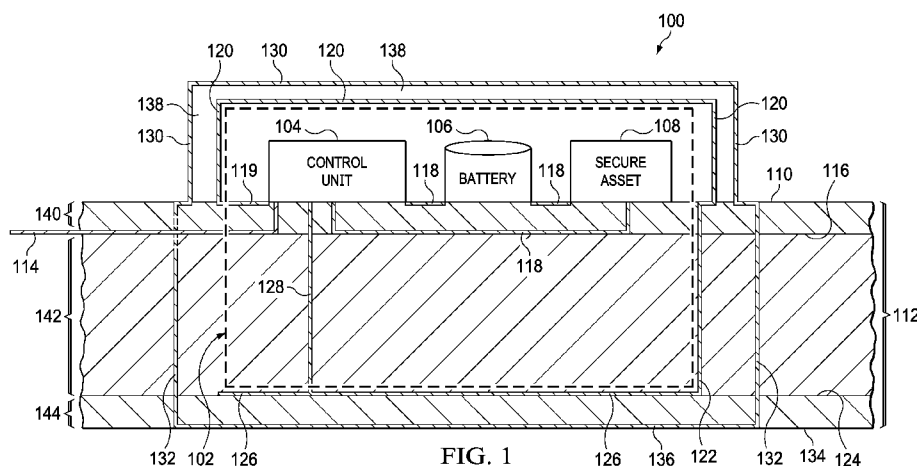




- (51) International Patent Classification:
G08B 13/12 (2006.01) *G08B 13/22* (2006.01)
- (21) International Application Number:
PCT/US2020/015569
- (22) International Filing Date:
29 January 2020 (29.01.2020)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
16/263,261 31 January 2019 (31.01.2019) US
- (63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 16/263,261 (CIP)
Filed on 31 January 2019 (31.01.2019)
- (71) Applicant: **TEXAS INSTRUMENTS INCORPORATED** [US/US]; P.O. Box 655474, Mail Station 3999, Dallas, TX 75265-5474 (US).
- (71) Applicant (for JP only): **TEXAS INSTRUMENTS JAPAN LIMITED** [JP/JP]; 24-1, Nishi-shinjuku 6-chome, Shinjuku-ku Tokyo, 160-8366 (JP).
- (72) Inventors: **LEEK, Alan, Henry**; 10023 Deerfield Dr., Frisco, TX 75033 (US). **HALL, Jace, Hunter**; 5005 Galleria Dr. Apt. 3433, Farmers Branch, TX 75244 (US).
- (74) Agent: **GRAHAM, Brian** et al.; TEXAS INSTRUMENTS INCORPORATED, P.O. Box 655474, Mail Station 3999, Dallas, TX 75265-5474 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

(54) Title: TAMPER DETECTION



(57) **Abstract:** An enclosure for circuitry 108 includes a platform 112, a charge source 106, a first capacitive plate 120, 122, 126, a second capacitive plate 130, 132, 136, and a capacitive sensor 104. The circuitry is fixedly coupled to the platform 112. The first capacitive plate 120, 122, 126 is also fixedly coupled to the platform 112, and either alone, or together with the platform 112, surrounds a volume 102 containing the circuitry 108 and the charge source 106, the charge source 106 electrically coupled to and configured to charge the first capacitive plate 120, 122, 126. The second capacitive plate 130, 132, 136 is fixedly coupled to the platform 112 without touching the first capacitive plate 120, 122, 126, and either alone, or together with the platform 112, surrounds the first capacitive plate 120, 122, 126. The second capacitive plate 130, 132, 136 is configured so that there is an electric potential difference between the first capacitive plate 120, 122, 126 and the second capacitive plate 130, 132, 136. The capacitive sensor 104 is electrically connected to

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

TAMPER DETECTION

BACKGROUND

[0001] This application relates generally to tamper-proofing of electronic systems, and more particularly to tamper-proof housings for sensitive electronic circuitry at the printed circuit board (PCB) level.

[0002] Many forms of electronic security are made vulnerable to penetration if an adverse party has physical access to the system. Reverse engineering, decapsulation, hardware-based man-in-the-middle attacks, and other methods can enable an attacker with physical access to system busses and connected integrated circuits (ICs) to circumvent system-level and/or device-level security. Physical attack tampering may allow certain intellectual property (IP) assets to be uncovered, stolen, altered, manipulated, destroyed, or otherwise compromised. Such IP assets can include software and its related data, including as examples financial information, authentication keys, or firmware images; or hardware, such as sensitive chip-level or PCB designs, or other physical systems such as clock sources, digital sequence sources, or actuator control. Prior art tamper-proof system coverings include, for example, potting, electro-mechanical switches configured to break contact on tampering, PCB tamper mesh enclosures, or a switch or button using inductive sensing coils, Hall effect detection, or ambient light detection.

SUMMARY

[0003] In described examples, an enclosure for circuitry includes a platform, a charge source, a first capacitive plate, a second capacitive plate, and a capacitive sensor. The circuitry is fixedly coupled to the platform. The first capacitive plate is also fixedly coupled to the platform, and either alone, or together with the platform, surrounds a volume containing the circuitry and the charge source, the charge source electrically coupled to and configured to charge the first capacitive plate. The second capacitive plate is fixedly coupled to the platform without touching the first capacitive plate, and either alone, or together with the platform, surrounds the first capacitive plate. The second capacitive plate is configured so that there is an electric potential difference between the first capacitive plate and the second capacitive plate. The capacitive sensor is electrically connected to the first capacitive plate and configured to determine when a

capacitance between the first and second capacitive plates is changed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 shows an example of a side view of an electrical block diagram view of a system 100 including a secure enclosure for tamper detection using capacitive sensing.

[0005] FIG. 2 shows an example plan and schematic view of the system of FIG. 1.

[0006]

[0007] FIG. 3A shows a three-quarters perspective view of an example implementation of a system including a secure enclosure (visible in FIG. 3C) for tamper detection using capacitive sensing.

[0008] FIG. 3B shows a three-quarters perspective view of the example system implementation of FIG. 3A.

[0009] FIG. 3C shows a three-quarters perspective view of the example system implementation of FIG. 3A.

[0010] FIG. 4 shows an example of a process for tamper detection using capacitive sensing.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

[0011] FIG. 1 shows an example of a side view of an electrical block diagram view of a system 100 including a secure enclosure 102 for tamper detection using capacitive sensing, where by way of introduction secure enclosure 102 includes a conductive structural inner volume (120, 122, 126, 128) and a conductive structural outer volume (130, 132, 136). The conductive structural outer volume surrounds the conductive structural inner volume, thereby presenting capacitance between the inner and outer volumes. As shown in FIG. 1, a control unit 104, a battery 106, and a secure asset 108 (such as one or more ICs) are mounted on a top surface 110 of a top layer 140 of a multi-layer PCB 112 (such as an FR4 PCB). The control unit 104 includes a capacitive sensor and logic for determining whether tampering has occurred based on capacitance measurements of the sensor. (“Capacitive sensor” refers to a sensor which senses capacitance. Changes in capacitance are preferably measured as relative changes in capacitance. In some embodiments, changes in capacitance can be measured as absolute changes in capacitance.) Changes in capacitance between the conductive structural inner volume and the conductive structural outer volume (e.g., changes greater than a threshold) indicate tampering.

[0012] The PCB 112 has a top layer 140, a middle layer 142, and a bottom layer, 144. The top layer 140 has a top surface 110. The middle layer 142 has a middle-top surface 116 at an

interface between the top layer 140 and the middle layer 142, and a middle-bottom surface 124 at an interface between the middle layer 142 and the bottom layer 144. The bottom layer has a bottom surface 134.

[0013] The “inside” of the secure enclosure 102 refers herein to the interior of the above-introduced inner volume, which is between (enclosed by) an inner top shield 120, such as a hollow rectangular parallelepiped open along one larger face and mounted on the top surface 110, and an inner bottom shield 126, such as a conductive plate located on the middle-bottom surface 124 (between the middle layer 142 and bottom layer 144 of the PCB 112). The “outside” of the secure enclosure 102 refers herein to a volume external to the above-introduced outer volume, which is beyond an outer top shield 130, such as a hollow rectangular parallelepiped open along one larger face but larger than inner top shield 120 and mounted on the top surface 110, and an outer bottom shield 136, such as a conductive plate mounted on the bottom surface 134. The inner top shield 120, inner bottom shield 126, outer top shield 130, and outer bottom shield 136 are further described below. There is preferably a single electrical connection 114 connecting circuitry inside the secure enclosure to circuitry outside the secure enclosure 102, to avoid providing routes – physical openings in the conductive structural volumes – by which an attacker might attempt to gain physical access to the inside of the secure enclosure. The connection 114 preferably runs along the middle-top surface 116, thereby embedding a length of the connection 114 within the PCB 112 so that tampering with the connection 114 more difficult, and connects to the control unit 104.

[0014] In some embodiments, electrical activity within the secure enclosure 102, or between the inside and outside of the secure enclosure 102, can affect sensed capacitance. This can be mitigated by, for example, PCB design, such as routing (direction and size of connections); bandwidth (or associated data rate) of signals; and timing and/or forced synchronicity capacitance measurements (for example, the system could force local electrical activity to stop when capacitance measurements are taken).

[0015] The control unit 104 is preferably connected by electrical lines 118 to the battery 106 and the secure asset 108 to mediate input and output (I/O) between the secure asset 106 and the outside of the secure enclosure 102, preventing I/O if tampering is detected. The control unit 104 is electrically connected through an electrical connection 119 to the inner top shield 120. The inner top shield 120 surrounds the inside of the secure enclosure 102 without gaps in the

inner top shield 120 or between the inner top shield 120 and the PCB 112. The inner top shield 120 is made of material appropriate as a capacitive plate (e.g., conductor), preferably selected to act as electromagnetic (EM) shielding, both with respect to photons (i.e., the capacitive material is opaque), and with respect to electric and magnetic fields. The inner top shield 120 is mounted on the top surface 110 of the PCB 112 and is electrically connected to the control unit 104 and the battery 106, and to one or more capacitive sense vias 122. Capacitive sense vias are conductive, and electrically couple the control unit 104 (and its integrated capacitive sensor) to the top and bottom inner shields 120, 130. One such via 122 is shown in FIG. 1, but as shown in FIG. 2, multiple adjacent capacitive sense vias 122 are preferably implemented.

[0016] In the example shown in FIG. 1, the battery 106 is connected to the inner top shield 120 via the control unit 104 (using the electrical connection 119), so that the control unit 104 can regulate the charge on the inner top shield 120 and the inner bottom shield 126. That is, the battery 106 is connected to power the control unit 104, and the control unit 104 applies charge to the inner top shield 120, the capacitive sense vias 122, and the inner bottom shield 130.

[0017] The capacitive sense vias 122 interpenetrate the PCB 112 from the top surface 110 to the middle-bottom surface 124. The capacitive sense vias 122 are electrically connected to the inner bottom shield 126. The inner bottom shield 126 is mounted on the bottom surface 124 of the PCB 112, covers an area of the middle-bottom surface 124 matching and aligned (e.g., vertically) with an area of the top surface 110 covered by the inner top shield 120, and is made of a conductive material selected to act as a capacitive plate and as EM shielding. A return line 128 electrically connects the inner bottom shield 126 to a channel of the control unit 104. As further described below, e.g., with respect to FIG. 2, there are preferably multiple capacitive sense vias 122, located within a perimeter of the top and bottom inner shields 120, 130 (viewing the system 100 looking towards and perpendicularly to the top surface 110, as in FIG. 2). The preferred arrangement of the vias 122, 132 can also be described as staggered placement of the capacitive sense vias 122 and ground vias 132, or analogized to an alternating crenellation (with ground vias 132 in the upper portions of crenellation notches, and capacitive sense vias 122 in lower portions of crenellation notches, or vice versa). From the preceding, therefore, one skilled in the art should now appreciate, as introduced earlier, that the inner top shield 120, capacitive sense vias 122, and inner bottom shield 126 (together referred to herein as the inner shield) together surround and enclose the secure enclosure 102.

[0018] The outer top shield 130 is mounted on the PCB 112 so that the outer top shield 130 surrounds and is near to, but not in electrical contact with, the inner top shield 120. That is, the inner top shield 120 is nested within the outer top shield 130. There are preferably no gaps in the outer top shield 130, or between the outer top shield 130 and the PCB 112, to prevent exterior access to the inside of the secure enclosure 102. The outer top shield 130, like the inner top shield 120, is made of a conductive material, preferably selected to act as a capacitive plate and as EM shielding. The inner and outer top shields 120, 130 can be mounted on the PCB using, for example, solder or mounting brackets which create a reliable electrical connection between the shields and power or ground (respectively).

[0019] The outer top shield 130 is connected to multiple ground vias 132, which are connected to a ground (not shown) located outside of the secure enclosure 102. The ground vias 132 interpenetrate the PCB 112 from the top surface 110 to the bottom surface 134. The ground vias 132 are electrically connected to the outer bottom shield 136. The outer bottom shield 136 is mounted on the bottom surface 134 of the PCB, covers an area of the bottom surface 134 matching and aligned (e.g., vertically) with an area of the top surface 110 covered by the outer top shield 130, and is made of a material selected to act as a capacitive plate and as EM shielding. The ground vias 132 are preferably disposed in a ring (i.e., surrounding alignment, but not necessarily circular) near the perimeter of the outer bottom shield 136. The capacitive sense vias 122 and the ground vias 132 are preferably “blind” vias. Accordingly, they are preferably not externally visible or physically accessible when the secure enclosure 102 is fully assembled (for example, a portion of the capacitive sense vias 122 connected to the middle-bottom surface 124 is covered by the inner bottom shield 126, and a portion of the ground vias 132 connected to the bottom surface 134 is covered by the outer bottom shield 136). The outer top shield 130, the ground vias 132, and the outer bottom shield 136 together surround and enclose the secure enclosure 102, the inner top shield 120, the capacitive sense vias 122, and the inner bottom shield 130.

[0020] Preferably, secure asset 108 devices are placed only on a side of the PCB 112 enclosed by the inner and outer top shields 120, 130. (In some embodiments, volumes which can fit secure assets 108 can be located on more than one side of the PCB 112, such as on both sides of a planar PCB 112.) Also, preferably, sensitive power planes and signal traces reside within the secure enclosure 102.

[0021] The inner top shield 120 and the outer top shield 130 act as a top plate capacitor, driven by the control unit 104 (powered by the battery 106) using the capacitive sense vias 122, and grounded by the ground vias 132. Similarly, the inner bottom shield 126 and the outer bottom shield 136 act as a bottom plate capacitor, driven by the battery 106 using the capacitive sense vias 122, and grounded by the ground vias 132. EM field lines run between the inner top shield 120 and the outer top shield 130, and between the inner bottom shield 126 and the outer bottom shield 136. The control unit 104 preferably controls the inner top shield 120, capacitive sense vias 122, and inner bottom shield 130 to charge and (partially) discharge at a high frequency, for example, 1 MHz.

[0022] The control unit 114 is configured to measure changes in capacitance of the top and bottom plate capacitors. An empty volume 138 between the inner and outer top shields 120, 130 or inner and outer bottom shields 126, 136 (PCB material, rather than an empty volume, is located between the bottom shields 126, 136 in the example shown in FIG. 1) can be filled using a dielectric material comprising air or another dielectric material, such as a dielectric material with increased capacitance and/or reduced production handling requirements and/or cost.

[0023] FIG. 2 shows an example plan and schematic view 200 of the system 100 of FIG. 1. From the above description and the plan view of FIG. 2, one skilled in the art will further appreciate that the outer perimeter of inner top shield 120 encloses each of the control unit 104, the battery 106, and the secure asset 108. Further, the plural capacitive sense vias 122 form a generally inner perimeter which, from FIG. 1, extends into the page from the perspective of FIG. 2, and that is located within the outer boundary (perimeter) of inner top shield 120 and within the outer boundary (perimeter) of outer top shield 130. Similarly, the plural ground vias 132 form a generally outer perimeter which, also from FIG. 1, extends into the page from the perspective of FIG. 2, and that is located outside the outer boundary (perimeter) of outer top shield 130 and/or overlapping the outer boundary (perimeter) of outer top shield 130.

[0024] In operation and as further detailed below with respect to FIG. 4, the control unit 104 can detect changes in capacitance as between shields 120, 126, 130, 136, for instance were such a change to occur based on an attempt to tamper with the system 100. Changes in capacitance measured by the control unit 104 can occur as a result of, for example, one of the shields 120, 126, 130, 136 being moved, removed, distorted, or deflected (changing distances between plates), drilled through or ablated (changing the size, and therefore total conductor area, of a

plate; and/or shorting the inner and outer plates if a drill bit is conductive), or charged by an exterior source (changing the charge on a plate). Changes in capacitance measured by the control unit 104 can also occur as a result of, for example, a drill bit (or other device for removing material) being used to access the inside of the secure enclosure 102 and drilling through or contacting a ground via 132 or a capacitive sense via 122 on the way; or an electrically conductive probe contacting one (or more) of the shields 120, 126, 130, 136 or the vias 122, 132.

[0025] As shown in FIG. 2, the capacitive sense vias 122 and the ground vias 132 are preferably arranged in closely spaced concentric geometries around a perimeter of the secure enclosure 102, with inner ring vias (capacitive sense vias 122) having alternating positions (staggered) with outer ring vias (ground vias 132), for example to prevent the PCB 112 from being drilled through by an attacker seeking access to the secure enclosure. (A break in the via rings, through which the connection 114 passes, is shown for clarity and simplicity. In preferred embodiments, the connection 114 is routed between the capacitive sense vias 122 and the ground vias 132 without a break in the via rings.) Also, the perimeter of the capacitive sense vias 122 is preferably within the perimeter of the top and bottom inner shields 120, 130, and the perimeter of the ground vias 132 is preferably within or overlaps the perimeter of the top and bottom outer shields 126, 136. Together, the shields 120, 126, 130, 136 and the vias 122, 132 thus provide a physical barrier against attacks attempting to physically access the secure enclosure, while allowing sufficient spacing to be arranged in or on the surface of the PCB 112 to pass power and/or signaling traces from the outside to the inside of the secure enclosure 102.

[0026] The outer shield is electrically connected and surrounds the secure enclosure 102 in three dimensions, forming a Faraday cage around the secure enclosure 102. That is, the outer shield will generally block EM fields originating outside the secure enclosure 102 from penetrating to affect the inside of the secure enclosure 102 (isolating the secure enclosure 102 from external galvanic and photonic signals). This means that the outer shield being connected to the system ground shields the secure enclosure 102 from EM-based attacks (such as electrical overvoltage stress), and from unintended EM interference (reducing noise within the secure enclosure 102). Thus, the control unit 104 is less sensitive to false tamper detection events, such as during system assembly or other intended end-user handling, because the outer shield being connected to system ground means that in ordinary handling, changes in capacitance in the top and bottom

plate capacitors will generally be caused only by removal of the top or outer bottom shield 126, 136.

[0027] In some embodiments, when the control unit 104 detects tampering (a change in capacitance in the top and/or bottom plate capacitors), it can cause the secure asset 108 to be disabled. For example, the secure asset 108 can be caused to delete sensitive data, make sensitive data unchangeable, or trigger a physically self-destructive event (for example, burning an entire array of programmable fuses to make data previously stored in a select portion of the fuses unreadable).

[0028] FIG. 3A shows a three-quarters perspective view 300 of an example implementation of a system 100 as shown in and described with respect to FIG. 1A. FIG. 3A shows the system 100 with the inner top shield 120 (not visible) and the outer top shield 130 covering the secure enclosure 102. Outer brackets 302 (partially visible) hold the outer top shield 130 in place against the PCB 112. The ground vias 132 are visible outside the perimeter of the outer top shield 130.

[0029] FIG. 3B shows a three-quarters perspective view 304 of the example system 100 implementation of FIG. 3A. In FIG. 3B, the outer top shield 130 is exploded away from the surface of the PCB 112 to reveal the inner top shield 120. Inner brackets 306 hold the inner top shield 120 in place against the PCB 112.

[0030] FIG. 3C shows a three-quarters perspective view 308 of the example system 300 implementation of FIG. 3A. In FIG. 3C, the outer top shield 130 and the inner top shield 120 are exploded away from the surface of the PCB 112 to reveal the secure enclosure 102. The capacitive sense vias 122 are visible within the perimeter of the inner top shield 120. (For clarity and simplicity, the inner and outer top shields 120, 130 are spaced relatively far apart in FIGs. 3A, 3B, and 3C. The capacitive sense vias 122 and ground vias 132 are preferably closer together than shown – for example, close enough to deter and/or prevent physical attack by drilling into the secure enclosure 102, as described above.) The control unit 104, the battery 106, and the secure asset 108 are also visible within the space comprising the secure enclosure 102 when the outer and inner top shields 120, 130 are fixedly attached to the PCB 112.

[0031] As shown in FIGs. 3A, 3B, and 3C, when the outer and inner top shields 120, 130 are fixedly attached to the PCB 112 by the outer and inner brackets 302, 306, the conductive structural inner volume (120, 122, 126, 128) is capacitively coupled to the conductive structural

outer volume (130, 132, 136). Accordingly, changes in the capacitance between the conductive structural inner volume (120, 122, 126, 128) and the conductive structural outer volume (130, 132, 136) (as measured by the capacitive sensor in the control unit 104) indicate tampering such as attempts to physically or electrically access the inside of the secure enclosure 102.

[0032] FIG. 4 shows an example of a process 400 for tamper detection using capacitive sensing. In step 402, a volume containing a secure asset (for example, circuitry) is enclosed within an inner shield, the inner shield including a charged inner capacitive plate coupled to a charge source within the volume, and capacitive sense vias coupling the inner capacitive plate to a capacitive sensor located within the volume. In step 404, the volume and the inner shield are enclosed within an outer shield, the outer shield including a grounded outer capacitive plate, and ground vias coupling the outer capacitive plate to a ground, the outer shield not touching the inner shield. In step 406, a capacitance between the inner capacitive plate and the outer capacitive plate is measured using the capacitive sensor. In step 408, the circuitry is operated in dependence on the measuring – for example, if a measured change in capacitance is detected, then tampering is thusly presumed as the cause and a portion of the secure asset is caused to become inoperable. Also, a reporting element can be triggered when tampering is detected. For example, an alarm can be activated, information about the detected change in capacitance can be stored in storage within the secure enclosure, or a signal indicating the detected tampering can be sent to the outside of the secure enclosure.

[0033] Modifications are possible in the described embodiments, and other embodiments are possible, within the scope of the claims.

[0034] In some embodiments, there is more than one electrical connection between the inside and the outside of the secure enclosure.

[0035] In some embodiments, there is a direct electrical connection between the exterior of the secure enclosure and the secure asset.

[0036] In some embodiments, there is no electrical connection between the inside and the outside of the secure enclosure.

[0037] In some embodiments, power requirements of the control unit and secure asset are small. In some embodiments in which the secure enclosure is isolated from power sources outside of the secure enclosure, a small battery, such as a coin cell battery, can be used.

[0038] In some embodiments, only one of the inner top and outer shields comprises

electromagnetic shielding. In some embodiments, only one of the bottom inner and outer shields comprises electromagnetic shielding.

[0039] In some embodiments, I/O between the secure enclosure and the exterior is routed through the control unit. In some embodiments, the control unit is not connected to communicate with the secure asset. In some embodiments, the control unit is not electrically connected to the secure asset.

[0040] In some embodiments, an MSP430FR2633 or other MSP430 CapTivate enabled device comprises or is used in a control unit. These devices are commercially available from Texas Instruments.

[0041] In some embodiments, the secure enclosure can contain, for example, one or more of: a processor, a memory, or a communications device.

[0042] In some embodiments, more than two via rings are used. In some embodiments, vias are arranged other than in a ring.

[0043] In some embodiments, tamper sensors in addition to the control unit are used, such as photon or pressure sensors.

[0044] In some embodiments, the battery is selected to be large enough to last for a projected lifetime of the secure asset. In some embodiments, the battery's lifetime defines the useful lifetime of the secure asset. In some embodiments, power is supplied by wires extending from the outside to the inside of the secure enclosure. That is, the charge source for charging the top and bottom inner shields can be powered by a power source outside the secure enclosure, and connected to the control unit by, for example, the connection.

[0045] In some embodiments, capacitive sensing and data protection (such as a hardware-level security key) can be implemented on the same device.

[0046] In some embodiments, one or more of the outer top shield, the inner top shield, the outer bottom shield, and the inner bottom shield, is detachable. In some embodiments, one or more of the outer top shield, the inner top shield, the outer bottom shield, and the inner bottom shield, is not detachable (for example, is soldered onto the PCB or is connected to the PCB using an adhesive).

[0047] In some embodiments, voltage, temperature, and humidity monitoring subsystems can be included in a tamper detection system, insider or outside of the secure enclosure, to assist in detecting physical tamper attacks, and/or to provide measurements which can be analyzed to

compensate for environmental factors which can affect capacitance measurements. In some embodiments, these subsystems are located inside the secure enclosure for use in conjunction with the capacitance measurement system. In some embodiments, these subsystems are integrated into the control unit (for example, integrated into an integrated circuit which includes capacitance measurement circuits). In some embodiments, the timing of capacitance measurements, and/or the timing of activating voltage, temperature, and humidity monitoring subsystems, can be controlled to appear non-deterministic to an attacker, for example, using random or pseudorandom timing for measurement polling events.

[0048] In some embodiments, devices within the secure enclosure are powered only by a battery or other energy storage fully contained within the secure enclosure. In some embodiments, devices within the secure enclosure can receive power from outside the secure enclosure.

[0049] In some embodiments, the secure asset and/or the control unit is programmable from outside of the secure enclosure. In some embodiments, the secure asset can be reprogrammed by the control unit. In some embodiments, the control unit can be reprogrammed by the secure asset.

[0050] In some embodiments, an inner shield and an outer shield fully surround the PCB (or other platform on which the secure asset is mounted). In some such embodiments, there is only one inner shield and only one outer shield. In some such embodiments, the shields alone (without the PCB) are sufficient to surround and enclose the secure enclosure.

[0051] In some embodiments, the control unit changes the operation of the secure asset (for example, causing reprogramming or destruction of portions or all of the secure asset) if a change in capacitance between the inner and outer plate capacitors is greater than a threshold. In some embodiments, the threshold is dependent on a state of charging the inner plate capacitor or on environmental factors (such as sensed voltage, temperature, and humidity).

[0052] In some embodiments, the charge source for the inner capacitive plate is other than a battery.

[0053] In some embodiments, the inner top shield and the outer top shield are shaped as five-sided boxes, as N-sided polyhedra with N-1 closed sides, or as continuous portions of a sphere.

[0054] In some embodiments, the electrical connection between the inside and outside of the secure enclosure can be configured to provide into the secure enclosure (from a communications node outside of the secure enclosure to which the electrical connection is connected) one or more

of power, control signals for the circuitry and/or the capacitive sensor, or data for use in operation of the circuitry and/or the capacitive sensor.

[0055] In some embodiments, ground vias and/or capacitive sense vias are larger or smaller. In some embodiments, more or fewer ground vias and/or capacitive sense vias are used.

[0056] In some embodiments, polyhedral shapes made of conductive material, including polyhedral shapes other than rectangular parallelepipeds, which open on one or more faces and configured to fixedly or removeably attach to the PCB without a gap in the shape or between the shape and the PCB, can be used as shields (capacitive plates).

[0057] In some embodiments, inner and outer bottom shields are mounted on the bottom surface and enclose an empty volume, similarly to the inner and outer top shields. In some such embodiments, circuitry is located within the empty volume enclosed by the inner and outer bottom shields.

[0058] In some embodiments, there are gaps in one or more of the inner top shield, the outer top shield, the inner bottom shield, or the outer bottom shield, or between one or more of the shields and the PCB (or other platform on which devices in the secure enclosure are mounted), such that the gaps are too small for an attacker to use to gain access to the inside of the secure enclosure.

[0059] In some embodiments, the control unit uses different (or randomized) frequencies to charge and discharge the inner shield (the top and bottom inner plate and the capacitive sense vias).

[0060] In some embodiments, the outer shield is electrically coupled to a ground, but is not at a voltage of the ground. For example, the outer shield can be electrically coupled to a ground via a resistor and/or one or more other impedance elements. In some embodiments, the outer shield is configured so that there is an electric potential difference between the outer shield and the inner shield (for example, other than a potential difference corresponding to a charged inner shield and a grounded outer shield).

[0061] In some embodiments, a conductive structural inner volume does not include capacitive sense vias and/or an inner bottom plate. In some embodiments, a conductive structural outer volume does not include ground vias and/or an outer bottom plate. In some embodiments, different capacitive sensors measure capacitance with respect to inner and outer top plates than with respect to inner and outer bottom plates and/or with respect to ground vias and capacitive sense vias.

[0062] In some embodiments, the outer shield(s) can be coated and/or covered with a non-conductive material. In some embodiments, exposed portions of vias can be coated and/or covered with a non-conductive material.

[0063] In some embodiments, the secure enclosure is hermetically sealed.

[0064] In some embodiments, the secure enclosure and/or the empty volume is wholly or partially filled with a non-conductive material, such as a potting material (encapsulation material).

[0065] In some embodiments, a key can be transmitted into the control unit from outside the secure enclosure which disables at least part of the control unit functionality; for example, to allow for intended access to the interior of the secure enclosure.

[0066] In some embodiments, capacitive sense vias can be located outside the perimeter of the inner top and/or bottom shields and within the perimeter of the outer top and/or bottom shields. In some embodiments, capacitive sense vias can be located to overlap the perimeter of the inner inner top and/or bottom shields. In some embodiments, ground vias can be located inside the perimeter of the outer top and/or bottom shields and within the perimeter of the inner top and/or bottom shields.

[0067] In some embodiments, no return line is used. In some embodiments, the battery and the control unit are coupled to the ground via the capacitive coupling between the inner and outer shields.

[0068] In some embodiments, the inner top plate is driven (charged) separately from the inner bottom plate and/or the capacitive sense vias. That is, the inner top plate, the inner bottom plate, and the capacitive sense vias can be driven using separate channels from the capacitive sensor (or otherwise directly or indirectly from the battery or other charge source). Power can also be distributed on the same or additional separate channel(s) to other devices within the secure enclosure.

[0069] In some embodiments, the connection uses a medium other than electricity through a wire to transmit signals, e.g., photonic or galvanic signal transmission.

[0070] In some embodiments, the capacitive sense vias are capacitively coupled to the ground vias.

CLAIMS

What is claimed is:

1. An enclosure for circuitry, comprising:
 - a platform to which the circuitry is fixedly coupled;
 - a charge source;
 - a first capacitive plate fixedly coupled to the platform, and either alone, or together with the platform, surrounding a volume containing the circuitry and the charge source, the charge source electrically coupled to and configured to charge the first capacitive plate;
 - a second capacitive plate fixedly coupled to the platform without touching the first capacitive plate, and either alone, or together with the platform, surrounding the first capacitive plate, the second capacitive plate configured so that there is an electric potential difference between the first capacitive plate and the second capacitive plate; and
 - a capacitive sensor electrically connected to the first capacitive plate and configured to determine when a capacitance between the first and second capacitive plates is changed.
2. The enclosure of claim 1, wherein the second capacitive plate is electrically coupled to a ground.
3. The enclosure of claim 1,
 - wherein the first capacitive plate includes a first top portion;
 - wherein the charge source, the circuitry, and the first top portion are fixedly coupled to a surface of the platform;
 - wherein the second capacitive plate includes a second top portion, the first top portion being nested within the second top portion;
 - wherein the first capacitive plate includes a first bottom portion fixedly coupled to a portion of the platform which is displaced in a direction orthogonal to, and towards an interior of the platform from, the surface; and
 - wherein the second capacitive plate includes a second bottom portion fixedly coupled to a portion of the platform which is displaced, more than the first bottom portion, in a direction orthogonal to, and towards an interior of the platform from, the surface;
 - further comprising multiple capacitive sense vias coupling the first top portion to the first bottom portion, and multiple ground vias coupling the second top portion to the second bottom portion.

4. The enclosure of claim 3, wherein the ground vias are arranged in a ring, to form a ring of ground vias, around a perimeter of the volume.

5. The enclosure of claim 4, wherein the capacitive sense vias are arranged in a ring concentrically within the ring of ground vias, and wherein the capacitive sense vias are close to and in alternating position with the ground vias.

6. The enclosure of claim 3, wherein the ground vias and/or the capacitive sense vias are arranged around a perimeter of the volume such that drilling into the volume without contacting at least one of the first capacitive plate, the second capacitive plate, the ground vias, and the capacitive sense vias, is prevented.

7. The enclosure of claim 1, further comprising:
a communications node not surrounded by the first capacitive plate or the second capacitive plate, the communications node configured to receive an electronic signal; and
a communications line electronically coupling the capacitive sensor and/or the circuitry to the communications node.

8. The enclosure of claim 7, wherein the electronic signal can include one or more of power, control signals for the circuitry and/or the capacitive sensor, data for use in operation of the circuitry and/or the capacitive sensor, or programming for the capacitive sensor.

9. The enclosure of claim 1, wherein the first capacitive plate either alone, or together with the platform, surrounds the volume without gaps, and wherein the second capacitive plate either alone, or together with the platform, surrounds the first capacitive plate without gaps.

10. The enclosure of claim 1, wherein at least one of the first capacitive plate and the second capacitive plate is configured to shield the volume against electric and/or magnetic fields.

11. The enclosure of claim 1, wherein the first and second capacitive plates are shaped as five-sided boxes, as N-sided boxes with N-1 closed sides, or as portions of a sphere.

12. The enclosure of claim 1, wherein the capacitive sensor is configured to cause a specified portion of the circuitry to become inoperable if the capacitive sensor detects the capacitance between the first and second capacitive plates is changed, more than by a threshold amount of change, and other than by the charge source.

13. The enclosure of claim 1, wherein the circuitry and the capacitive sensor are configured not to receive power from outside of the volume.

14. The enclosure of claim 1, wherein the charge source is configured to be powered via an electrical coupling between the charge source and a power node outside the volume, the power node configured to receive power.

15. A method of protecting circuitry from tampering, the method comprising:
enclosing, within an inner shield, a volume which contains the circuitry, the inner shield including a charged inner capacitive plate coupled to a charge source within the volume, and capacitive sense vias coupling the inner capacitive plate to a capacitance sensor;
enclosing, within an outer shield, the volume and the inner shield, the outer shield including a grounded outer capacitive plate, and ground vias coupling the outer capacitive plate to a ground, the outer shield not touching the inner shield;
measuring a capacitance between the inner capacitive plate and the outer capacitive plate using a sensor located within the volume; and
operating the circuitry in dependence on the measuring.

16. The method of claim 15, wherein the operating includes causing a specified portion of the circuitry to become inoperable if the capacitive sensor detects the capacitance between the first and second capacitive plates is changed other than by the charge source.

17. The method of claim 16, wherein the causing a specified portion of the circuitry to become inoperable includes one or more of deleting specified data, making specified data unchangeable, or inducing a physically self-destructive event.

18. The method of claim 16, wherein the capacitance being changed other than by the charge source is determined in dependence on a comparison between the capacitance and a threshold.

19. The method of claim 15, wherein a polling frequency of a capacitance between the inner shield and the outer shield is random and/or pseudo-random.

20. The method of claim 15, further comprising shielding the volume against electric and/or magnetic fields using the inner shield and the outer shield.

21. The method of claim 15, further comprising measuring one or more of voltage, temperature, and humidity, and compensating in the measuring step for a measured voltage, temperature, and/or humidity.

22. The method of claim 15, wherein the charge source is powered by a power source outside the volume.

23. A method of protecting circuitry from tampering, the method comprising:

wherein an inner shield encloses a volume which contains the circuitry, the inner shield including a charged inner capacitive plate coupled to a charge source within the volume, and capacitive sense vias coupling the inner capacitive plate to a capacitance sensor;

wherein an outer shield encloses the volume and the inner shield, the outer shield including a grounded outer capacitive plate, and ground vias coupling the outer capacitive plate to a ground, the outer shield not touching the inner shield;

measuring a capacitance between the inner capacitive plate and the outer capacitive plate using a sensor located within the volume; and

operating the circuitry in dependence on the measuring.

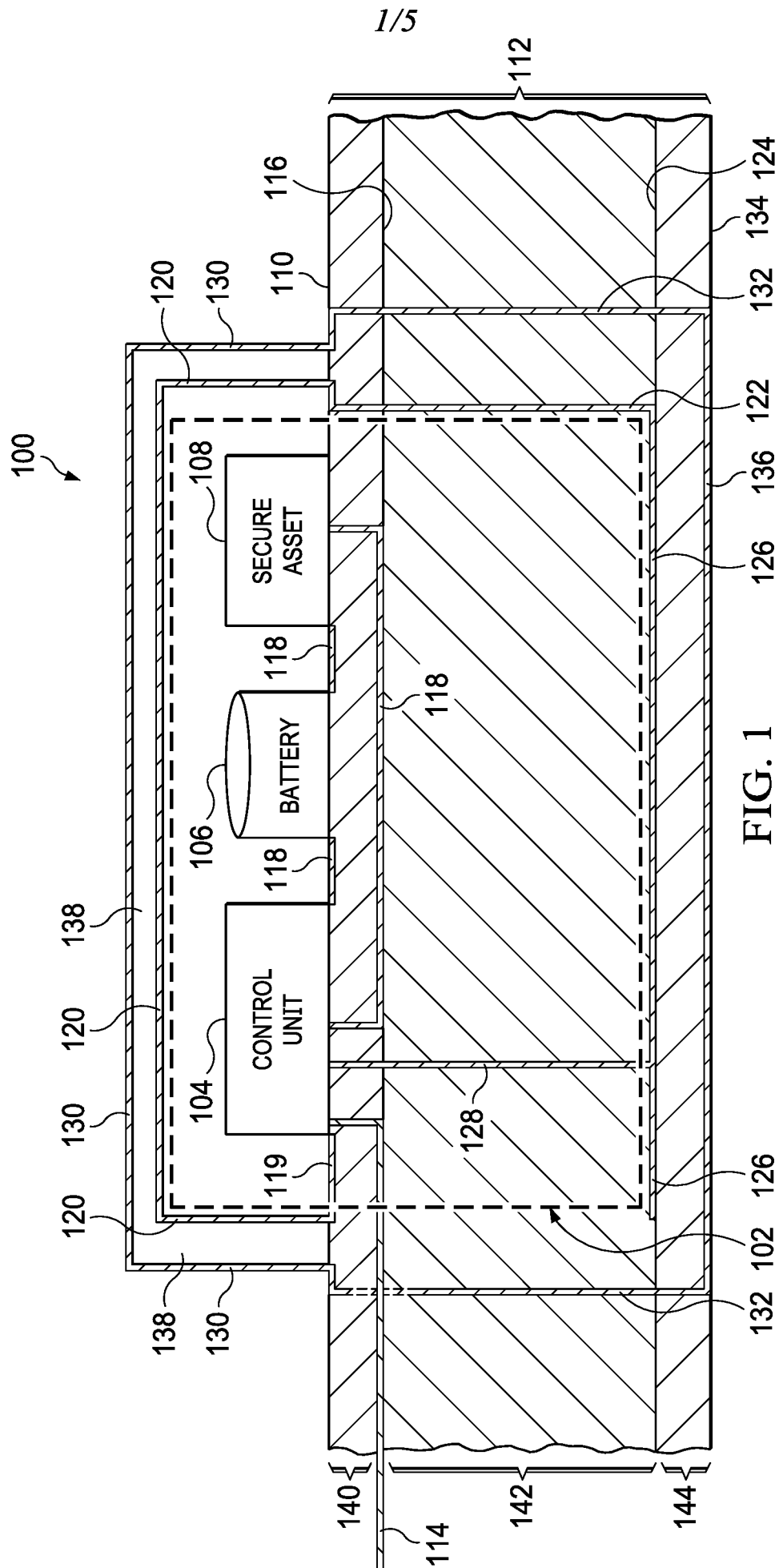


FIG. 1

2/5

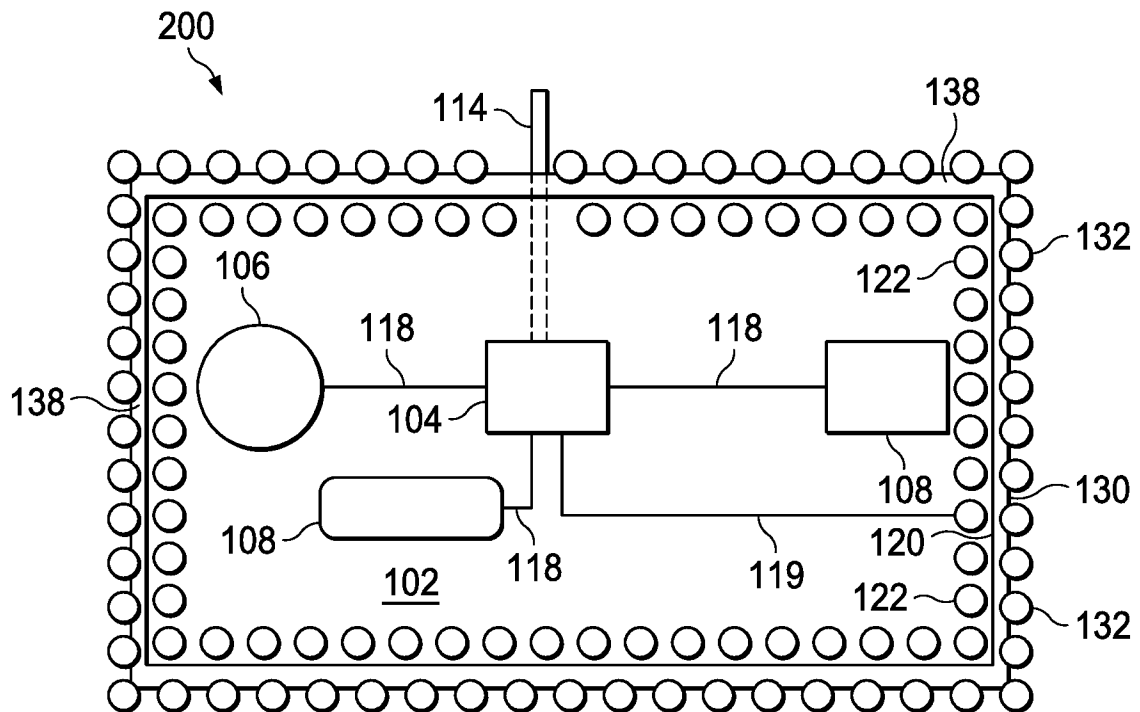


FIG. 2

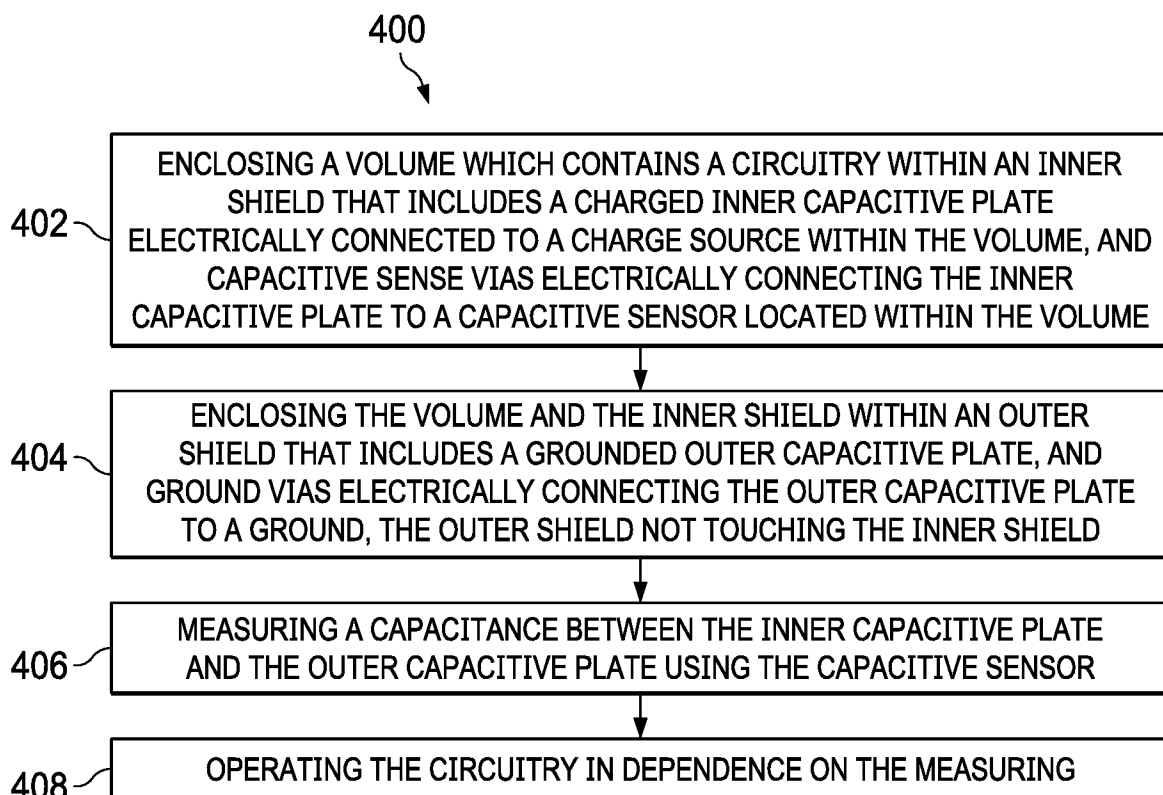


FIG. 4

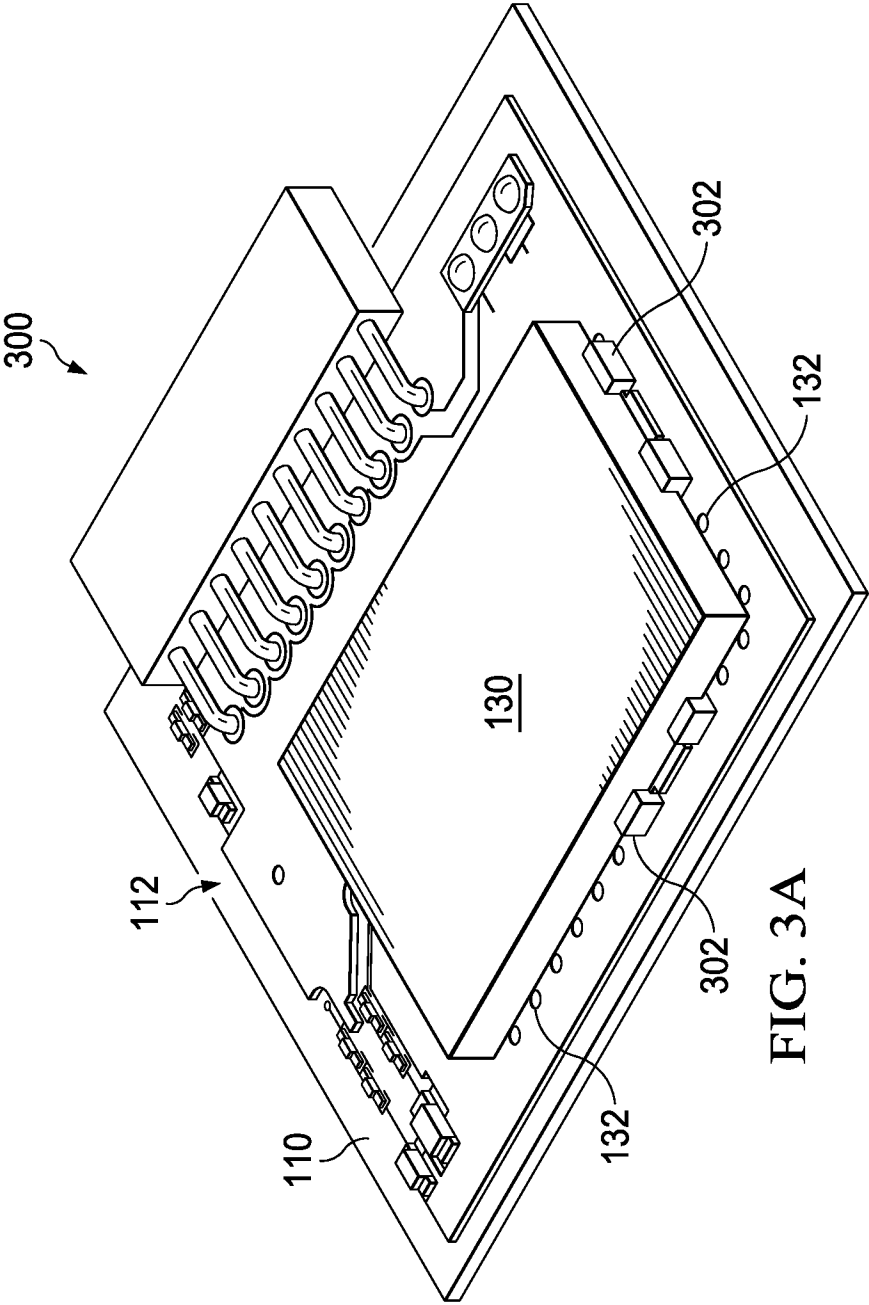
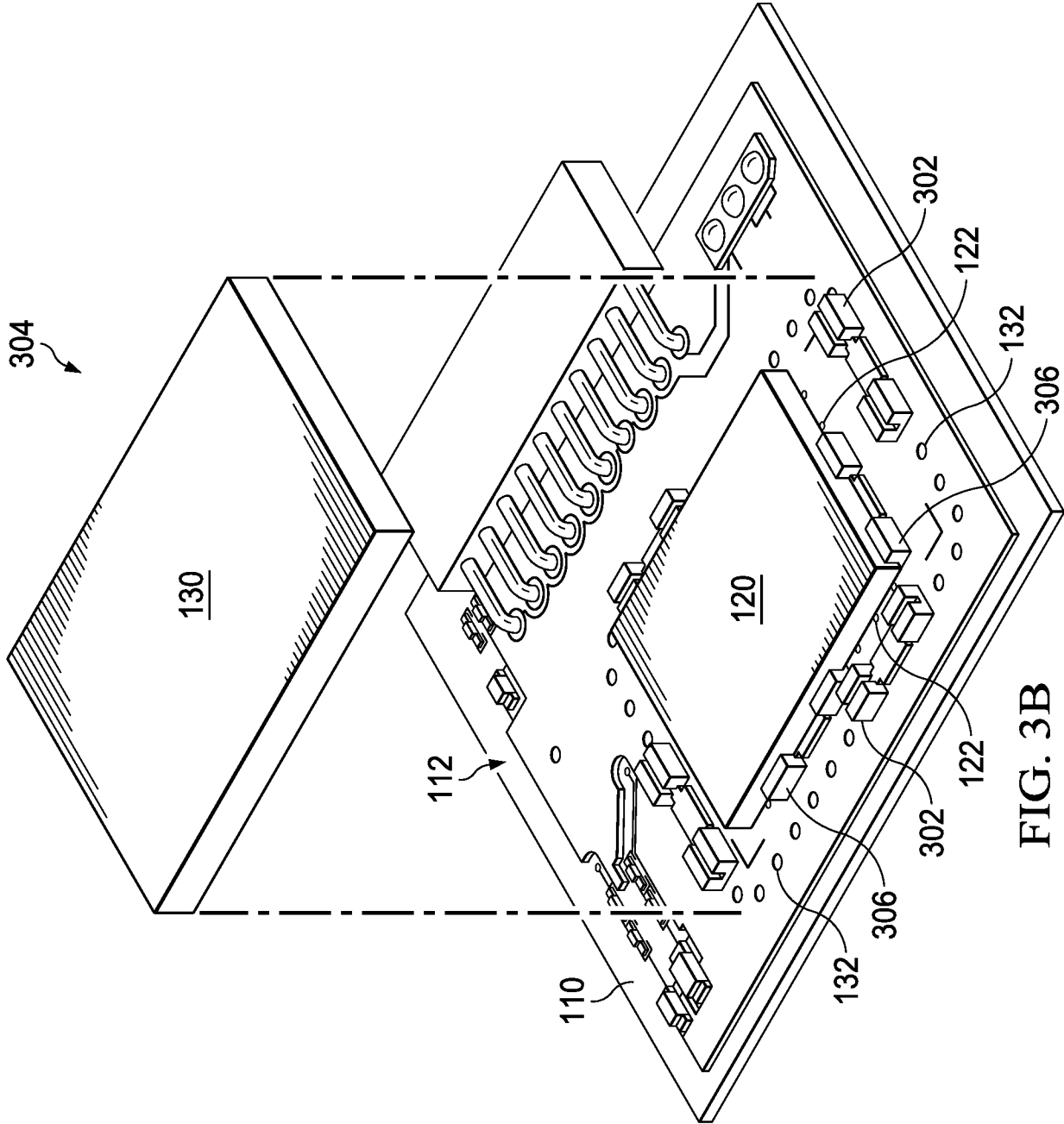


FIG. 3A



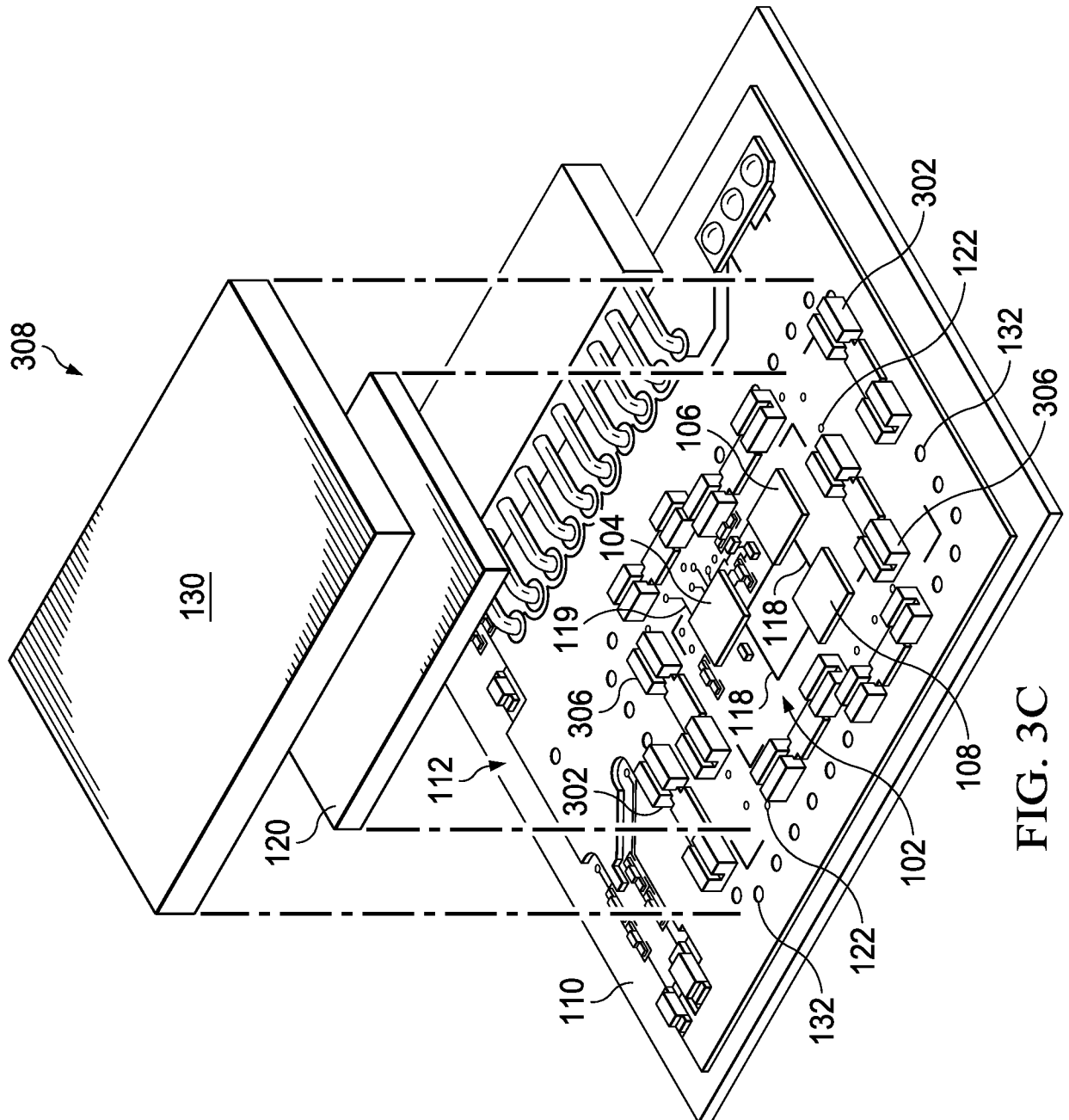


FIG. 3C

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2020/015569

A. CLASSIFICATION OF SUBJECT MATTER		
<i>G08B 13/12 (2006.01)</i> <i>G08B 13/22 (2006.01)</i> According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
G08B 13/12, 3/22		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
PatSearch (RUPTO internal), USPTO, PAJ, Esp@cenet, Information Retrieval System of FIPS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 1999/021142 A1 (W. L. GORE & ASSOCIATES (UK) LIMITED) 29.04.1999, fig.1, ref. sign 22. p.7 lines 7-10, p.7 lines 1-10, fig.1,5, p.3 lines 26-28	1-3, 6-23 4, 5
Y	WO 2012/155057 A2 (THE TRUSTEES OF DARTMOUTH COLLEGE) 15.11.2012, abstract, paragraphs [0009], [0028]	4, 5
A	GB 2256956 A (WL GORE AND ASSOCIATES UK LTD) 23.12.1992	1-23
A	GB 2174830 A (CLARK DAVID) 12.11.1986	1-23
☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents: “A” document defining the general state of the art which is not considered to be of particular relevance “E” earlier document but published on or after the international filing date “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) “O” document referring to an oral disclosure, use, exhibition or other means “P” document published prior to the international filing date but later than the priority date claimed “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art “&” document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
25 May 2020 (25.05.2020)		28 May 2020 (28.05.2020)
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37		Authorized officer S. Zhuravlev Telephone No. (495) 531-64-81