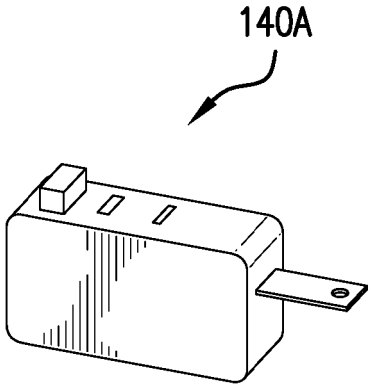

FIG.10B

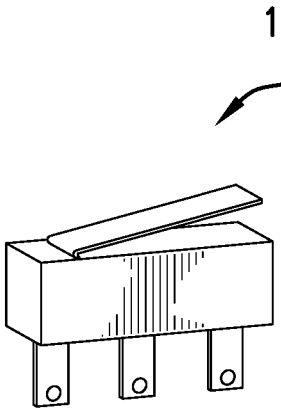

FIG.10C

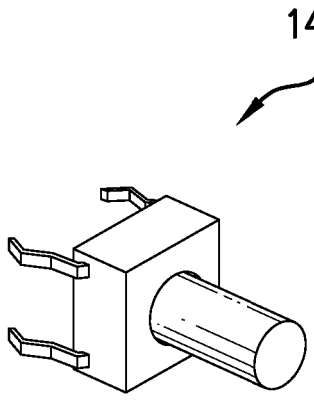

FIG.10D

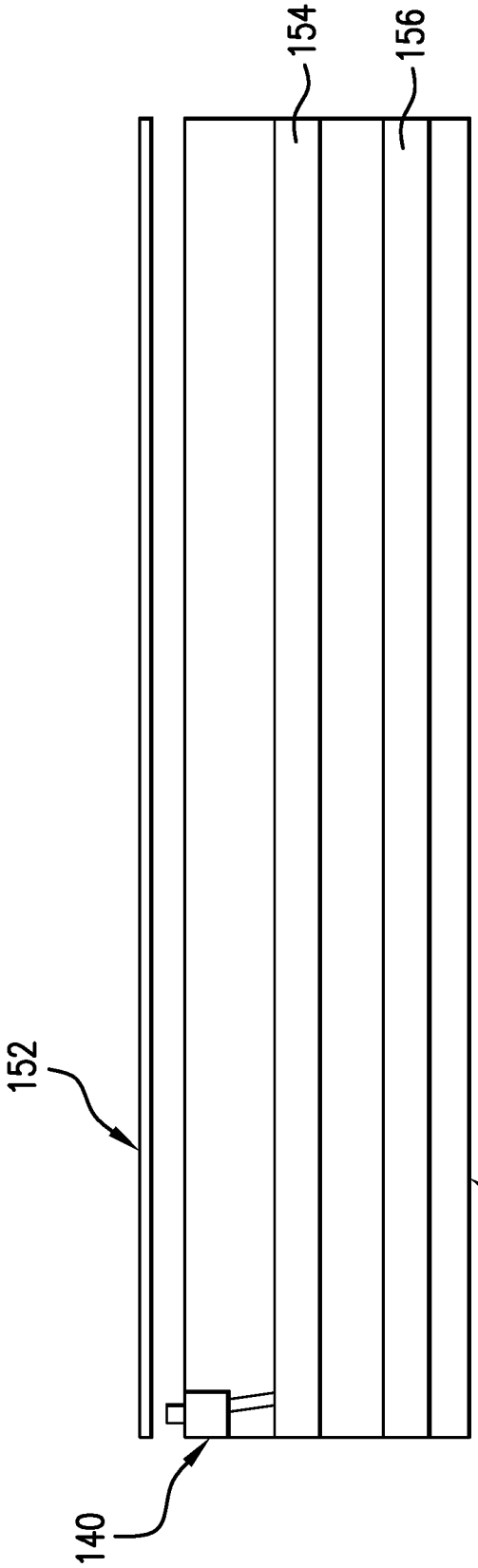

FIG. 11

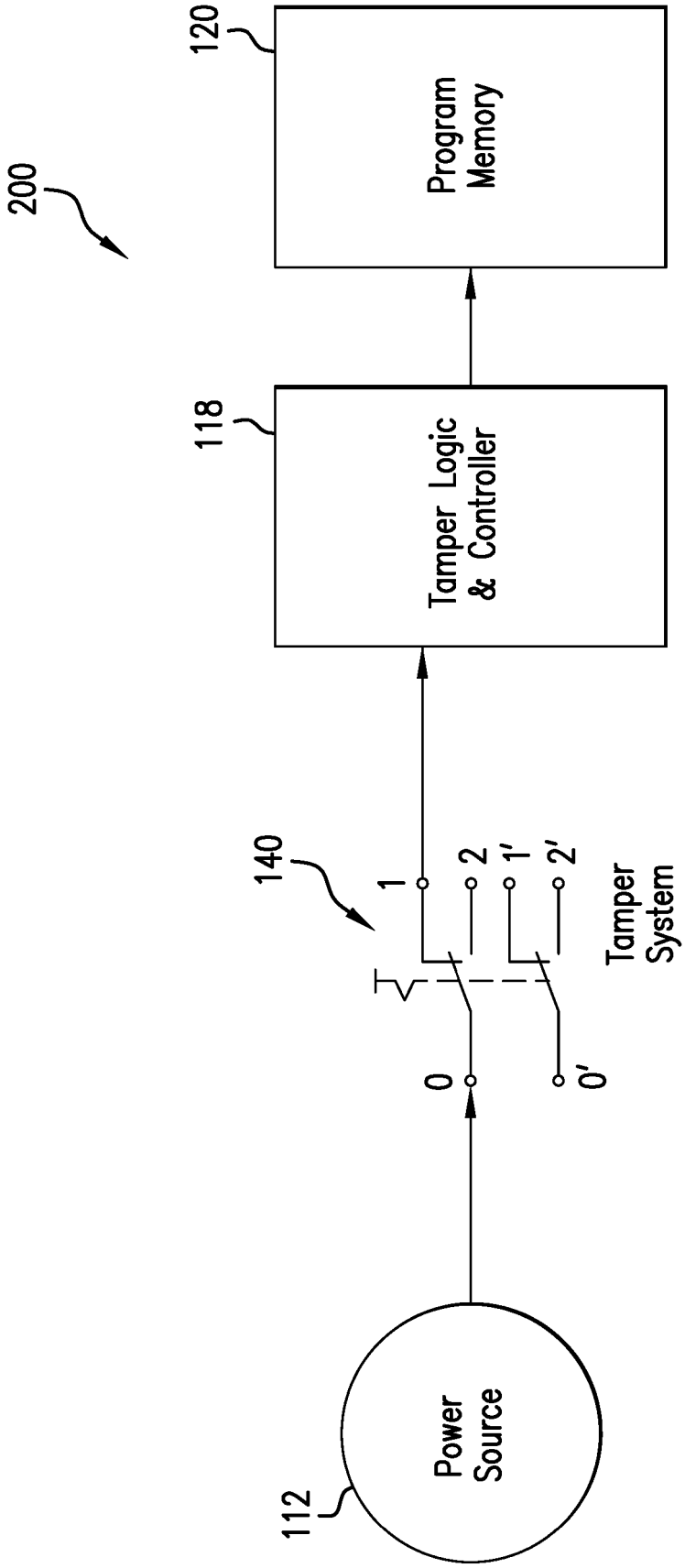
200
120
Program Memory
118
Tamper Logic & Controller
140
1
2
1'
2'
0
0'
Tamper System
130
112
Power Source

FIG. 12

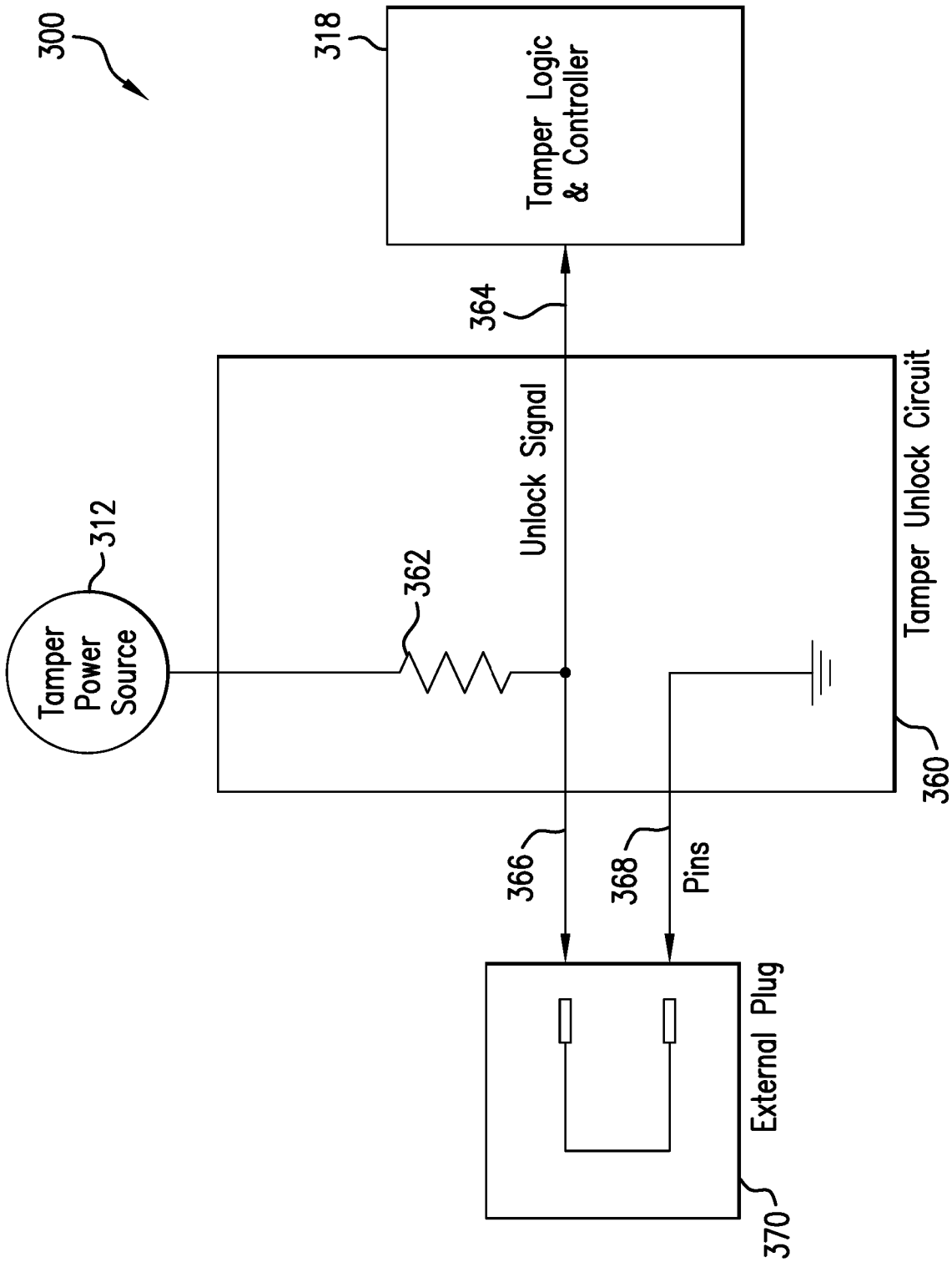
300
318
Tamper Logic & Controller
364
Unlock Signal
Tamper Unlock Circuit
312
362
Tamper Power Source
360
366
368
Pins
External Plug
370

FIG. 13

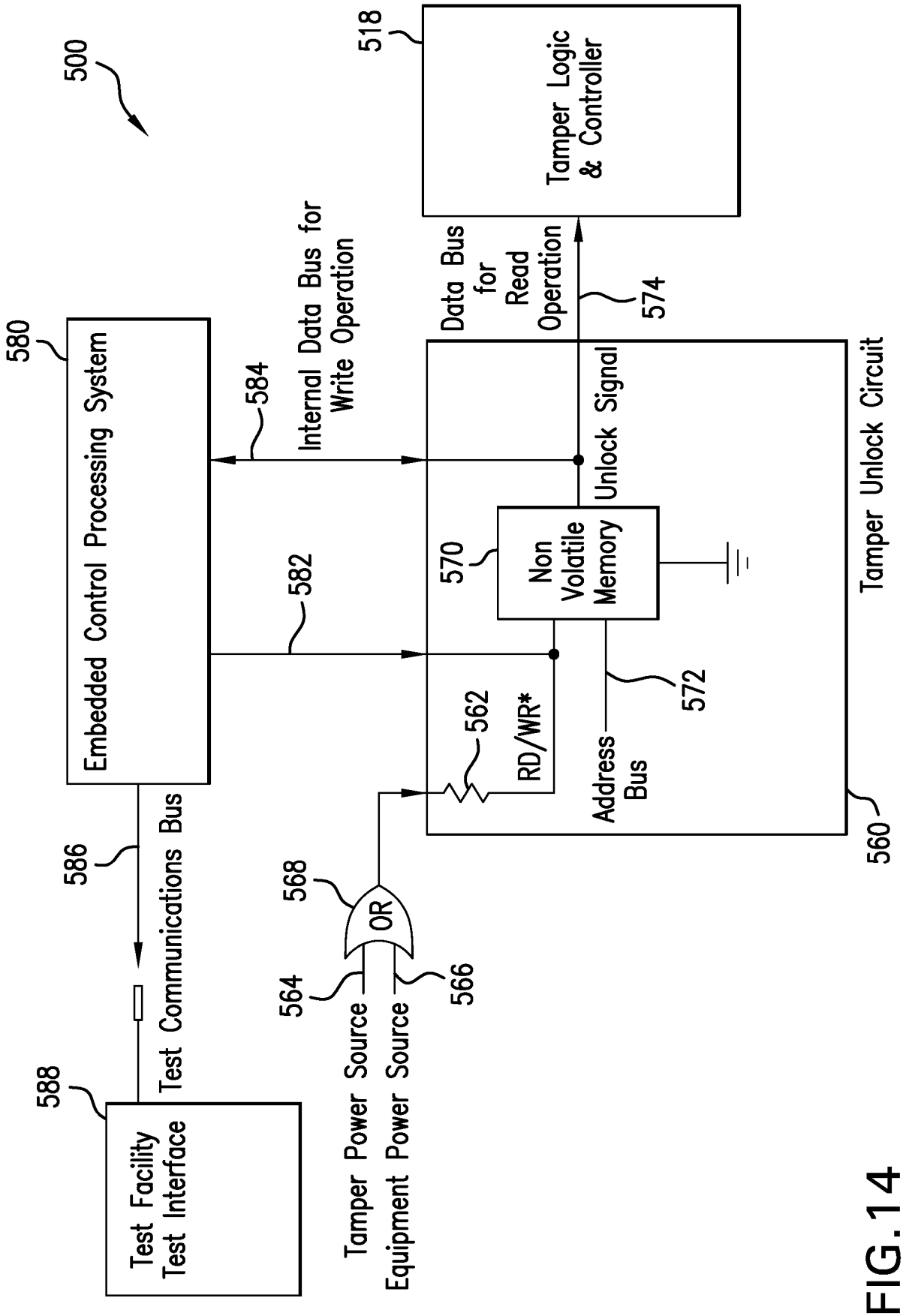
500
518
Tamper Logic & Controller
Data Bus for Read Operation
574
580
Embedded Control Processing System
584
Internal Data Bus for Write Operation
582
570
Non Volatile Memory
Unlock Signal
562
RD/WR*
572
Address Bus
Tamper Unlock Circuit
560
586
Test Communications Bus
568
OR
564
566
Tamper Power Source
Equipment Power Source
588
Test Facility Test Interface

FIG. 14

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

- US 9798902 B, Ludlow **[0003]**
- US 8499173 B, Caci **[0003]**
- US 8736286 B, Johnson **[0003]**
- US 2017116440 A **[0003]**
- US 2017354027 A **[0003]**