(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
05 March 2020 (05.03.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/046875 A1

(51) International Patent Classification:
G06F 21/86 (2013.01) *H01L 23/00* (2006.01)

(21) International Application Number:
PCT/US2019/048258

(22) International Filing Date:
27 August 2019 (27.08.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/724,581 29 August 2018 (29.08.2018) US
16/293,543 05 March 2019 (05.03.2019) US

(71) Applicant: **VAREX IMAGING CORPORATION** [US/US]; 1678 S. PIONEER ROAD, SALT LAKE CITY, Utah 84104 (US).

(72) Inventors: **MEILER, Michael R.**; 1678 S. Pioneer Road, Salt Lake City, Utah 84104 (US). **YOON, Inwoo**; 1678 S. Pioneer Road, Salt Lake City, Utah 84104 (US). **JOLLEY, Lincoln C.**; 1678 S. Pioneer Road, Salt Lake City, Utah 84095 (US). **GINZTON, Christopher D.**; 1678 S. Pioneer Road, Salt Lake City, Utah 84104 (US).

(74) Agent: **WILDING, David**; 1678 S. Pioneer Road, Salt Lake City, Utah 84104 (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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

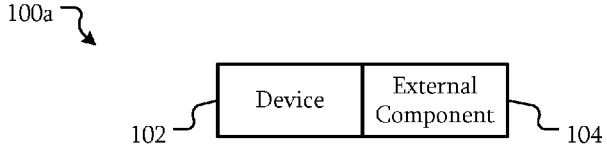
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, 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 the identity of the inventor (Rule 4.17(i))*

Published:
— *with international search report (Art. 21(3))*

(54) Title: ANTI-TAMPER CIRCUITRY

FIG. 1A



(57) Abstract: Embodiments include a device, comprising: a mounting structure configured to mount the device to an external component; first circuitry; and anti-tamper circuitry electrically connected to the first circuitry and configured to disable at least one function of the first circuitry when the device is removed from the external component and methods of operating the device.

WO 2020/046875 A1

ANTI-TAMPER CIRCUITRY

BACKGROUND

[001] Systems may be formed from a variety of different devices. Manufacturers, system integrators, or the like may design and install a particular system with authorized components. However, a third-party supplier may swap devices on similar systems, install used components, or third-party components that may lead to performance issues and/or damage to components of the system.

BRIEF DESCRIPTION OF THE DRAWINGS

[002] FIGS. 1A-1C are block diagrams of systems including a device with anti-tamper circuitry according to some embodiments.

[003] FIG. 2 is a block diagram of a device with anti-tamper circuitry according to some embodiments.

[004] FIGS. 3A-3C are block diagrams of circuitry of devices with anti-tamper circuitry according to some embodiments.

[005] FIG. 4A-4B are cross-sectional diagrams illustrating mounting a device with anti-tamper circuitry on an external component according to some embodiments.

[006] FIGS. 5A-5D are schematic diagrams of circuitry of anti-tamper circuitry according to some embodiments.

[007] FIGS. 6A and 6B are flowcharts showing techniques of operating a device with anti-tamper circuitry according to some embodiments.

[008] FIG. 7 is a block diagram of an x-ray system according to some embodiments.

[009] FIG. 8A-8B are block diagrams of systems including an authorization system according to some embodiments.

[010] FIGS. 9A-10C are flowcharts showing examples of techniques of operating an authorization system according to some embodiments.

DETAILED DESCRIPTION OF SOME EXAMPLE EMBODIMENTS

[011] Before any embodiments of the invention are explained in detail, it is to be understood that the invention is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the following drawings. The invention is capable of other embodiments and of being practiced or of being carried out in various ways. Numbers provided in flow charts and processes are provided for clarity in illustrating steps and operations and do not necessarily indicate a particular order or sequence. Unless otherwise defined, the term "or" can refer to a choice of alternatives (e.g., a disjunction operator, or an exclusive or) or a combination of the alternatives (e.g., a conjunction operator, and/or, a logical or, or a Boolean OR).

[012] Some embodiments relate generally to mechanisms, methods, and systems to disable component authentication system when removed from a component. Some embodiments relate generally to switches and disabling components and/or circuitry.

[013] Electronic devices may be used in an attempt to block the use of third-party components in systems such as computed tomography (CT) and x-ray systems. However, such electronic devices may be removed from systems including old, broken, worn out components, such as x-ray tubes. The electronic devices may then be installed on third-party or used tubes to be sold for use in an original equipment manufacturer (OEM) system. For example, a third-party may access an old, used, or broken x-ray tube from which the electronic devices can be removed. The electronic device can then be installed on a new, used, or third-party tube to enable the tube to simulate a genuine tube in the system.

[014] As described herein, anti-tamper circuitry may not prevent the removal of the components or the electronic devices themselves but may disable at least some to all of the functionality of the device such as disabling authentication or other functions, deleting configuration information, or the like. As a result, the electronic device may not be able to perform those functions without having a manufacturer or authorized service representative reprogram the device. Thus, an unauthorized party may no longer be able

to reuse the electronic device and access some to all of the functionality. As will be described in further detail below, the effect of the loss of some to all of the functionality may result in a range of effects from a warning message to disabling of the electronic device or a system including the electronic device.

[015] In some embodiments, in an x-ray system, an x-ray tubes designed and built by the manufacturer may include tube specific information to be used in conjunction with a tube auxiliary unit (TAU) to function with proper imaging and without damage to the tube. That tube specific information may reside in non-volatile random-access memory (NVRAM), such as flash memory or solid-state storage, of the TAU. Since some of the information stored in the TAU is tube specific, if its TAU were to be swapped to a different tube, its tube specific information would no longer match the specific x-ray tube. The mismatch could cause image quality issues and/or irreparable x-ray tube damage if used. The anti-tamper circuitry may reduce or eliminate a chance that the TAU is swapped between different x-ray tubes and providing the incorrect tube specific information to a system.

[016] FIGS. 1A-1C are block diagrams of systems including a device with anti-tamper circuitry according to some embodiments. FIG. 2 is a block diagram of a device with anti-tamper circuitry according to some embodiments.

[017] Referring to FIGS. 1A and 2, the system 100a includes a device 102 configured to be mounted to an external component 104. The device 102 includes anti-tamper circuitry 110 and circuitry 112.

[018] Examples of the device 102 include devices with circuitry 112 that may include customized components, firmware, software, data or the like. The firmware or software may include instructions that implement proprietary communication and/or control techniques with other circuitry 122 or circuitry 120 of the external component 104. In other embodiments, the data may include authentication information, cryptographic information, performance data, or the like. Particular examples of the device 102 include an authentication circuit for a system, a control circuity for an x-ray tube, or the like.

[019] The external component 104 may include a purely structural component and/or a circuity with some functional capabilities. For example, in some embodiments, the external component 104 is a housing of a system that includes the device 102. The device 102 may be mounted to that housing and hence, mounted to the external component 104.

[020] The device 102 includes a housing 116 configured to restrict access to disarm the disarm the anti-tamper circuitry 110 when the device 102 is mounted to the external component 104. For example, the housing 116 may include a sealed case surrounding the anti-tamper circuitry 110 and the circuitry 112. When the housing 116 is mounted to the external component 104, the combination of the housing 116 and the external component 104, such as a wall 124 of the external component 104, may completely enclose the anti-tamper circuitry 110 and the circuitry 112. In some embodiments, the combination may enclose the anti-tamper circuitry 110 and the circuitry 112 sufficiently to prevent access to the anti-tamper circuitry 110 or the circuitry 112 without significantly modifying or destroying the housing 116. The combination of the housing 116 and the external component 104 may be configured such that accessing the anti-tamper circuitry 110 or the circuitry 112 is significantly more difficult than removing the device 102 from the external component 104.

[021] The device 102 includes anti-tamper circuitry 110 electrically connected to circuitry 112. The anti-tamper circuitry 110 is configured to disable at least one function of the circuitry 112 when the device 102 is removed from the external component 104. In particular, the anti-tamper circuitry 110 is coupled to the external component 104 through coupling 114. This coupling 114 may be a mechanical, electrical, optical, magnetic, other similar couplings, or a combination of such couplings. For example, a switch may be switched when the device 102 is mounted on the external component 104. Switched can refer to either toggling from an on state to an off state or toggling from an off state to an on state. The switch may have a mechanically or magnetically switchable pole. A state of the switch may change depending on whether the device 102 is a mounted on the external component 104 or if it is being removed from the external component. In other embodiments, the switch may change state when a fastener that is

used to mount the device 102 on the external component is removed. In other embodiments, an electrical circuit may be created through a portion of the external component 104, such as through a metallic portion of the wall 124. Removal of the device 102 from the external component may be detected by a break in that circuit. Although some circuits and structures have been used as examples of configurations by which the anti-tamper circuitry 110 may sense the removal of the device 102 from the external component 104, the anti-tamper circuitry 110 may sense the removal in other ways.

[022] Embodiments described herein may be used anywhere where a device 102 should stay physically paired to the system 100a, the external component circuitry 120, the other circuitry 122, or another component or device to which they are mounted and/or associated. Paired in this sense could mean physically in touch, in proximity, in communication with, integrated into the device, or the like.

[023] In response to sensing the removal of the anti-tamper circuitry 110 from the external component 104, the anti-tamper circuitry 110 may be configured to disable at least one function of the circuitry 112. The particular function of the circuitry 112 may include a capability of general processing, the use of particular data, the ability to properly respond to authentication challenges, or the like. In some embodiments, data stored in the circuitry 112 may be erased. The data may include cryptographic information, authentication information, identification information, operational information, firmware, software, or the like. In some embodiments, non-volatile memory of the circuitry 112 may be erased to disable at least one function. In other embodiments, fuses that affect operation of the circuitry 112 may be blown to disable at least one function. While some embodiments may disable at least one function, in other embodiments, the anti-tamper circuitry 110 may be configured to disable all functions of the circuitry 112 or the entire device 102.

[024] In some embodiments, the circuitry 112 is configured to control the external component. The circuitry 112 may be coupled to the external component circuitry 120. In a particular example, the circuitry 112 may include control circuitry for an x-ray tube.

The external component circuitry 120 may include an anode, cathode, filament, emitter, motor, steering electronics, focusing electronics, or other circuitry that may be part of an x-ray tube.

[025] In some embodiments, other techniques for preventing reuse could be triggered by radio-frequency identification sensors (RFID), light sensors, proximity sensors, bar code readers, cameras that process the tube serial number or other identifying features, trip wires, tamper resistant mounting, or any combination of such techniques. These techniques could be paired with the ability of the anti-tamper circuitry 110 to disable at least one function of the circuitry 112 as described herein.

[026] Referring to FIGS. 1B and 2, in some embodiments, the external component 104 may be another device 106. For example, the device 106 may be an interface circuit board configured to provide an interface between a system control component and other components of the system. In a particular example, the device 106 may be an interface board that converts controls and/or communication between the system controller for an x-ray system and particular sub-systems, such as an x-ray generation subsystem, a power sub-system, a detector sub-system, a cooling subsystem, a user interface sub-system, or the like.

[027] The device 102 may be an authentication daughter board (ADB) configured to store authentication information, perform authentication functions, negotiate authentication between a system controller and the device 106 or other sub-systems of the system 100b, or the like.

[028] Referring to FIG. 1C, in some embodiments, more than one device 102 may be mounted on the external component 104. In this example, N devices 102 are mounted on the external component 104. The devices 102-1 to 102-N may be the same, similar, or different. However, some to all of the devices 102-1 to 102-N may include the anti-tamper circuitry 110 described herein.

[029] In some embodiments, the anti-tamper circuitry 110 prevents the reuse, modification, tampering, replacement, or reinstallation of the device 102, by a third-party or onto a third-party component. As described above, the device 102 may be part of an

authentication system. The authentication system may be configured to determine whether or not a component in the system, which may be the device 102, the external component 104, or another component, is a genuine manufacturer or OEM component by issuing an encrypted challenge question to a cryptographic electronic device on the component.

[030] In a particular example, the device 102 may include the cryptographic electronic device as part of the circuitry 112. The device 102 includes the circuitry that controls the external component 104. If the cryptographic electronic device can be removed from the genuine component and installed on a counterfeit component, then the authentication system can be defeated. However, the anti-tamper circuitry 110 is triggered upon removal of the device 102. The at least one function of the circuitry 112 that is disabled may include the authentication functions, authentication information, or the like. After the anti-tamper circuitry 110 is triggered, the cryptographic electronic device would no longer respond properly to authentication requests. As a result, the system 100 would have an indication that the device 102 and/or external component 104 can no longer be trusted to be a genuine manufacturer or OEM component.

[031] In some embodiments, service contracts may be a large source of revenue for an OEM. Anti-tamper circuitry 110 as described herein may be used by the OEM to reduce or eliminate an ability of third-party manufacturers or resellers to install competing or replacement products, or incompatible components that can result in performance and patient safety issues.

[032] FIGS. 3A-3C are block diagrams of circuitry of devices with anti-tamper circuitry according to some embodiments. In these embodiments, the circuitry includes anti-tamper circuitry 110 similar to that described above, a processor 113, and a memory 118. The processor 113 and memory 118 are examples of circuitry 112 described above.

[033] The processor 113 may be a general-purpose processor, a digital signal processor (DSP), an application specific integrated circuit, a microcontroller, a programmable logic device, discrete circuits, a combination of such devices, or the like. The processor 113 may include internal portions, such as registers, cache memory, volatile memory, non-

volatile memory, processing cores, or the like, and may also include external interfaces, such as address and data bus interfaces, interrupt interfaces, or the like. Although only one processor 113 is illustrated, multiple processors 113 may be present. In addition, other interface devices, such as logic chipsets, hubs, memory controllers, communication interfaces, or the like may be included to connect the processor 113 to internal and external components.

[034] The processor 113 is coupled to the memory 118. The memory 118 includes data such as cryptographic information, authentication information, identification information, operational information, firmware, software, or the like as described above. The anti-tamper circuitry 110 is configured to erase at least a portion of the memory 118 used by the processor 113 when the device 102 is removed from the external component 104. In some embodiments, the erasure may be of all of such data. In other embodiments, the erasure may be of a sufficient quantity and quality of the data to render the device 102 inoperable, such as the erasure of secret information such as cryptographic keys.

[035] Referring to FIG. 3A, in some embodiments, the processor 113 includes on-chip or otherwise integrated memory 118a. As a result, when the anti-tamper circuitry 110 erases at least a portion of the memory 118a, the memory erased is memory integrated with the processor 113.

[036] Referring to FIG. 3B, in some embodiments, the anti-tamper circuitry 110 is coupled to the processor 113. The processor 113 is coupled to external memory 118b. The anti-tamper circuitry 110 may be configured to activate the processor 113 and cause the processor 113 to execute commands to erase the at least a portion of the external memory 118b. For example, the anti-tamper circuitry 110 may cause the processor to execute an interrupt service routine that erases the portion of the memory 118b. In another example, the anti-tamper circuitry 110 may be configured to boot the processor 113 in a mode specifically designed to erase the portion of the memory 118b. Although the processor 113 is illustrated as being directly coupled to the memory 118b, in other embodiments, other intervening circuitry may be present, such as a memory controller.

[037] Referring to FIG. 3C, in some embodiments, the anti-tamper circuitry 110 may be configured to access the memory 118c without accessing the processor 113. Accordingly, the anti-tamper circuitry 110 may be configured to erase the portion of the memory by controlling the memory 118c.

[038] While a variety of configurations of the anti-tamper circuitry 110, processor 113, and memory 118 have been described above, in other embodiments, the anti-tamper circuitry 110, processor 113, and memory 118 may be coupled in any manner such that the anti-tamper circuitry 110 may cause the portion of the memory 118 used by the processor 113 to be erased.

[039] FIG. 4A-4B are cross-sectional diagrams illustrating mounting a device with anti-tamper circuitry on an external component according to some embodiments. FIG. 4A illustrates a state of a device 102 and an external component 104 before the device 102 is mounted to the external component 104 or after the device 102 is removed from the external component 104. FIG. 4B illustrates a state of the device 102 and the external component 104 when the device 102 is mounted to the external component 104.

[040] Referring to FIGS. 4A and 4B, in some embodiments, the device 102 includes a housing 116. The device 102 includes a switch 220. The switch 220 is coupled to the housing 116. Although the housing 116 is illustrated as an example of a mounting structure of the device 102, in other embodiments, the mounting structure may be a structure other than the housing 116. The mounting structure may be any structure, board, component, or the like that remains with the device 102 when the device is moved relative to the external component 104. The housing includes a flange 212. A fastener 214 may be used to attach the housing 116 to the wall 124 of the external component 104. While mounting components such as the flange 212 and fastener 214 have been used as examples, in other embodiments, different mounting techniques may be used.

[041] The switch 220 is configured to switch when the device 102 is removed from the external component 104. When the device 102 is in the state illustrated in FIG. 4A, the switch 220 has a pole 222 in a first state. In a particular example, the switch 220 may be a

momentary normally closed switch. Thus, in the state illustrated in FIG. 4A, the switch 220 is closed.

[042] As the device 102 is mounted on the external component 104 as illustrated in FIG. 4B, a structure 204 of the external component 104 causes the pole 222 of the switch 220 to switch. Thus, the switch 220 is opened.

[043] In some embodiments, the structure 204 is a protrusion, wall, rib, gusset, fastener, or the like. The structure 204 disposed on the external component 104 such that when the device 102 is mounted on the external component 104, the structure 204 toggles the state of the switch 220.

[044] Although a particular structure of the device 102, external component 104, and switch 220 has been used as an example, any mechanism and associated structures may be used that causes the switch 220 to be in a first state when mounted and in a second state when removed. In particular, the mechanism and associated structures may be formed such that the switch 220 changes state before the anti-tamper circuitry 110 may be accessed to disable the anti-tamper circuitry 110 or otherwise prevent it from disabling at least one function of the circuitry 112 as described above.

[045] In addition, the switch 220 need not be mechanically switched. For example, the switch 220 may be magnetically switched. The structure 204 may include a magnet or a ferromagnetic material according to the structure of the switch 220 such that the switch 220 changes state as the device 102 is mounted to or removed from the external component 104.

[046] While a single switch 220 has been used as an example, in other embodiments, multiple switches 220 in different locations and/or different configurations may be used. In some embodiments, any one of these switches 220 may be used by the anti-tamper circuitry 110 to disable at least one function of the circuitry 112.

[047] FIGS. 5A-5D are schematic diagrams of circuitry of anti-tamper circuitry according to some embodiments. Referring to FIG. 5A, the anti-tamper circuitry 110a includes a power supply 502 and a disable circuit 504. The power supply 502 is

configured to generate power that may be used by the disable circuit 504 and potentially a portion of the circuitry 112.

[048] The power supply 502 is disposed within the device 102. The power supply 502 is configured to supply power after detecting removal of the device 102 from the external component 104. The power supply 502 may include a battery, a capacitor, a supercapacitor, or any other energy storage device that may be disposed within the device 102. In some embodiments, the power supply 502 may be charged by an external power source 506.

[049] In some embodiments, the power supply 502 may include switches that connect the power supply 502 to other components of the anti-tamper circuitry 110 when the device 102 is removed from the external component 104.

[050] The disable circuit 504 is a circuit configured to disable the at least one function of the circuitry 112. In this example, the disable circuit 504 includes an ERASE output. The ERASE output is a signal coupled to an ERASE input on a processor, memory, or the like of the circuitry 112 that would initiate an erase command to erase memory or otherwise disable the at least one function.

[051] In some embodiments, power PWR may also be provided to some components of the circuitry 112. In particular, the device 102 may not be connected to an external power source or the external power source may be disabled when the device 102 is being removed from the external component 104. The power supply 502 may instead supply the power needed to allow the disable circuit 504 to disable the at least one function of the circuitry 112.

[052] Referring to FIG. 5B, the anti-tamper circuitry 110b includes battery B1 and switch SW1. A single battery B1 is illustrated; however, in other embodiments, multiple batteries may be used. The switch SW1 is a double-pole double-throw switch (DPDT). The switch SW1 is coupled such that in the illustrated state, 3.3V is coupled to VDD_CPU and no connection is made to ERASE-CPU. In the other state, both VDD_CPU and ERASE_CPU are coupled to the battery B1.

[053] VDD_CPU is a power supply for a processor that may be part of the circuitry 112. ERASE_CPU is a signal that commands the processor of the circuitry 112 to erase some or all of its memory. As a result, the at least one function of the circuitry 112 may be disabled. The switch SW1 is illustrated in the state when the corresponding device 102 is mounted to the external component 104. When removed, the switch SW1 will transition to the other state, which will supply power to the processor through VDD_CPU and supply the erase signal through ERASE_CPU.

[054] The isolator I is a removable structure configured to disconnect the battery B1 from the switch. When in place, the battery B1 be disconnected and will not supply power to the switch SW1. Thus, ERASE_CPU will not be activated. The isolator I may be in place during installation to disable the anti-tamper circuitry 110b.

[055] Other circuitry illustrated may provide a status indicator for a variety of states. R1 is coupled to VDD_CPU and pulls down the input to AND gate U1. The other input to AND gate U1 is an error signal ERROR_N. When the device 102 is being installed and the 3.3V power is applied, the switch SW1 will be in the opposite state. However, as the isolator I is present, the battery will not enable ERASE_CPU. VDD_CPU will not be coupled to 3.3V and will be pulled down by R1. Thus, the output of AND gate U1 will be low, turning on LED D1. Once the device 102 is properly installed, the switch SW1 will change to the illustrated state and VDD_CPU will be set to 3.3V. The AND gate U1 output will switch to high, assuming there is no error indicated by a low on ERROR_N. The high output will cause the LED D1 to turn off. As a result, an installer will receive a visual indication that the device 102 is installed such that the switch SW1 is in the illustrated state.

[056] Once installed, the isolator I may be removed. ERROR_N will control the output of the AND gate U1 and whether LED D1 is on. Thus, the LED D1 will act as an error indicator. However, if the device 102 is removed, the switch SW1 will change state, activating VDD_CPU and ERASE_CPU.

[057] In an example, the SW1 switch is a normally closed (NC) double pole, double throw (DPDT) switch where the closed state couples the battery B1 to ERASE_CPU. The

switch can be normally closed (NC) and open when the switch is depressed, such as when the device 102 is installed and a feature of the external component 104 presses on the switch.

[058] Referring to FIG. 5C, the operation may be similar to that of FIG. 5B. However, VCC_INSTALL is a power voltage supplied during installation when 3.3V may not be active. Resistors R3 and R4 are in series with LED D2 for either VCC_INSTALL or 3.3V. Thus, when the cathode of LED D2 is pulled low, LED D2 will turn on. Buffer U2 is an open-drain buffer. Inverter U3 is an open-drain inverter. Thus, if the input to U2 is low or if the input to U3 is high, the LED D2 will be turned on.

[059] When the switch is in the installed state, ERASE_CPU and the nodes coupled to resistors R5, R6, R7, and Q1 are pulled to ground and transistor Q1 is off. However, once the device 102 is removed from the external component 104, switch SW1 changes state, increasing the voltage of node N1, pulsing ERASE_CPU until C1 charges. R5 and C1 are selected to provide a sufficient pulse to erase a portion of the memory to disable the at least one function.

[060] Referring to FIG. 5D, the operation of U2, U3, resistors R8, R9, and R10, diodes D3 and D4, and LED D5 may be similar to that of FIG. 5C. Here diodes D3 and D4 may isolate VCC_INSTALL from 3.3V. The operation of the anti-tamper circuitry 110d may be similar to that of anti-tamper circuitry 110c of FIG. 5C.

[061] Although 3.3V has been used as an example of a power supply voltage, in other embodiments, the power supply voltage may be different.

[062] FIGS. 6A and 6B are flowcharts showing techniques of operating a device with anti-tamper circuitry according to some embodiments. Referring to FIG. 6A, in 604 the removal of a device 102 from an external component 104 is detected. As described above, a variety of techniques may be used to detect the removal of the device 102. For example, the change in the state of a switch, the change in a magnetic field, the breaking of a circuit or the like may provide an indication of whether the device 102 is being removed from the external component 104.

[063] In 606, at least one function of the device 102 is disabled. As described above, the at least one function may be disabled by erasing data, disabling components, such as a processor, or the like. Various forms of the anti-tamper circuitry 110 may be used to perform the disabling.

[064] In some embodiments, the detecting of the removal of the device 102 may include detecting the physical separation of structure of the device 102 and a structure of the external component 104. For example, the switch 220 may detect when device 102 is moved relative to the external component 104.

[065] Referring to FIG. 6B, in 600, the device 102 is installed on the external component 104. For example, during authorized installation, replacement of a part, and/or maintenance of a system, a device 102 may be prepared and mounted on the external component 104. During installation, the anti-tamper circuitry 110 may be disarmed. For example, as described above, a removable isolator I such as an insulating tape may be disposed between the power supply 502 contacts and the disable circuit 504.

[066] In 602, the anti-tamper circuitry 110 may be armed. For example, once the device 102 is installed, the insulating tape may be removed, arming the anti-tamper circuitry 110. Before the insulating tape is removed, the device 102 may be mounted and removed repeatedly without engaging the anti-tamper circuitry 110. However, once removed, the anti-tamper circuitry 110 is armed and any attempt to remove the device 102 from the external component 104 may be detected and used to disable at least on function of the circuitry 112 of the device 102 in operations 604 and 606.

[067] Once the anti-tamper circuitry 110 has been triggered and at least one function of the circuitry 112 has been disabled, the device 102 may be reset in 608. Resetting the device 102 includes operations that return the device 102 to a state where it may again be installed or operated in an authorized manner. For example, the device 102 may be returned to an authorized repair facility. The erased data may be restored to the device 102, the disabled components may be reenabled, disabled components may be replaced, the isolator I described above may be reinstalled, or the like such that the device 102 is in a state similar to a device 102 that had not had the at least one function of the circuitry

112 disabled. Although returning the device 102 to an authorized repair facility has been used as an example, the resetting of the device 102 may be performed by an authorized repair technician with the appropriate data and/or components. An unauthorized party may not have the appropriate data and/or components and would not be able to restore the device 102 to an operating condition.

[068] FIG. 7 is a block diagram of an x-ray system according to some embodiments. The x-ray system 700 includes a host controller 702, an interface board (IFB) 704, and tube auxiliary unit (TAU) 732, and an x-ray tube 736. These components may be mounted on a rotatable gantry 710.

[069] In some embodiments, a device 102 is the IFB 704 or is part of the IFB 704. The external component 104 may be the gantry 710. Thus, if the IFB 704 is removed from the gantry, at least one function of the IFB 704 may be disabled if the interface board is removed from the gantry 710. The IFB 704 may include firmware, software, calibration data, secret information such as keys, IDs, or other cryptographic information, or the like that may be erased to disable at least one function.

[070] In some embodiments, a device 102 is an authentication daughter board (ADB) 703 that is mounted on the IFB 704. The external component 104 may be the IFB 704. Information such as that described above may be erased if the ADB 703 is removed from the IFB 704.

[071] In some embodiments, a device 102 is the TAU 732. The TAU 732 may be mounted on the x-ray tube 736. The external component 104 may be the x-ray tube 736. Thus, if the TAU 732 is removed from the x-ray tube 736, at least on function of the TAU 732 may be disabled. The TAU 732 may include data or firmware that may be erased similar to the IFB 704 or ADB 703.

[072] In some embodiments, the host controller 702 is configured to control operations of components such as the gantry 710, the IFB 704, the x-ray tube 736 though the TAU 732. While these components are used as examples, other components may be present such as an image detector, a high voltage (HV) generator, a heat exchanger, or the like. The host controller 702 may also be configured to communicate with the IFB 704 and

perform various actions such as identification, authentication, or the like in addition to directing control of the system 700.

[073] As described above, in some embodiments the IFB 704 includes the ADB 703. This configuration may allow for easier retrofitting of the ADB 703 to existing CT systems. The IFB 704 has a communication link to the host controller 702 and another communication link to the TAU 732. The ADB 703 contains cryptographic authentication hardware/firmware that allows for encrypted communication with both the host controller 702 and the TAU 732. The IFB 704 is a device that holds the ADB 703 and supplies power to it and translates the communications to the ADB's 703 native communication protocol.

[074] The TAU 732 contains cryptographic authentication hardware/firmware that allows for encrypted communication with the IFB 704/ADB 703 and is attached to the x-ray tube 736. When a hospital installs a new x-ray tube with its attached TAU 732 the IFB 704/ADB 703 may challenge the TAU 732 to see if it is a genuine manufacturer or OEM x-ray tube.

[075] In some embodiments, the authentication unit of the TAU 732 is mounted to the x-ray tube 736, but the authentication unit could also be an integral part of the x-ray tube 736. The anti-tamper circuitry 110 would be part of that authentication unit. Similarly, with other components such as an x-ray detector or imager, accelerator, or other device where it may be beneficial to render the unusable after its removal from its original installation location may include a device 102. Each of those may have associated anti-tamper circuitry 110.

[076] In a particular example, the removal of a used x-ray tube, x-ray detector, or imager from an x-ray or mammography system for the purpose of resale into another system may be prevented. Upon removal of the device 102, a switch in the anti-tamper circuitry 110 would trigger and could disable the authentication function, render the firmware unusable, prevent communication, or any other essential function that would allow further usage of the device 102.

[077] In some embodiments, the anti-tamper circuitry 110 could also be used to reinforce software/firmware (SW/FW) licensing of TAU 732, x-ray tube 736, detector, or other device software that was sold to a specific customer under a license agreement that would only allow the original buyer to utilize the firmware/software (FW/SW) or hardware. In such an embodiment, the respective FW/SW would be automatically erased when the device is removed.

[078] While a CT system with a rotatable gantry 710 has been used as an example of an x-ray system 700, the x-ray system 700 may take other forms.

[079] Some embodiments relate generally to mechanisms, methods, and systems using a system identifier (ID) (or a device ID) in an encrypted form to a component.

[080] In some embodiments, the mechanisms, methods, and systems described herein allows manufacturers or OEMs to detect unauthorized installation of components into their system. Currently, third-party suppliers can swap components on a system against used OEM components or third-party components which can lead to warranty issues, quality issues, and, in the case of an imaging system, image quality issues, diagnostic issues, and misdiagnosis. Embodiments described herein allow for the detection of such unauthorized component changes to ensure the integrity of the system.

[081] Without a system such as those described herein, third parties can buy used components and sell them back to customers and undercut OEM service contracts. In contrast, embodiments described herein allow OEM host systems to determine if their components are being swapped without their permission and/or prevent installation of old, outdated or compromised component into a system that may affect operation, such as replacing a component in an imaging system that will affect the diagnosis of patients. Defective or not optimally functional components can lead to misdiagnosis and in extreme case can cause permanent harm to the patient and even death.

[082] FIG. 8A-8B are block diagrams of systems including an authorization system according to some embodiments. Referring to FIG. 8A, the system 800a includes a first device 802 and a second device 804. The devices 802 and 804 are coupled through a communication link 806. The communication link may be any medium that allows the

devices 802 and 804 to communication. For example, the communication link 806 may include a serial link, a parallel link, and automation communication link such as Modbus, CANbus, or the like, a computer bus such as peripheral component interconnect express (PCIe), nonvolatile memory express (NVMe), or the like, and/or a network such as an Ethernet network, a Fibre Channel network, or the like.

[083] The second device 804 includes a non-volatile memory 808. The memory 808 may include any variety of non-volatile memory such as static random access memory (SRAM), flash memory, electrically erasable programmable read only memory (EEPROM), magnetic storage, or the like. In particular, the memory 808 includes at least a portion that is operable in a one-time-write manner. The memory 808 may include other non-volatile memory that is not configured for one-time-writes and/or volatile memory such as a dynamic random access memory (DRAM), a double data rate synchronous dynamic random access memory (DDR SDRAM) according to various standards such as DDR, DDR2, DDR3, DDR4.

[084] Being one-time-write means that the portion of the memory 808 is writable once in a normal write operation. In some embodiments, the one-time write memory 808 may not be erased by other means. As a result, to change a value stored in the memory 808 would require replacing the memory 808. However, in other embodiments, the portion of the memory 808 may be erased by erasing the entire memory 808.

[085] The memory 808 is configured to store a system identifier (ID) in the one-time-write portion. The system ID is an identifier associated with the system 800a. The system ID may be unique to the system 800a such as by being a universally unique ID (UUID) or globally unique ID (GUID). The system ID for all devices 804 and 812 may be the same. However, in other embodiments, the system ID for a particular device 804 or 812 may be unique to both the system 800a and that device 804 or 812. In some embodiments, the system ID may include a portion unique to the system 800a and a portion unique to the particular device 804 or 812, the particular type of device 804 or 812, or the like.

[086] The value of the system ID may take a variety of forms. For example, the system ID may exist in an original form where the stored data is the system ID. However, in other examples, an encrypted form of the system ID, a hash of the system ID, or other representations of the system ID may be stored as the system ID and treated as such with appropriate decoding or other manipulation.

[087] As will be described in further detail below, a system ID can be stored on devices 804 in a system 800a. The first device 802 can verify that the system ID stored on the second device 804 or third device 812 matches the expected system ID such as a system ID associated with the system 800a. A match of the system ID may indicate that the second device 804 or third device 812 is a genuine component intended and originally installed on the system 800a. If the system ID does not match, the device 804 or 812 may have been provided or installed by an unauthorized party. As a result, swapping of devices from other systems of the same manufacturer or from a third party may be detected.

[088] In some embodiments, the first device 802 may be coupled to multiple second devices 804-1 to 804-N. Each second device 804 may be coupled to zero to multiple third devices 812-1 to 812-M.

[089] FIGS. 9A-10C are flowcharts showing examples of techniques of operating an authorization system according to some embodiments. In the following descriptions of techniques of operating the system, operations of a first device 802, a second device 804, and a third device 812 of FIG. 8A will be used as examples.

[090] Referring to FIG. 8A and 9A, in 902, the first device 802 transmits a request for a system ID stored on the second device 804 to the second device. The second device 804 receives the request in 903. This transmission and other similar operations may occur over the communication link 806.

[091] In 904, the second device 804 determines if the system ID stored on the second device has an empty value. The empty value represents a state where the second device 804 has not stored a system ID in the memory 808. An actual value may not be stored in the memory 808. Instead, a flag, register, state, or the like may indicate that the system

ID has not been programmed into the memory 808. Checking such an indicator may be part of determining if the system ID has the empty value. A processor of the second device 804 may be configured to attempt to read the system ID, flag, register, state, or the like to make the determination.

[092] In 906, a response based on the empty value is transmitted to the first device 802. In some embodiments, the response may be a system ID that has a specific meaning. For example, all zeros or all ones may be designated as an empty value for the system ID. In other embodiments, a particular value or values of the system ID may be designated as the empty value. That specific value may be specific to the second device 804 or the type of the second device 804, specific to the system 800a or the type of the system 800a, or the like. Regardless, it is a value that the first device 802 will recognize as indicating that the second device 804 does not store a system ID or that the system ID is the empty value.

[093] In other embodiments, the empty value response may be a different type of message from that used to transmit an actual system ID. For example, the empty value response may be an error message. The error message may have an error number or code that indicates that the system ID is empty.

[094] In 908, the empty value response is received by the first device 802. In response, the first device 802 transmits the system ID to the second device 804 in 910. The second device 804 receives the system ID in 912 and stores it in the one-time write portion of the memory 808. Once the system ID is stored, the memory 808 cannot be reprogrammed with a different system ID without extraordinary steps as described above. As a result, the second device 804 is paired with the system 800a. If the second device 804 is removed from the system 800a and placed in another system, even an identical system, the system ID may not match.

[095] If the system ID is determined to be stored at the second device 804 in 904, a response based on the system ID is returned to the first device 802 in 914. For example, the second device 804 may read the system ID, encrypt it, and transmit the encrypted system ID to the first device 802.

[096] The first device 802 receives the response based on the system ID stored at the second device 804 in 916 and determines if the response indicates that the system ID stored at the second device 804 matches the actual system ID in 918. For example, the first device 802 may extract the system ID by reading it from the response, decoding an encrypted response, or the like and comparing it to the system ID stored on the first device 802. As described above, the system ID may be stored or encoded in a variety of formats. The comparison may be performed in a manner appropriate to the different formats.

[097] If the system ID indicated by the response from the second device 804 is not correct, if the second device 804 does not respond or times out, if the second device 804 returns an improper response, or the like, counter measures may be performed in 920. The counter measures may take a variety of forms. For example, in some embodiments, the system 800a may be shutdown, the devices 802, 804, 816, or the like may be disabled temporarily or permanently, particular functions may be disabled, ranges of operation may be reduced or limited, or the like. In other embodiments, a notification, a warning, or other communication of the mismatched system IDs may be presented to a user of the system 800a, reported over a network, or the like. In other embodiments, information related to the mismatching system IDs may be recorded in memory 808 of the first device 802 and/or the second device 804. The related information may include a timestamp, model numbers and/or serial numbers of the first device 802 and/or the second device 804, number of times the system IDs had not matched, the mismatched system ID, the entire response received in 916, or the like.

[098] In some embodiments, when response based on the system ID is transmitted to the first device 802 from the second device 804 in 914, the communication may be encrypted. For example, a secure communication link may be established between the first and second devices 802 and 804, the response or portions of it may be encrypted, the system ID stored on the second device 804 may be encrypted, or the like. As a result, it may be more difficult for an eavesdropper to obtain the correct system ID response from the second device 804.

[099] The system 800a may be a hierarchical system that includes a third device or devices 812 that are downstream from an associated second device 804. In some embodiments, some or all communication between the first device 802 and the third device 812 may pass through or be manipulated by the associated second device 804. However, in other embodiments, only the communications related to the system ID may pass through or be manipulated by the associated second device 804.

[100] In some embodiments, the interactions between the second device 804 and the third device 812 may be the same or similar to the operations described with respect to the first device 802 and the second device 804. That is, once the second device 804 stores the system ID, the requesting, storing if empty, and verifying of the system ID may be performed between the second and third devices 804 and 812.

[101] Referring to FIGS. 8A, 9A, and 9B, in some embodiments, once the second device 804 has transmitted the system ID response in 914, the second device 804 may begin the operations described above with respect to FIG. 9B. A request for the system ID stored on the third device 812 may be transmitted in 922 from the second device 804 to the third device 812. The third device 812 may receive the request for the system ID stored on the third device 812 in 924. Similar to the operations in 904 and 906 of FIG. 9A, in 926 and 928, the third device 812 may determine if the system ID is the empty value or has not been stored and, if so, return the empty value response. Similar to the operations in 908 and 910 of FIG. 9A, in 930 and 932, the second device 803 receives the response indicating that the system ID stored on the third device 812 has the empty value and transmits the system ID in response. In 934, the third device 812 stores the system ID in the memory 808. Similar to the operations in 914 and 916, in 936 and 938, the third device 812 may transmit a response based on the system ID stored on the third device 812 and that response is received by the second device 804. Although the operations of the second device 804 and the third device 812 have been described as being similar to those of the first device 802 and second device 804, in other embodiments, the operations may be different. For example, different encodings of the system ID, encryption used in transmission, format of responses, particular protocol, or the like may be used.

[102] In 940, the second device 804 may prepare a verification response based on the responses from the third device 812. In some embodiments, the verification response may include the system ID response from the third device 812 itself. In other embodiments, the second device 804 may determine if the system ID stored on the third device 812 matches the system ID stored on the second device 804 similar to the interaction of the first device 802 in 918 of FIG. 9A. The verification response may include an indication of whether the system ID stored on the third device 812 is the correct system ID.

[103] Referring to FIGS. 8A, and 9A-9C, in some embodiments, if the system ID stored on the second device 804 is determined to be the correct system ID in 918, the first device 802 may transmit a verification request to the second device 804 in 941. In 942, the second device 804 receives the verification request. As described above, the second device 804 may prepare a verification response in 940. This verification response may be transmitted by the second device 804 to the first device 802 in 944. In 946, the first device 802 receives the verification response and determines if the verification was successful in 948 based on the response. If the verification was successful, operations continue in 952.

[104] However, if the verification was not successful, counter measures may be performed in 950. The counter measures may be similar to those described with respect to 920. However, as the verification response may be associated with the third device 812, the counter measures may also apply to the third device 812. For example, the third device 812 may be disabled, a notification may be presented identifying the third device 812, or the like.

[105] Referring to FIGS. 8A, 9A, 9B, and 9D, in some embodiments, once the second device 804 has prepared the verification response in 940, the second device 804 may transmit the verification response in 944 to the first device 802 without waiting for the request transmitted in 941. The operations of the first device 802 in 946, 948, 950, and 952 may be similar to those described above.

[106] Although the operations of the first device 802 and second device 804 have been described in the context of communications between the first device 802 and one second device, the same or similar communications may occur between the first device 802 and multiple second devices 804-1 to 804-N. That is, the first device 802 may request the system ID for each of the second devices 804-1 to 804-N and perform operations similar to those described above. The operations for different second devices 804-1 to 804-N may be performed serially or in parallel. Decisions may be based on responses of only one of the second devices 804-1 to 804-N, some of the second devices 804-1 to 804-N, or all of the second devices 804-1 to 804-N. The results of matching or mismatching system IDs may be the same, similar, or different for different second devices 803-1 to 804-N. The operations described between a second device 804 and a third device 812 may similarly be performed with multiple third devices 812. Moreover, although a three-tier hierarchy has been used as an example, and hierarchy of devices may be part of the system 800a where the first device 802 queries other devices for a system ID.

[107] Referring to FIG. 8B, in some embodiments, an x-ray system 800b includes a host controller 822, an ADB 824, a TAU 832, and an x-ray tube 836. The host controller 822 may be a system controller for the x-ray system 800b. The host controller 822 may act as the first device 802 of FIG. 8A and perform the associated operations described in FIGS. 9A-D.

[108] The ADB 824 may be a circuit that manages the system ID and authentication operations of the system 800b. The ADB 824 may include a memory 808. The ADB 824 may act as the second device 804 of FIG. 8A and perform the associated operations described in FIGS. 9A-D.

[109] The TAU 832 is a circuit configured to control the operation of the x-ray tube 836. For example, the TAU 832 may be configured to control cathode voltages/currents, anode voltages/currents, filament voltages/currents, focusing electronics, steering electronics, motors, or the like depending on the particular x-ray tube 836. The TAU 832 includes a memory 808 and may act as the third device 812 of FIG. 8A and perform the associated operations described in FIGS. 9A-D.

[110] While the TAU 832 has been used as an example of a device in an x-ray system 800b that may operate using a system ID as described herein, other devices in an x-ray system 800b may operate similarly. For example, a heat exchanger 840, detector 842, high voltage (HV) power supply, 844, accelerator 846, or the like may operate using a system ID as described herein.

[111] In some embodiments, at initialization or installation, a system ID may be transmitted from the host controller 822 to the ADB 824 and stored in memory 808. The ADB 824 may similarly propagate the system ID to the other devices 832, 840, 842, 844, 846, 848, or the like for storage in corresponding memory 808 of those devices. Thus, the devices of the system 800b may be paired with that system 800b. In normal operation, the devices will report the correct system ID and the system 800b may continue operation. However, if a part is replaced in an unauthorized manner with a different, existing system ID, the counter measures described above may be performed.

[112] In some embodiments, the host controller uses the ADB 824 to communicate with the rest of the manufacturer or OEM's components in the system 800b. In some embodiments the only components that are paired with the system 800b are the ADB 824 and the TAU 832.

[113] The use of the system ID as described herein in an x-ray system 800b may improve safety and/or longevity of the system 800b. In particular, the components of the system 800b may be aligned, calibrated, or otherwise configured for that specific x-ray system 800b. When the system 800b is initially installed, the empty system IDs in the various devices of the x-ray system 800b may be initialized to a system ID unique to that particular x-ray system 800b. If a device in the x-ray system 800b is replaced by a device from another system with a different system ID, the operation of the x-ray system 800b may not be the same and, with devices such as the x-ray tube 836, may become dangerous. As described above, the x-ray system 800b may take counter measures when such a situation is detected, notifying a user, shutting down the x-ray system 800b or a component, or the like. As a result, a chance that the x-ray system 800b will be operated

in a manner that may lead to erroneous results and/or dangerous operating conditions may be reduced or eliminated.

[114] In some embodiments, the storage and verification of the system ID as described herein may limit a manufacturer or vendor's customers ability to swap components themselves or through a third party. The verification process checks to see if the ADB 824, TAU 832, or the like is a genuine manufacturer or OEM product and that it hasn't been swapped to/from other x-ray systems. It prevents third party service organizations buying used x-ray tubes on the open market, refurbishing them and then selling them back to customers such as hospitals. A manufacturer, vendor, system integrator, or the like may reduce a chance that their system is modified with devices from other systems, which may lead to undesirable or dangerous results.

[115] In some embodiments, use of the system ID as described herein may reduce a chance that a reworked device is installed in a system for which it was not intended. For example, a device that has been paired with a system and has a system ID may returned for repair, updates, or the like. The device may be programmed with the original system ID or the system ID may be left intact. As a result, when that device is supplied to a customer or installer, the system ID will match the system ID of the original system. If the device is installed in a different system, even if a similar system or the same type of system, the system ID will not match and the counter measures described above may be performed. In some embodiments., the system ID may be left unprogrammed if a known customer or installer will reinstall the device in the same system.

[116] Referring to FIGS. 8A and 9A-10C, in some embodiments, authentication operations may be performed after successful verification in 948 described above. For example, in 1002, the first device 802 transmits an authentication request to the second device 804. In 1004, the authentication request is received by the second device 804. The second device 804 transmits an authentication request to the third device 812 in 1006.

[117] The third device 812 receives the authentication request in 1008. In 1010, the third device generates an authentication response and transmits that authentication response to the second device 804 in 1012.

[118] The second device 804 receives the authentication response from the third device 812 in 1014. The second device 804 analyzes the authentication response 1016, logs failures in 1018, and generates its own authentication response in 1020. The authentication response generated in 1020 may aggregate the authentication response or responses received from one or more third devices 812 and the second device's 804 own authentication response.

[119] In 1022, the first device 802 may transmit a request for the authentication status that is received by the second device in 1024 as illustrated in FIG. 10B. In response, the second device 804 transmits the authentication response to the first device 802 in 1026. Alternatively, the second device 804 may transmit the authentication response to the first device 802 in 1026 after generating it in 1020 as illustrated in FIGS. 10A and 10C.

[120] Once the authentication response is received in 1028, the response may be analyzed to determine if the authentication is successful in 1030. If so, the operations may continue in 1034. If not, counter measures make be performed in 1032 similar to the counter measures described above.

[121] A variety of different techniques may be used to authenticate the devices 804 and 812. In some embodiments, the authentication may be performed using a challenge using hidden numbers. An encryption algorithm may use an initialization vector (IV) and an encryption key (key). The first device 802 and/or the second device 804 may create a challenge (math problem) using its IV and key and sends it the downstream second device 804 or third device 812. If that device has the same key and IV then it may do the same math problem and get the same result. The second device 804 or third device 812 that was "challenged" may then send back the "answer" to that math problem in an encrypted form and the original component can make sure that it answered the challenge correctly. If it responded with the correct answer then the first device 802 and/or the

second device 804 may treat the corresponding second device 804 or third device 812 as a genuine part.

[122] In some embodiments, the IV and the key are maintained in restricted memory of a cryptographic authentication integrated circuit. For example, an ATSHA integrated circuit may include such restricted memory and may be capable of performing calculations related to encrypted communications. The authentication operations may be more secure if the IV and key are stored in such restricted memory.

[123] In some embodiments, the authentication process may be used to ensure that all required components are in the system, are designed for the particular customer, and/or are genuine manufacturer or OEM components. Different customers may have customer specific encryption keys so that a third party cannot take a component designed for one customer and sell it to another. Any missing components will fail the authentication process as they will not authenticate if they are not present. The authentication process may prevent a third party from supplying part of the system. If the full computed tomography (CT) system is designed to have 5 manufacturer or OEM components but only 4 of them are genuine and the fifth was sourced from a third party, the authentication process would identify that fifth component as not genuine.

[124] As described above, more than one second device 804 and more than one third device 812 may be present in the system 800a. The authentication with each of these as described with respect to the single second device 804 and single third device 812.

[125] While the system 800a of FIG. 8A was used as an example, the authentication operation operations described above with respect to FIGS. 10A-C may be implemented by other systems, such as the x-ray system 800b of FIG. 8B.

[126] Some embodiments include a device 102, comprising: a mounting structure configured to mount the device 102 to an external component 104; first circuitry 112; and anti-tamper circuitry electrically connected to the first circuitry 112 and configured to disable at least one function of the first circuitry 112 when the device 102 is removed from the external component 104. In some embodiments, the external component 104

may include a wall, housing, or other structure that is not controlled by the first circuitry 112.

[127] In some embodiments, the first circuitry 112 is configured to control the external component 104. In some embodiments, the at least one function of the first circuitry 112 include functions that are not related to the control of the external component 104.

[128] In some embodiments, the at least one function of the first circuitry 112 comprises functions of the first circuitry 112 that control the external component 104.

[129] In some embodiments, the device 102 further comprises: a housing 116 coupled to the mounting structure wherein the housing 116 is configured to restrict access to disarm the anti-tamper circuitry when the device 102 is mounted to the external component 104.

[130] In some embodiments, the anti-tamper circuitry 110 comprises: a switch 220 or SW1 coupled to the mounting structure 116 and configured to switch when the device 102 is removed from the external component 104.

[131] In some embodiments, the switch 220 or SW1 is configured to switch by a structure of the external component 104 when mounted on the external component 104.

[132] In some embodiments, the anti-tamper circuitry 110 comprises: a power supply 502 disposed within the device 102 and configured to supply power after detecting removal of the device 102 from the external component 104; and a disable circuit 504 configured to disable the at least one function of the first circuitry 112; wherein the switch 220 or SW1 is configured to electrically connect the power supply 502 to the disable circuit 504 when the device 102 is removed from the external component 104.

[133] In some embodiments, the first circuitry 112 includes a processor 113; and the anti-tamper circuitry 110 is configured to erase at least a portion of memory 118 or 808 used by the processor 113 when the device 102 is removed from the external component 104.

[134] In some embodiments, the at least a portion of memory 118 or 808 used by the processor 113 comprises memory 118 or 808 integrated with the processor 113.

[135] In some embodiments, the at least a portion of memory 118 or 808 used by the processor 113 stores cryptographic information.

[136] In some embodiments, the device 102 is part of electronics associated with an x-ray system; and the external component 104 is an x-ray tube 736 or 836 of the x-ray system 700 or 800b.

[137] In some embodiments, the device 102 is part of a component authentication system associated with an x-ray system 700 or 800b.

[138] Some embodiments include a method, comprising: detecting, by a device 102, removal of the device 102 from a component 104 external to the device 102; and disabling at least one function of circuitry 112 of the device 102 in response to detecting the removal of the device 102 from the component 104.

[139] In some embodiments, the detecting, by the device 102, removal of the device 102 from the component 104 comprises detecting physical separation of a structure of the device 102 and a structure of the component 104 external to the device 102.

[140] In some embodiments, the disabling of at least one function of the circuitry 112 of the device 102 comprises: powering a disable circuit 504 from an internal power supply 502; and disabling the at least one function of the circuitry of the device 102 using the disable circuit 504.

[141] In some embodiments, the detecting, by the device 102, removal of the device 102 from the component 104 comprises detecting physical separation of a structure of the device 102 and a structure of the component 104 external to the device 102.

[142] In some embodiments, the method further comprises: installing the device 102 on the component 104; and arming anti-tamper circuitry 110 configured to disable to at least one function of the circuitry of the device 102.

[143] In some embodiments, the method further comprises: resetting anti-tamper circuitry 110 configured to disable to at least one function of the circuitry 112 of the device 102.

[144] Some embodiments include a device, comprising: means for detecting, by a device, removal of the device from a component external to the device; and means for disabling at least one function of circuitry of the device in response to the means for detecting the removal of the device from the component. Examples of the means for detecting include

the anti-tamper circuitry 110, switch 220 or SW1, or the like. Examples of the means for disabling at least one function of circuitry of the device include the anti-tamper circuitry 110, the processor 113, the memory 118 or 808, or the like.

[145] In some embodiments, the device further comprises: means for detecting physical separation of the device from the component; and means for erasing at least part of memory of the circuitry in response to the means for detecting physical separation of the device 102 from the component. Examples of the means for detecting physical separation of the device from the component include the anti-tamper circuitry 110, switch 220 or SW1, or the like. Examples of the means for erasing at least part of memory of the circuitry comprise the anti-tamper circuitry 110, the processor 113, the memory 118 or 808, or the like.

[146] Some embodiments include a method, comprising: receiving from a first device 802 at a second device 804, a request for a system identifier (ID) stored on the second device 804; determining, by the second device 804, if the system ID stored on the second device 804 has an empty value; and when the system ID stored on the second device 804 does not have the empty value, transmitting, by the second device 804 to the first device 802, a response based on the system ID stored on the second device 804.

[147] In some embodiments, the method further comprises: when the system ID stored on the second device 804 has the empty value, communicating, by the second device 804 to the first device 802, that the system ID stored on the second device 804 has the empty value.

[148] In some embodiments, the method further comprises: receiving, from the first device 802 by the second device 804, the system ID; and storing, by the second device 804, the system ID received from the first device 802 as the system ID stored on the second device 804.

[149] In some embodiments, storing, by the second device 804, the system ID received from the first device 802 as the system ID stored on the second device 804 comprises storing, by the second device 804, the system ID received from the first device 802 in one-time-write memory 808.

[150] In some embodiments, transmitting, by the second device 804 to the first device 802, the response based on the system ID stored on the second device 804 comprises encrypting the system ID stored on the second device 804 and transmitting, by the second device 804 to the first device 802, the encrypted system ID.

[151] In some embodiments, the method further comprises: transmitting, by the second device 804 to a third device 812, a request for a system ID stored on the third device 812; and receiving, by the second device 804 from the third device 812, a response to the request for the system ID stored on the third device 812.

[152] In some embodiments, the method further comprises: transmitting, by the second device 804 to the first device 802, a response based on the response to the request for the system ID stored on the third device 812.

[153] In some embodiments, the method further comprises: determining, by the third device 812, if the system ID stored on the third device 812 has the empty value; and when the system ID stored on the third device 812 has the empty value, communicating, by the third device 812 to the second device 804, that the system ID stored on the third device 812 has the empty value.

[154] In some embodiments, the method further comprises: storing, by the third device 812, the system ID received from the second device 804 as the system ID stored on the third device 812.

[155] In some embodiments, the second device 804 is an authentication device for an x-ray system 800b; and the third device 812 is a control device for an x-ray tube 836 of the x-ray system 800b.

[156] Some embodiments include a method, comprising: transmitting, from a first device 802 to a second device 804, a request for a system identifier (ID) stored on the second device 804; receiving, from the second device 804 by the first device 802, a response to the request for the system ID stored on the second device 804; determining, by the first device 802, if the system ID stored on the second device 804 is a correct system ID for a system including the second device 804; and operating the system including the second

device 804, by the first device 802, based on whether the system ID stored on the second device 804 is the correct system ID for the system including the second device 804.

[157] In some embodiments, operating the system including the second device 804 comprises enabling counter measures when the system ID stored on the second device 804 is not the correct system ID for the system including the second device 804.

[158] In some embodiments, the counter measures comprise at least one of disabling the second device 804, disabling the system including the second device 804, presenting a warning that the system ID stored on the second device 804 and the correct system ID for the system including the second device 804 do not match to a user.

[159] In some embodiments, operating the system including the second device 804 comprises, when the system ID stored on the second device 804 matches the correct system ID for the system including the second device 804, transmitting, by the first device 802 to the second device 804, a request for verification of devices subordinate to the second device 804.

[160] In some embodiments, the method further comprises: receiving, by the first device 802 from the second device 804, a response to the request for verification of devices subordinate to the second device 804; wherein operating the system including the second device 804 comprises operating the system based on the response to the request for verification of at least one device subordinate to the second device 804.

[161] In some embodiments, the second device 804 is an authentication device for an x-ray system 800b; and the at least one device subordinate to the second device 804 is a control device for an x-ray tube 836 of the x-ray system 800b.

[162] In some embodiments, the method further comprises: transmitting, from the first device 802 to the second device 804, a request for authentication of the second device 804; and receiving, by the first device 802 from the second device 804, a response to the request for authentication of the second device 804; wherein operating the system including the second device 804 comprises operating the system including the second device 804 based on the response to the request for authentication of the second device 804.

[163] Some embodiments include a device, comprising: means for receiving, from a first external device, a request for a system identifier (ID) stored on the device; means for determining if the system ID stored on the device has an empty value; and means for transmitting, to the first device, a response based on the system ID stored on the device when the system ID stored on the device does not have the empty value. Examples of the means for receiving, from a first external device, a request for a system identifier and the means for transmitting, to the first device, a response based on the system ID include the second device 804, the third device 812 or the like.

[164] In some embodiments, the device further comprises: means for transmitting, to a second external device, a request for a system ID stored on the second external device; and means for receiving, from the third device, a response to the request for the system ID stored on the second external device. Examples of the means for transmitting, to a second external device, a request for a system ID and the means for receiving, from the third device, a response to the request for the system ID include the second device 804, the third device 812 or the like.

[165] Some embodiments include at least one non-transitory machine-readable storage medium comprising a plurality of instructions adapted to be executed to implement the method described above.

[166]

[167] The summary provided above is illustrative and is not intended to be in any way limiting. In addition to the examples described above, further aspects, features, and advantages of the invention will be made apparent by reference to the drawings, the following detailed description, and the appended claims.

[168] Circuitry can include hardware, firmware, program code, executable code, computer instructions, and/or software. A non-transitory computer readable storage medium can be a computer readable storage medium that does not include a signal.

[169] The operations described above may be implemented in various circuitry. For example, the operations may be implemented as a hardware circuit comprising custom very-large-scale integration (VLSI) circuits or gate arrays, including but not limited to

logic chips, transistors, or other components. The operations may also be implemented in programmable hardware devices, including but not limited to field programmable gate arrays (FPGA), programmable array logic, programmable logic devices or similar devices.

[170] Reference throughout this specification to an "example" or an "embodiment" means that a particular feature, structure, or characteristic described in connection with the example is included in at least one embodiment of the invention. Thus, appearances of the words an "example" or an "embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment.

[171] Furthermore, the described features, structures, or characteristics may be combined in a suitable manner in one or more embodiments. In the following description, numerous specific details are provided (e.g., examples of layouts and designs) to provide a thorough understanding of embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, layouts, etc. In other instances, well-known structures, components, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

[172] Elements specifically recited in means-plus-function format, if any, are intended to be construed to cover the corresponding structure, material, or acts described herein and equivalents thereof in accordance with 35 U.S.C. § 112 ¶ 6.

[173] While the forgoing examples are illustrative of the principles of the invention in one or more particular applications, it will be apparent to those of ordinary skill in the art that numerous modifications in form, usage and details of implementation can be made without the exercise of inventive faculty, and without departing from the principles and concepts of the invention. Accordingly, it is not intended that the invention be limited. Various features and advantages of the invention are set forth in the following claims.

What is claimed is:

1. A device, comprising:
a mounting structure configured to mount the device to an external component;
first circuitry; and
anti-tamper circuitry electrically connected to the first circuitry and configured to disable at least one function of the first circuitry when the device is removed from the external component.

2. The device of claim 1, wherein the first circuitry is configured to control the external component.

3. The device of claim 2, wherein the at least one function of the first circuitry comprises functions of the first circuitry that control the external component.

4. The device of claim 1, further comprising:
a housing coupled to the mounting structure wherein the housing is configured to restrict access to disarm the anti-tamper circuitry when the device is mounted to the external component.

5. The device of claim 1, wherein the anti-tamper circuitry comprises:
a switch coupled to the mounting structure and configured to switch when the device is removed from the external component.

6. The device of claim 5, wherein:
the switch is configured to be switched by a structure of the external component when mounted on the external component.

7. The device of claim 5, wherein the anti-tamper circuitry comprises:
a power supply disposed within the device and configured to supply power after detecting removal of the device from the external component; and
a disable circuit configured to disable the at least one function of the first circuitry;
wherein the switch is configured to electrically connect the power supply to the disable circuit when the device is removed from the external component.

8. The device of claim 1, wherein:
the first circuitry includes a processor; and
the anti-tamper circuitry is configured to erase at least a portion of memory used by the processor when the device is removed from the external component.

9. The device of claim 8, wherein the at least a portion of memory used by the processor comprises memory integrated with the processor.

10. The device of claim 8, wherein the at least a portion of memory used by the processor stores cryptographic information.

11. The device of claim 1, wherein:
the device is part of electronics associated with an x-ray system; and
the external component is an x-ray tube of the x-ray system.

12. The device of claim 1, wherein the device is part of a component authentication system associated with an x-ray system.

13. A method, comprising:
detecting, by a device, removal of the device from a component external to the device; and

disabling at least one function of circuitry of the device in response to detecting the removal of the device from the component.

14. The method of claim 13, wherein:

the detecting, by the device, removal of the device from the component comprises detecting physical separation of a structure of the device and a structure of the component external to the device.

15. The method of claim 14, wherein:

the disabling of at least one function of the circuitry of the device comprises:

powering a disable circuit from an internal power supply; and

disabling the at least one function of the circuitry of the device using the disable circuit.

16. The method of claim 13, wherein:

the detecting, by the device, removal of the device from the component comprises detecting physical separation of a structure of the device and a structure of the component external to the device.

17. The method of claim 13, further comprising:

installing the device on the component; and

arming anti-tamper circuitry configured to disable to at least one function of the circuitry of the device.

18. The method of claim 13, further comprising:

resetting anti-tamper circuitry configured to disable to at least one function of the circuitry of the device.

19. A device, comprising:

means for detecting, by a device, removal of the device from a component external to the device; and

means for disabling at least one function of circuitry of the device in response to the means for detecting the removal of the device from the component.

20. The device of claim 19, further comprising:

means for detecting physical separation of the device from the component; and

means for erasing at least part of memory of the circuitry in response to the means for detecting physical separation of the device from the component.

FIG. 1A

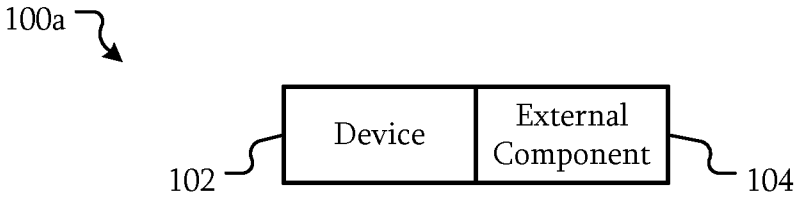


FIG. 1B

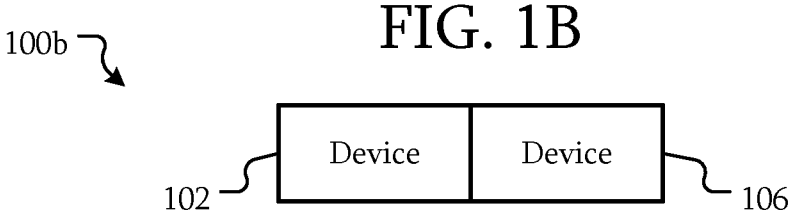


FIG. 1C

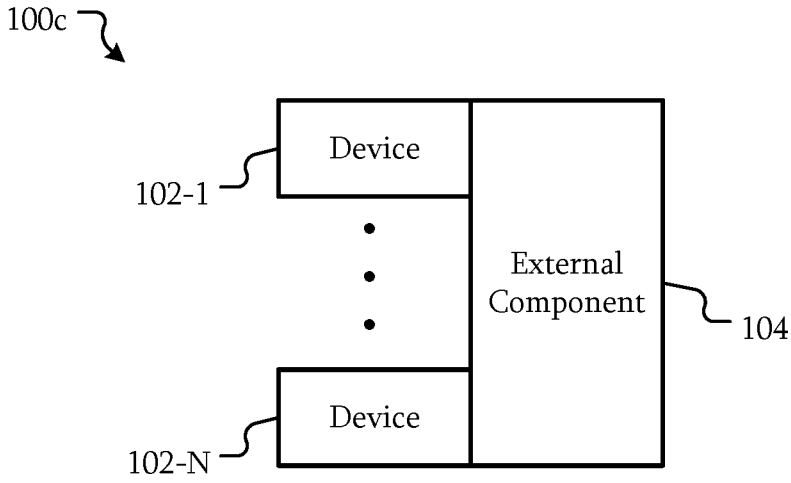


FIG. 2

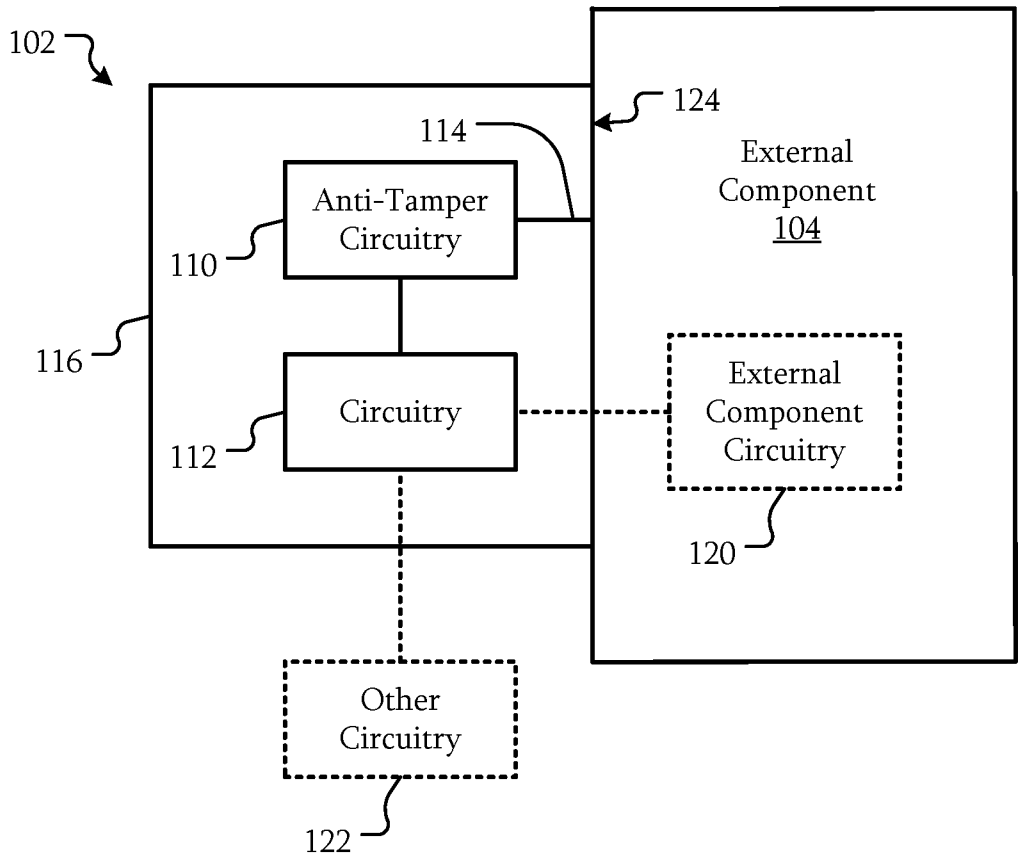

102
124
114
External
Component
104
Anti-Tamper
Circuitry
110
116
Circuitry
112
External
Component
Circuitry
120
Other
Circuitry
122

FIG. 3A

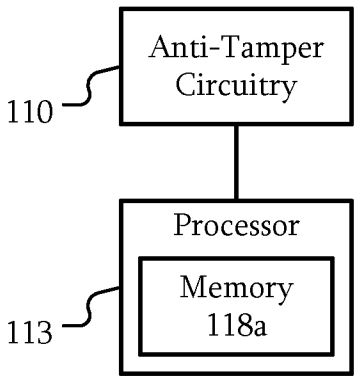

Anti-Tamper Circuitry
110
Processor
Memory 118a
113

FIG. 3B

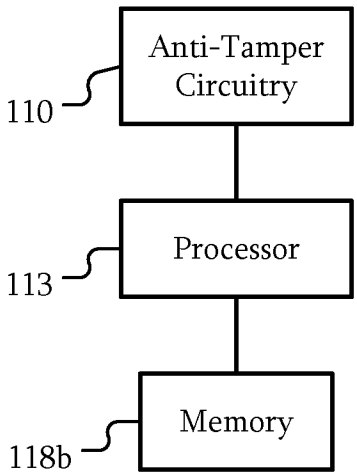

Anti-Tamper Circuitry
110
Processor
113
Memory
118b

FIG. 3C

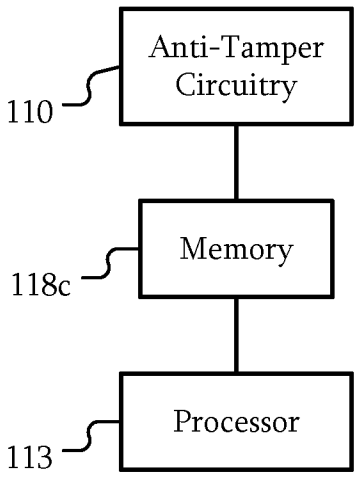


FIG. 4A

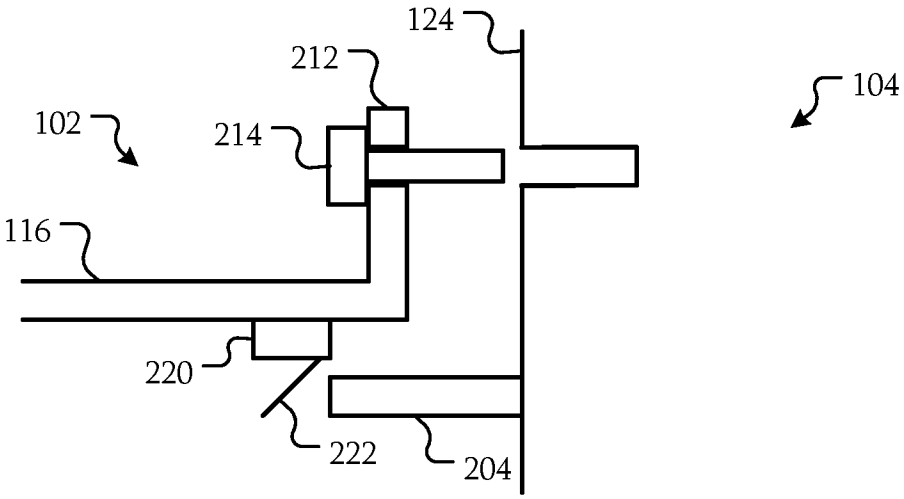

124
212
104
102
214
116
220
222
204

FIG. 4B

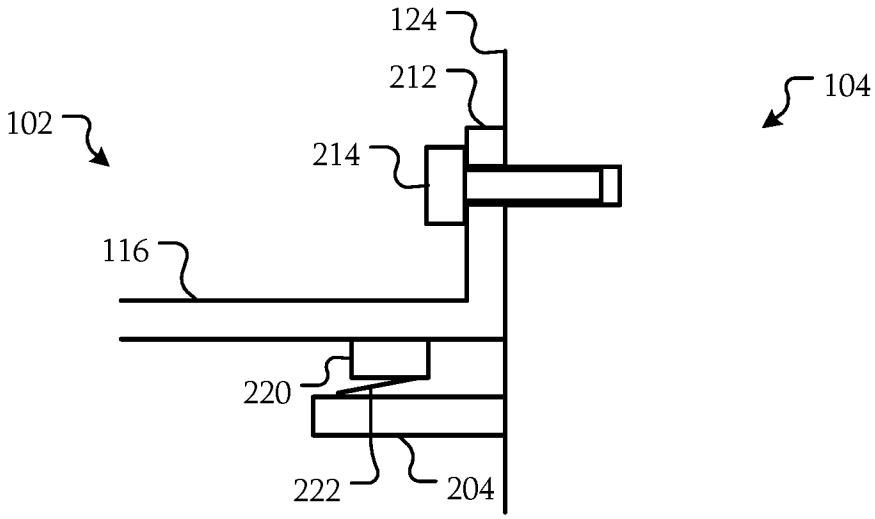

124
212
104
102
214
116
220
222
204

FIG. 5A

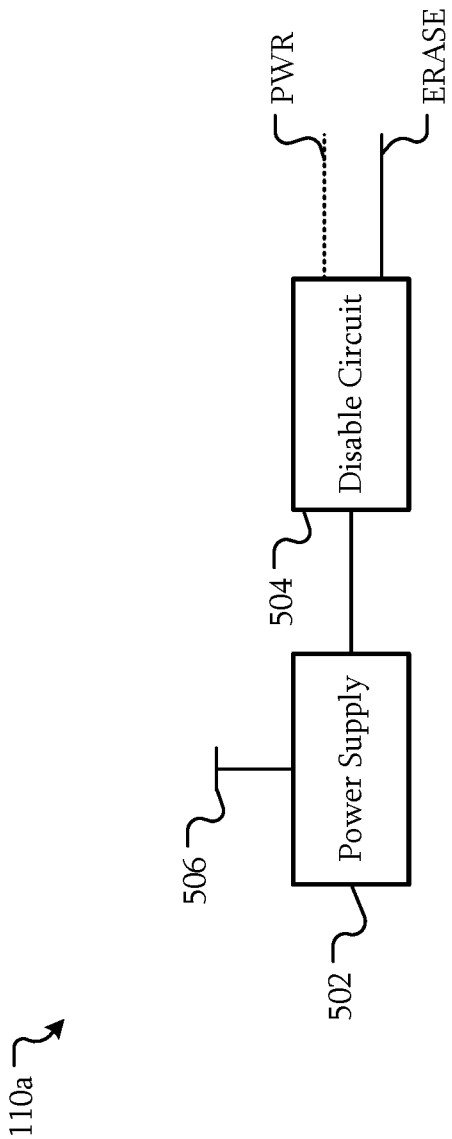


FIG. 5B

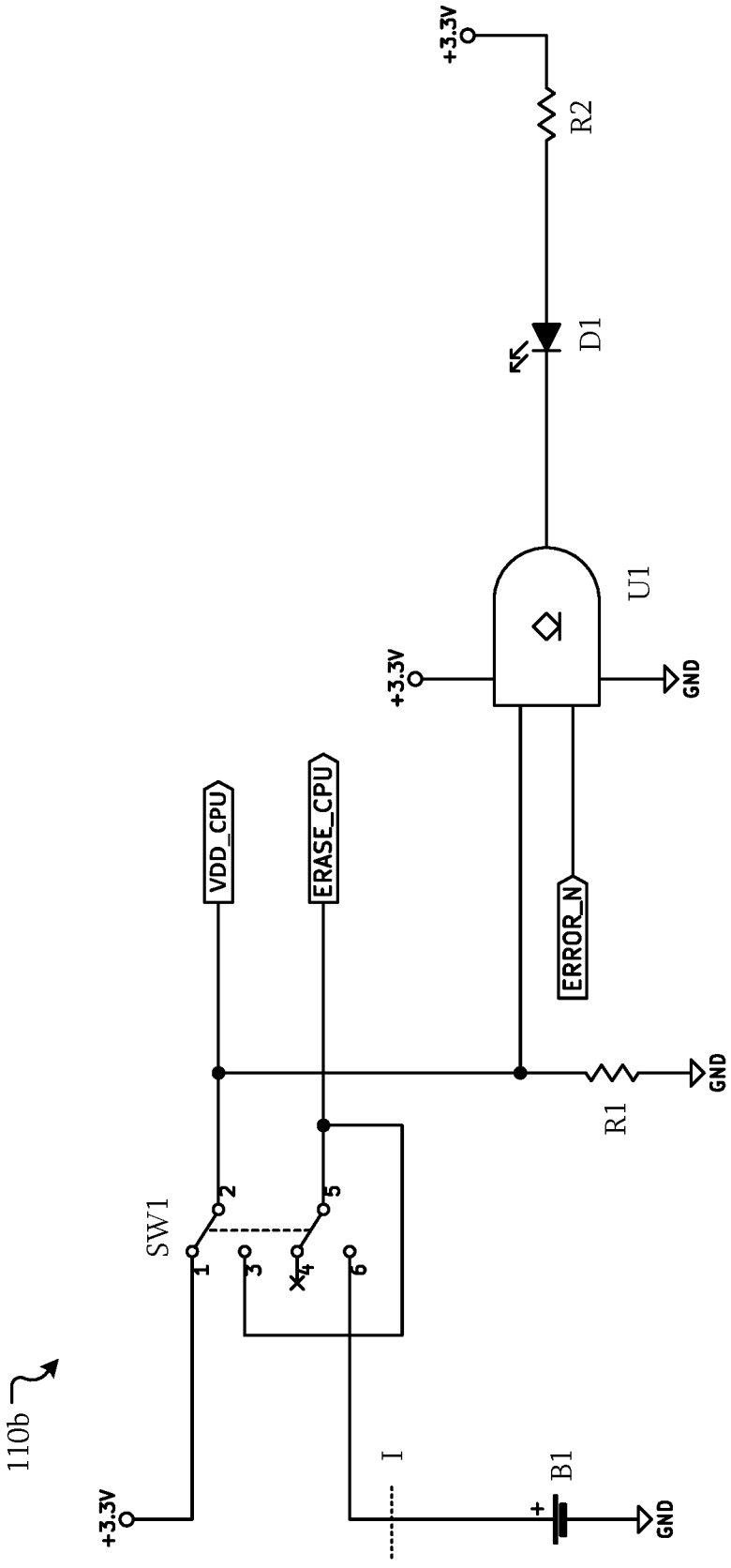

110b
+3.3V
SW1
1
2
3
4
5
6
VDD_CPU
ERASE_CPU
I
B1
+
GND
R1
GND
ERROR_N
+3.3V
U1
GND
D1
R2
+3.3V

FIG. 5C

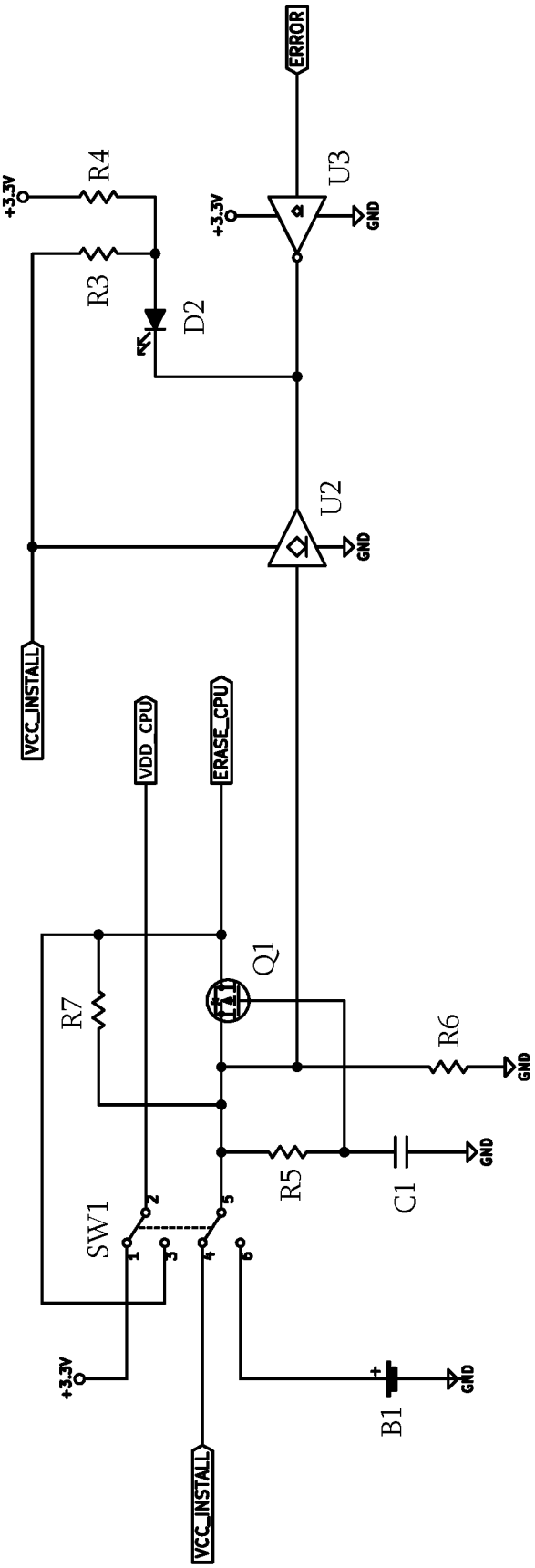

ERROR
U3
+3.3V
GND
R4
R3
D2
U2
VCC_INSTALL
VDD_CPU
ERASE_CPU
Q1
R7
R6
R5
C1
SW1
B1

FIG. 5D

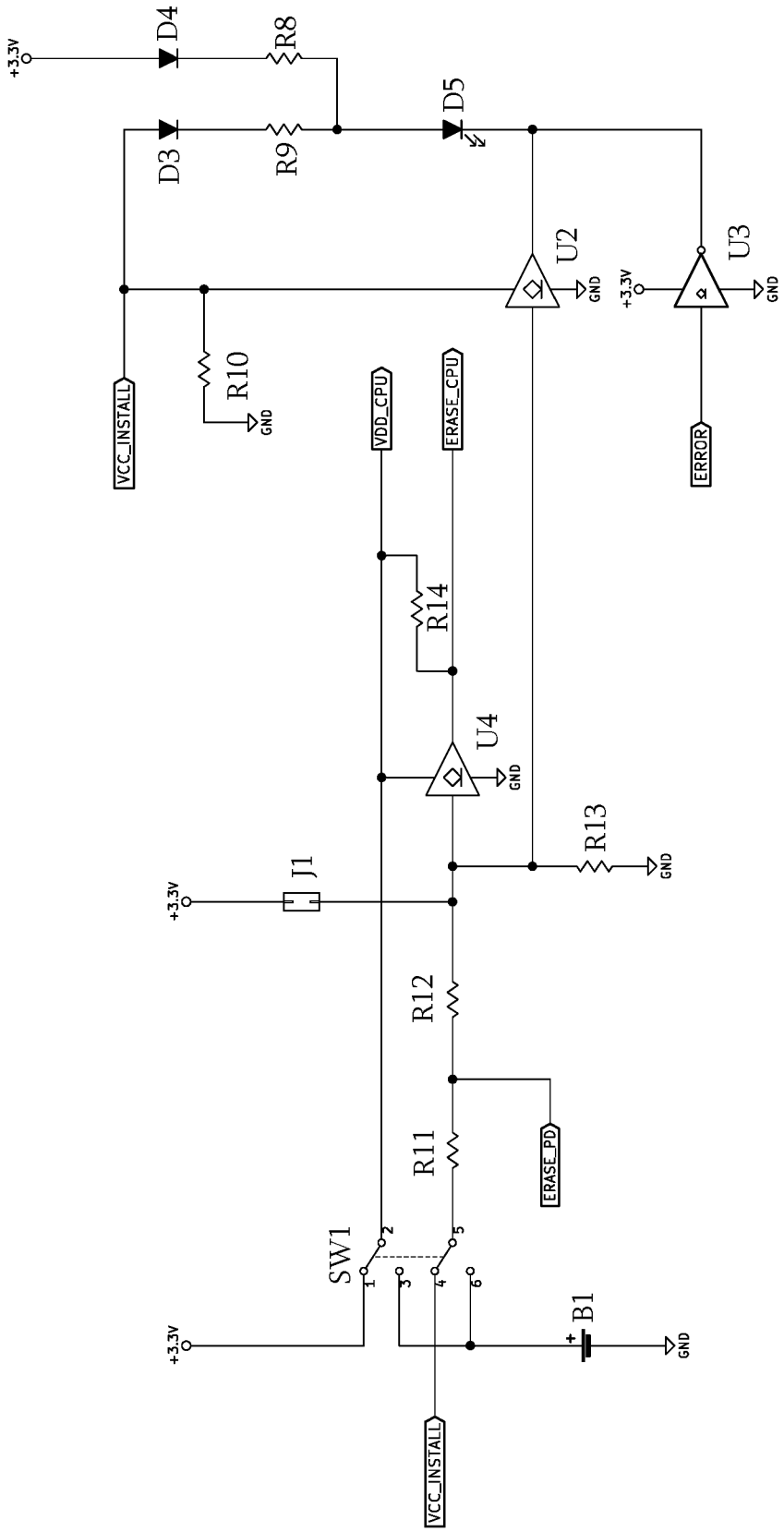

+3.3V
D4
R8
D5
D3
R9
U2
U3
GND
+3.3V
GND
R10
GND
VCC_INSTALL
VDD_CPU
ERASE_CPU
ERROR
R14
U4
GND
R13
GND
J1
+3.3V
R12
R11
ERASE_PD
SW1
1
2
3
4
5
6
+3.3V
B1
GND
VCC_INSTALL

FIG. 6A

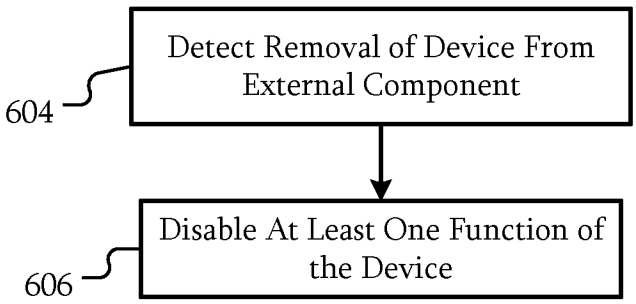

Detect Removal of Device From External Component
604
Disable At Least One Function of the Device
606

FIG. 6B

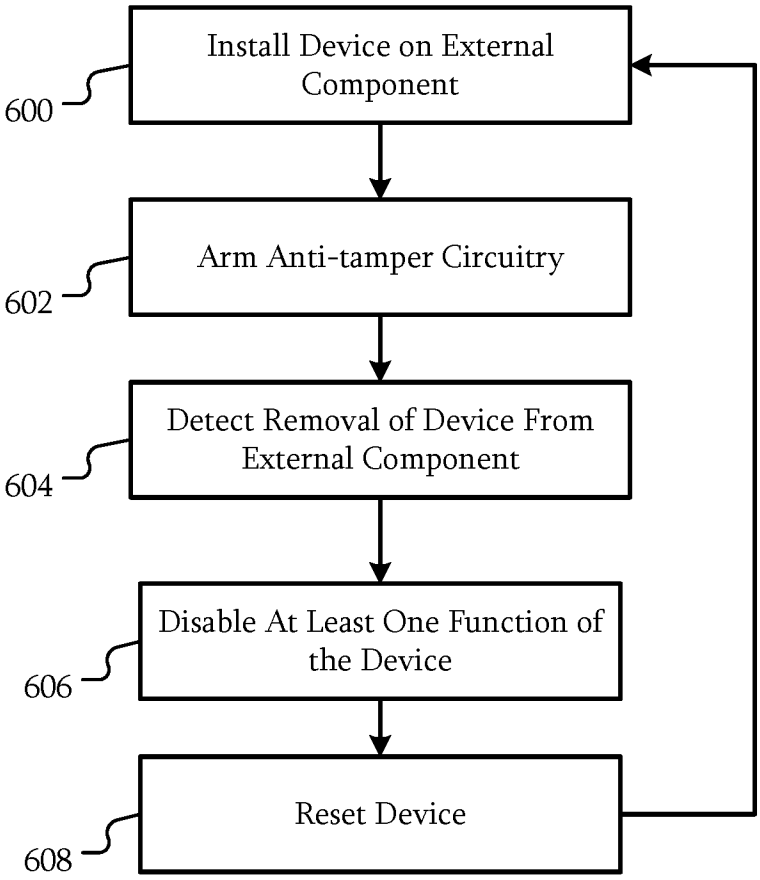

Install Device on External Component
600
Arm Anti-tamper Circuitry
602
Detect Removal of Device From External Component
604
Disable At Least One Function of the Device
606
Reset Device
608

FIG. 7

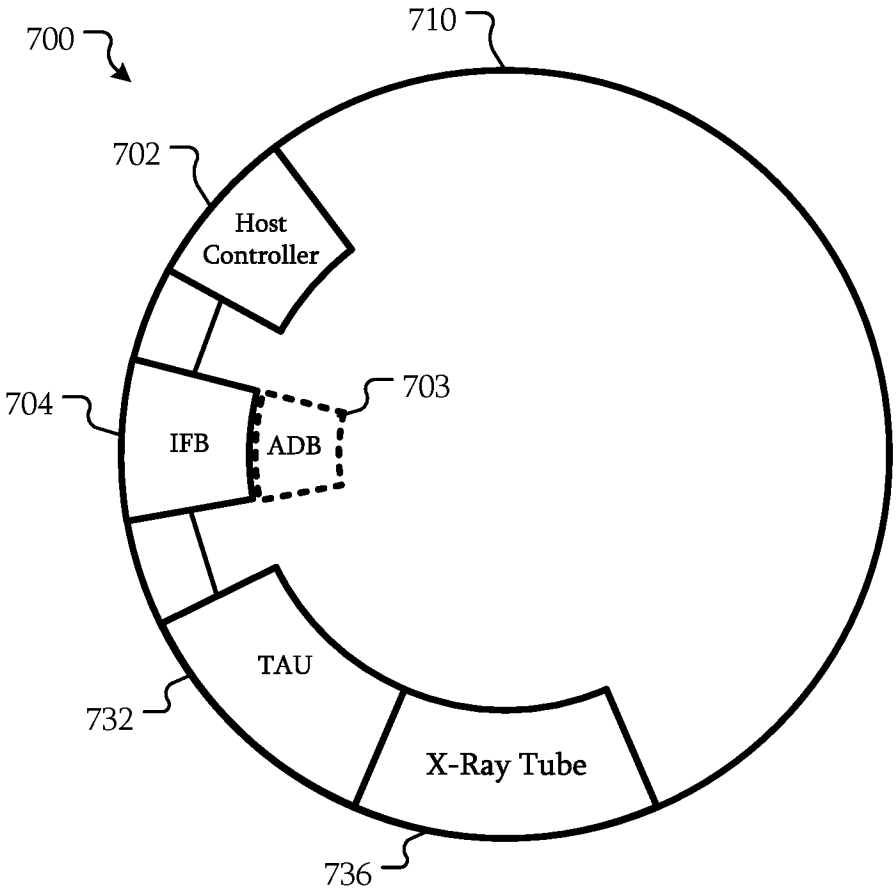

700
710
702
Host Controller
704
IFB
703
ADB
TAU
732
X-Ray Tube
736

FIG. 8A

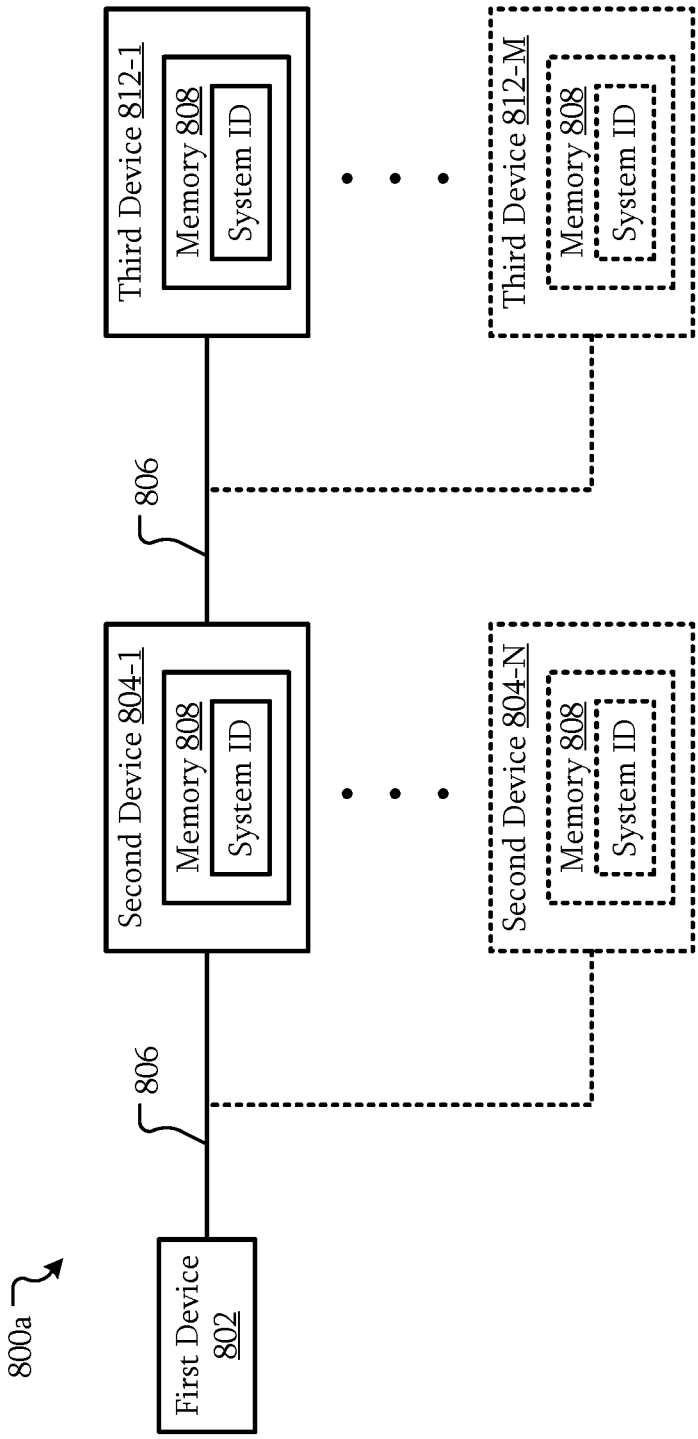

800a
First Device 802
806
Second Device 804-1
Memory 808
System ID
Second Device 804-N
Memory 808
System ID
806
Third Device 812-1
Memory 808
System ID
Third Device 812-M
Memory 808
System ID

FIG. 8B

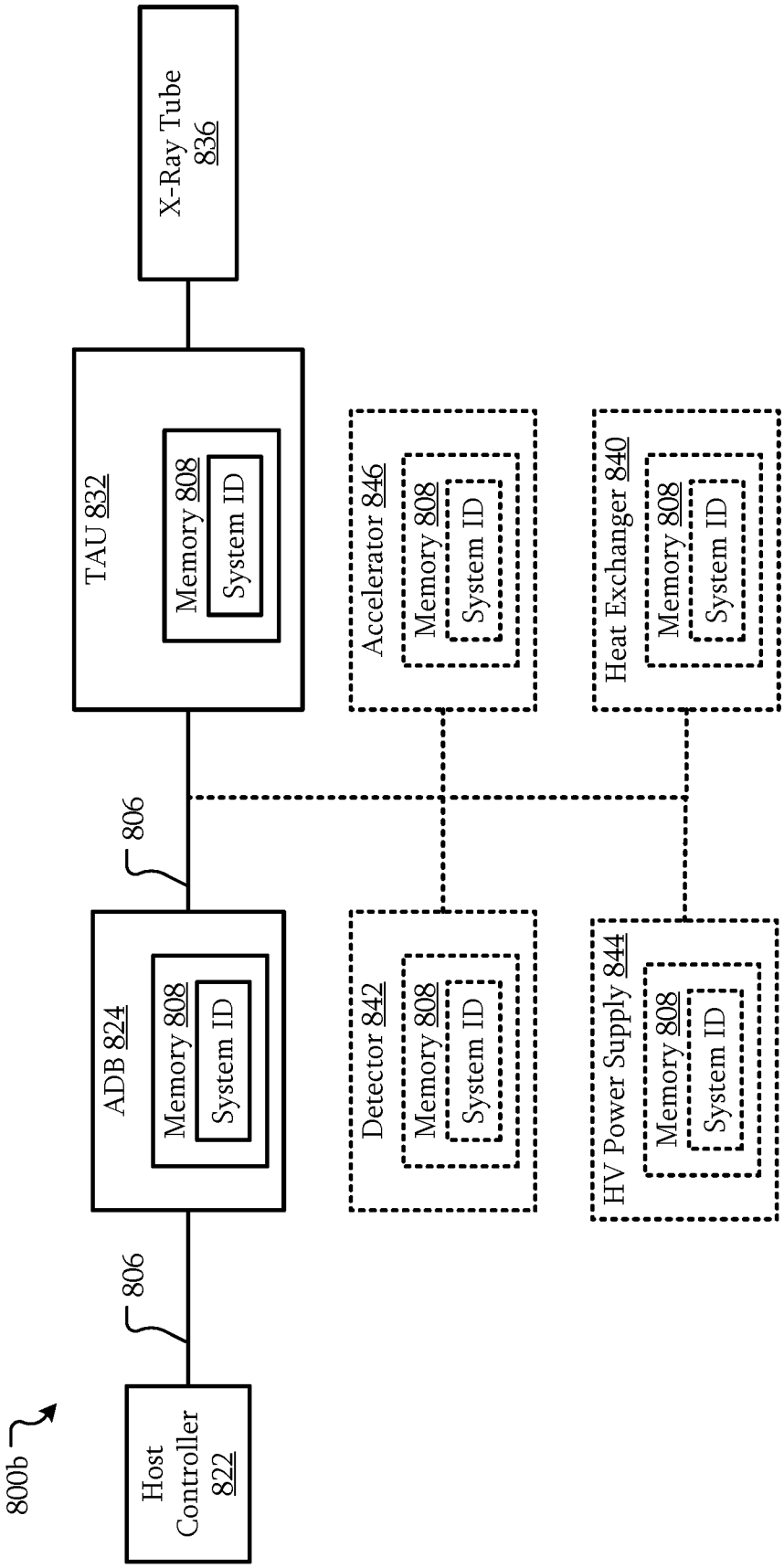

800b
Host Controller 822
806
ADB 824
Memory 808
System ID
806
TAU 832
Memory 808
System ID
X-Ray Tube 836
Detector 842
Memory 808
System ID
Accelerator 846
Memory 808
System ID
HV Power Supply 844
Memory 808
System ID
Heat Exchanger 840
Memory 808
System ID

FIG. 9A

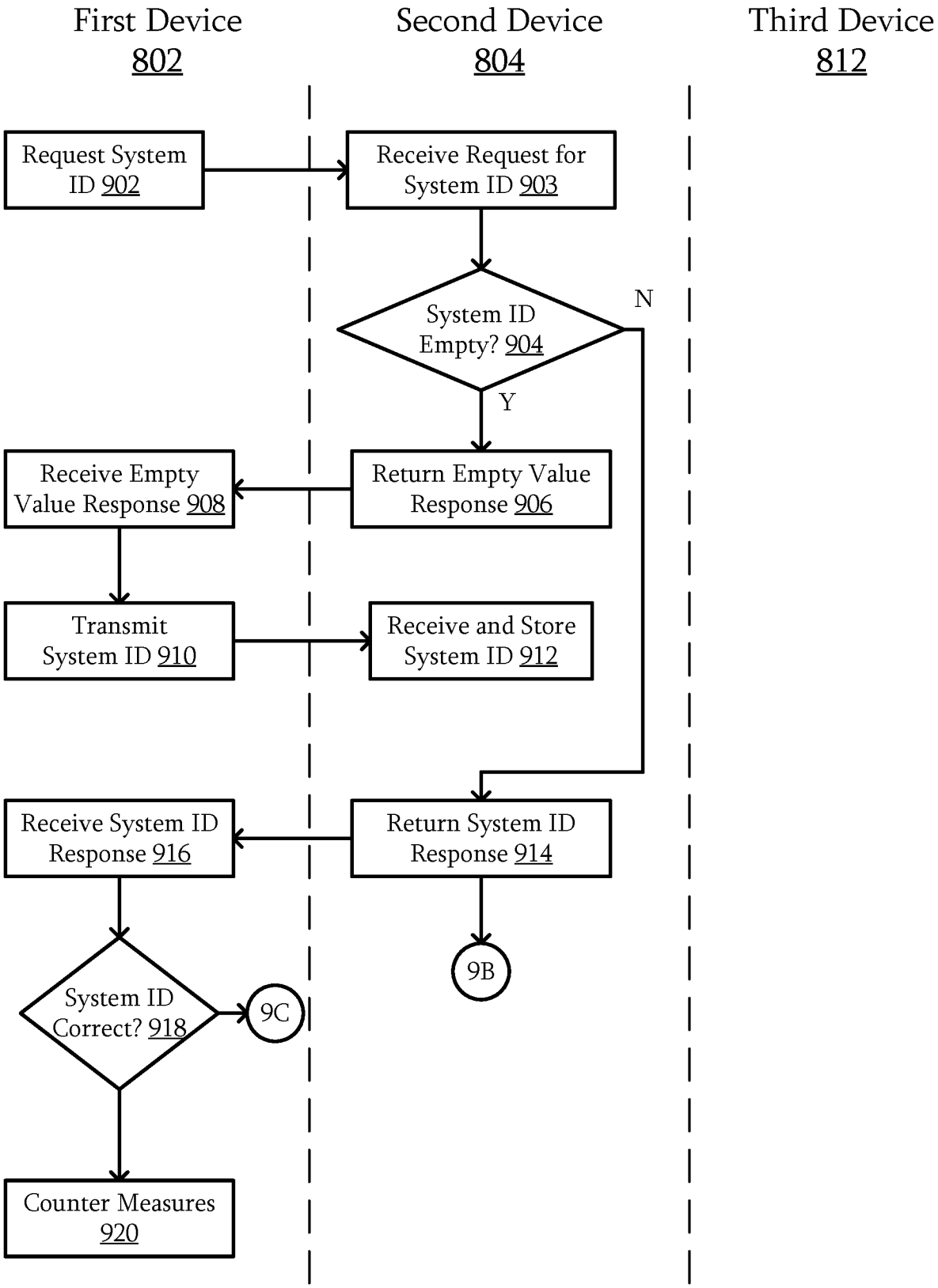

First Device
802
Second Device
804
Third Device
812
Request System ID 902
Receive Request for System ID 903
System ID Empty? 904
N
Y
Receive Empty Value Response 908
Return Empty Value Response 906
Transmit System ID 910
Receive and Store System ID 912
Receive System ID Response 916
Return System ID Response 914
9B
System ID Correct? 918
9C
Counter Measures 920

FIG. 9B

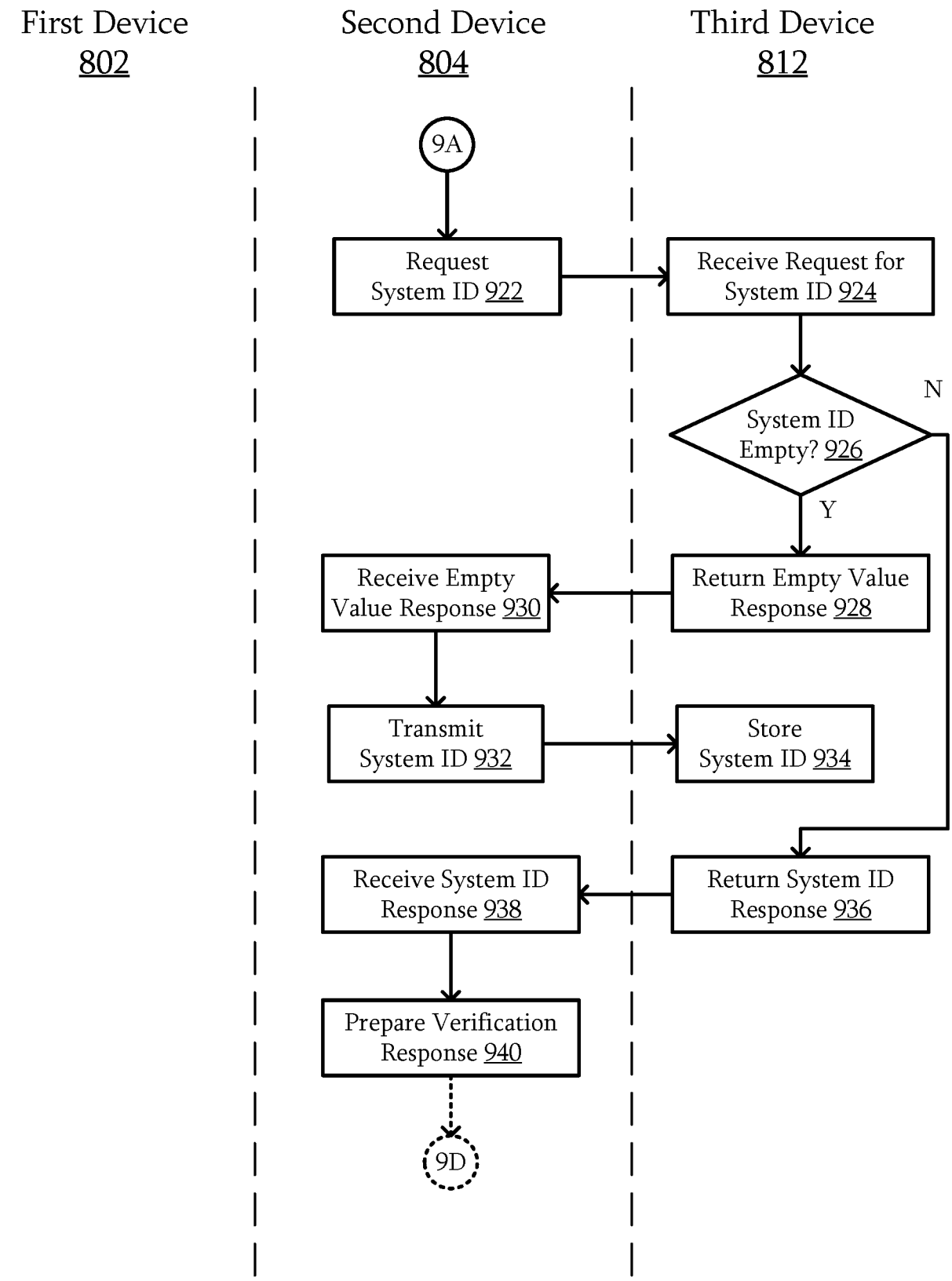

First Device
802
Second Device
804
Third Device
812
9A
Request System ID 922
Receive Request for System ID 924
System ID Empty? 926
N
Y
Return Empty Value Response 928
Receive Empty Value Response 930
Transmit System ID 932
Store System ID 934
Return System ID Response 936
Receive System ID Response 938
Prepare Verification Response 940
9D

FIG. 9C

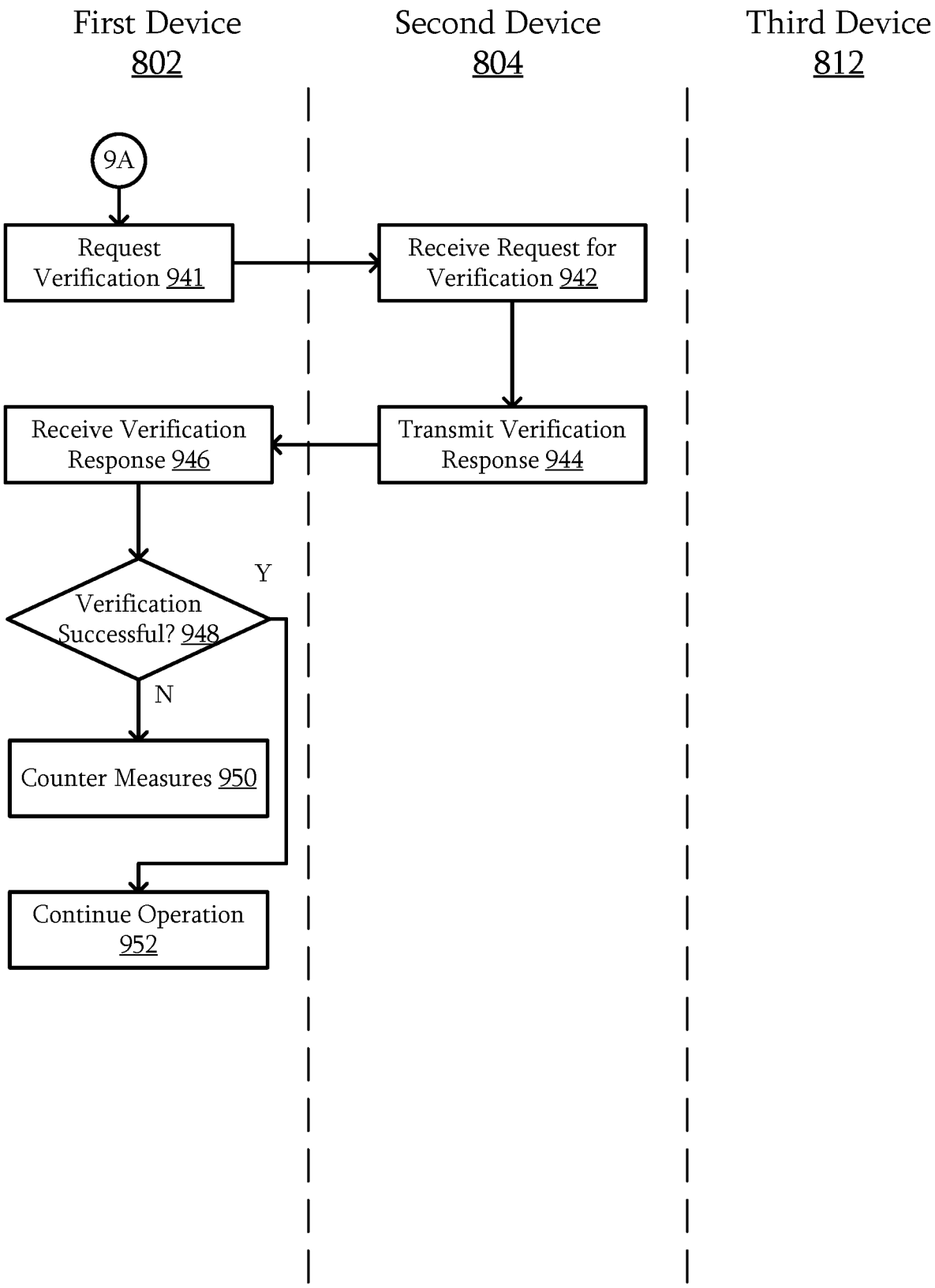

First Device
802
Second Device
804
Third Device
812
9A
Request Verification 941
Receive Request for Verification 942
Transmit Verification Response 944
Receive Verification Response 946
Verification Successful? 948
Y
N
Counter Measures 950
Continue Operation 952

FIG. 9D

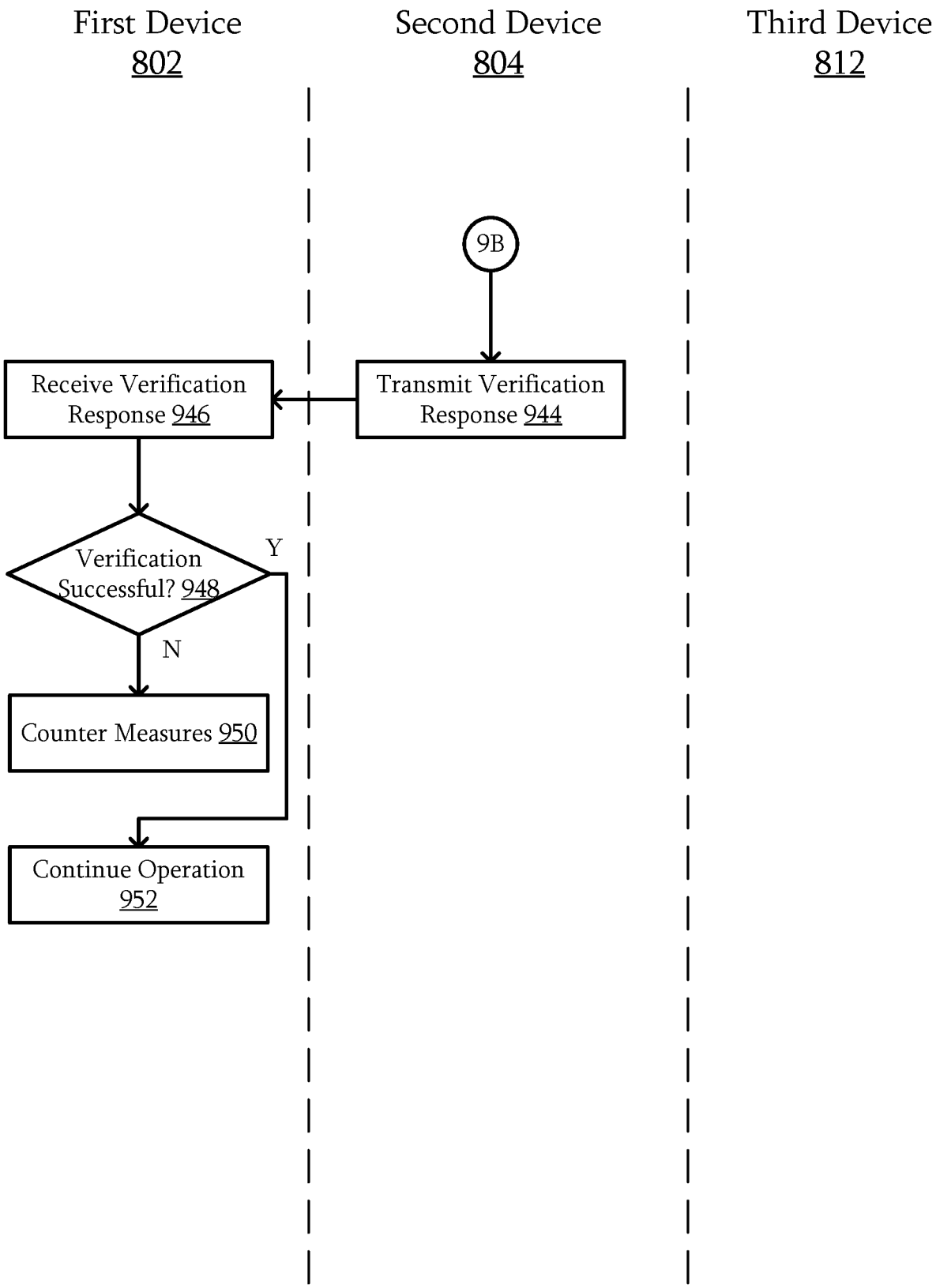

First Device
802
Second Device
804
Third Device
812
9B
Receive Verification Response 946
Transmit Verification Response 944
Verification Successful? 948
Y
N
Counter Measures 950
Continue Operation 952

FIG. 10A

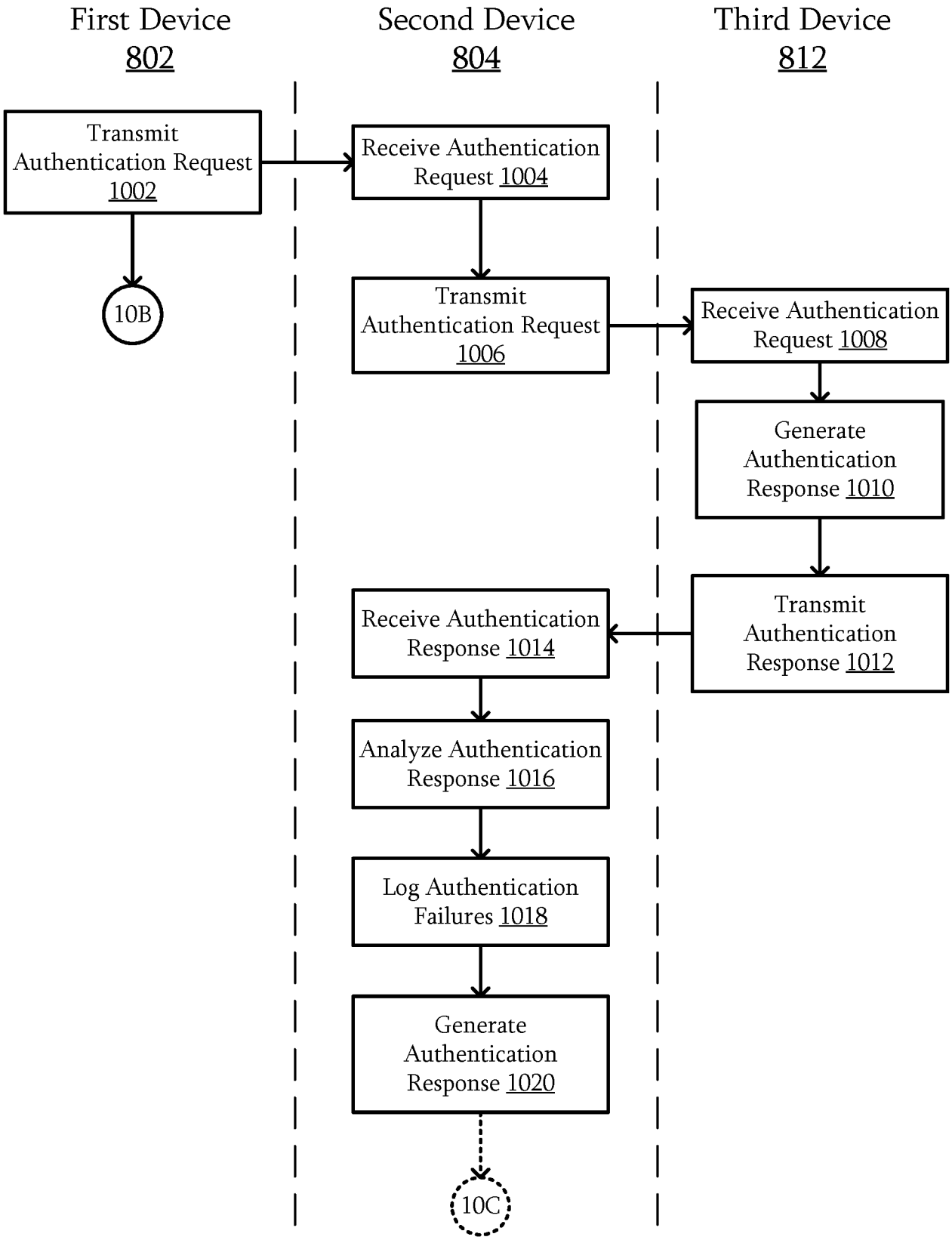

First Device
802
Second Device
804
Third Device
812
Transmit Authentication Request 1002
Receive Authentication Request 1004
10B
Transmit Authentication Request 1006
Receive Authentication Request 1008
Generate Authentication Response 1010
Transmit Authentication Response 1012
Receive Authentication Response 1014
Analyze Authentication Response 1016
Log Authentication Failures 1018
Generate Authentication Response 1020
10C

FIG. 10B

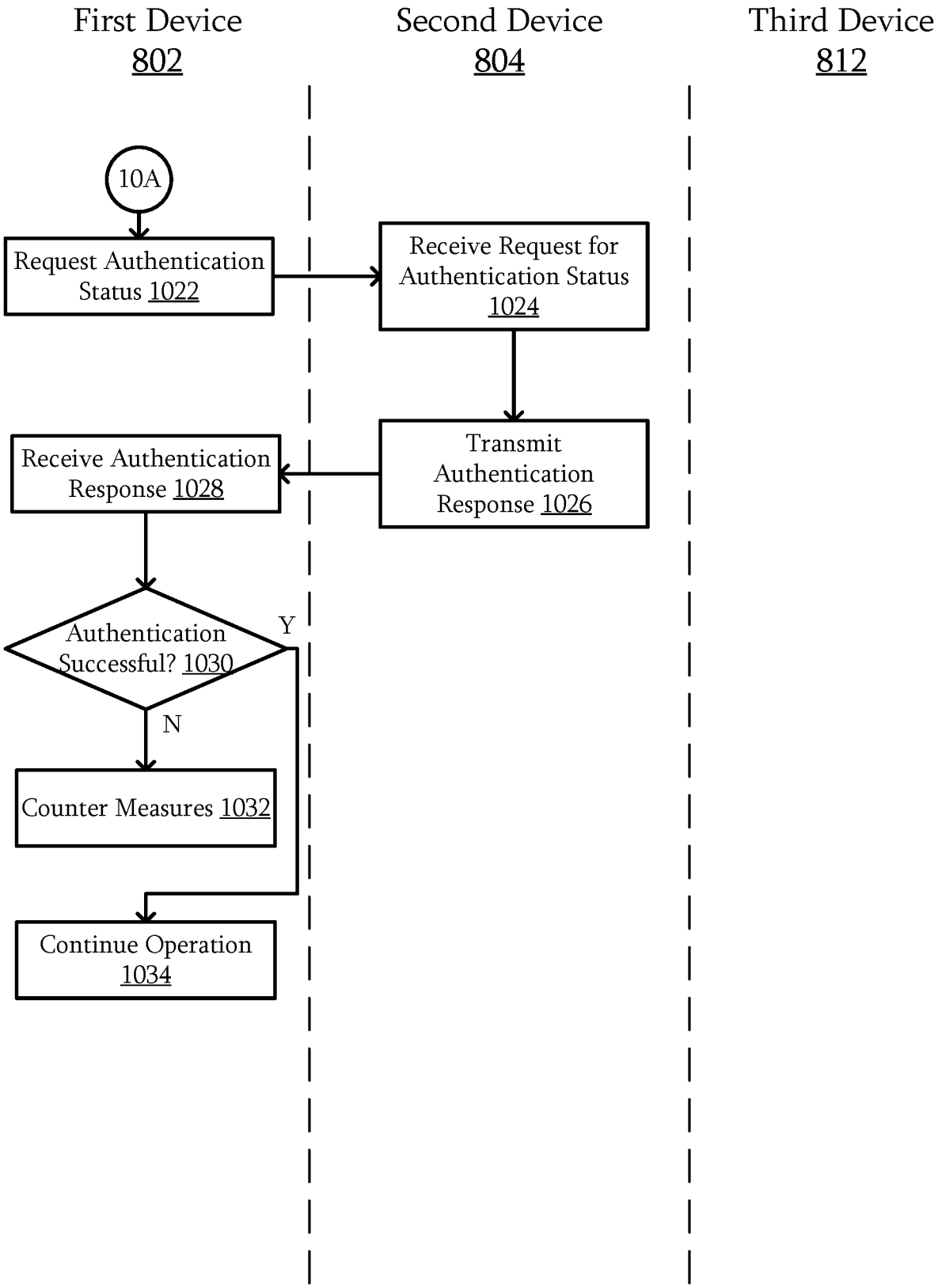
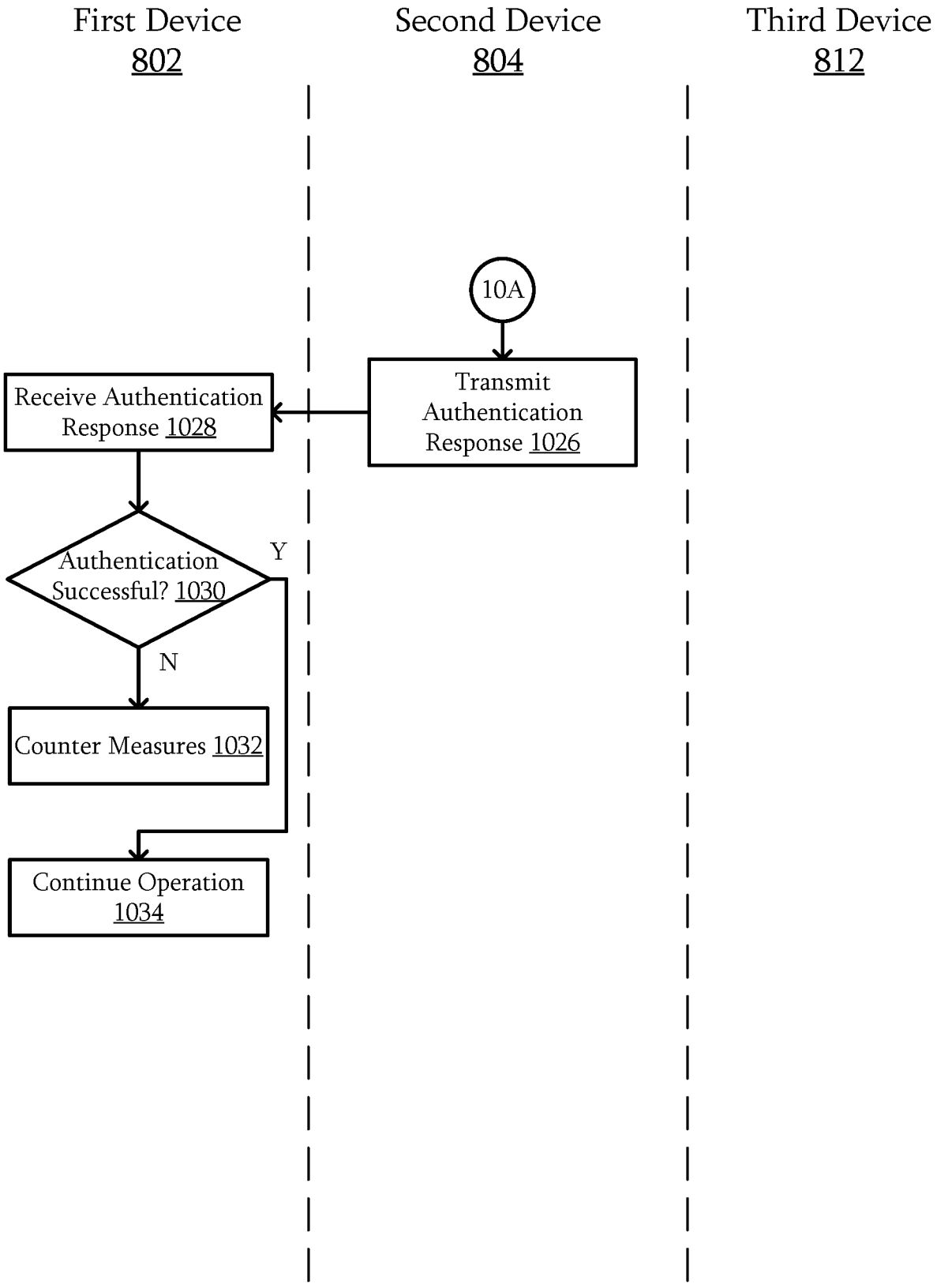

First Device
802
Second Device
804
Third Device
812
10A
Request Authentication Status 1022
Receive Request for Authentication Status 1024
Transmit Authentication Response 1026
Receive Authentication Response 1028
Authentication Successful? 1030
Y
N
Counter Measures 1032
Continue Operation 1034

FIG. 10C


First Device
802
Second Device
804
Third Device
812
10A
Transmit Authentication Response 1026
Receive Authentication Response 1028
Authentication Successful? 1030
Y
N
Counter Measures 1032
Continue Operation 1034

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/048258

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/86(2013.01)i, H01L 23/00(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)
G06F 21/86; G06F 1/26; G06F 21/06; G06F 21/24; G06F 21/87; H01J 35/02; H01J 35/06; H04L 9/10; H01L 23/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: external component, anti-tamper circuitry, remove, disable, power supply, erase

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2012-0131680 A1 (TSUTOMU BABA) 24 May 2012 See paragraphs [0003], [0033]-[0047]; claims 1-3; and figures 1-2.	1-20
Y	US 2013-0283386 A1 (CHEOL JAE LEE) 24 October 2013 See paragraphs [0026]-[0027]; claims 1, 5; and figure 2.	1-20
Y	US 2018-0082818 A1 (VAREX IMAGING CORPORATION) 22 March 2018 See paragraph [0071]; and figure 4.	11-12
A	US 2015-0254478 A1 (EMPIRE TECHNOLOGY DEVELOPMENT LLC) 10 September 2015 See paragraphs [0024], [0026]; claims 1-2, 4; and figure 1A.	1-20
A	JP 2006-229667 A (MATSUSHITA ELECTRIC IND. CO., LTD.) 31 August 2006 See claims 1-3.	1-20

☐ 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
"D" document cited by the applicant in the international application
"E" earlier application or patent 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
17 December 2019 (17.12.2019)	**17 December 2019 (17.12.2019)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
KIM, Sung Hee
Telephone No. +82-42-481-5659

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/048258

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012-0131680 A1	24/05/2012	JP 2011-018247 A	27/01/2011
		JP 5421679 B2	19/02/2014
		US 8745752 B2	03/06/2014
		WO 2011-004829 A1	13/01/2011
US 2013-0283386 A1	24/10/2013	KR 10-2013-0126804 A	21/11/2013
		US 8589703 B2	19/11/2013
		WO 2013-162843 A1	31/10/2013
US 2018-0082818 A1	22/03/2018	CN 107845556 A	27/03/2018
		EP 3297017 A1	21/03/2018
		EP 3297017 B1	13/11/2019
		JP 2018-049813 A	29/03/2018
		US 10297414 B2	21/05/2019
US 2015-0254478 A1	10/09/2015	US 9836625 B2	05/12/2017
		WO 2015-047283 A2	02/04/2015
		WO 2015-047283 A3	16/07/2015
JP 2006-229667 A	31/08/2006	None	