



(86) Date de dépôt PCT/PCT Filing Date: 2015/10/20
(87) Date publication PCT/PCT Publication Date: 2016/04/28
(85) Entrée phase nationale/National Entry: 2017/04/13
(86) N° demande PCT/PCT Application No.: US 2015/056490
(87) N° publication PCT/PCT Publication No.: 2016/064893
(30) Priorités/Priorities: 2014/10/20 (US62/066,083);
2015/07/14 (US62/192,466)

(51) Cl.Int./Int.Cl. *G05B 19/042* (2006.01),
G08C 17/00 (2006.01), *H04N 5/77* (2006.01)

(71) Demandeur/Applicant:
TASER INTERNATIONAL, INC., US

(72) Inventeurs/Inventors:
WAGNER, DANIEL J., US;
HANCHETT, MARK A., US;
KLOC, AARON J., US;
CONANT, TYLER, US

(74) Agent: BERESKIN & PARR LLP/S.E.N.C.R.L.,S.R.L.

(54) Titre : SYSTEMES ET PROCEDES POUR UNE COMMANDE DISTRIBUEE
(54) Title: SYSTEMS AND METHODS FOR DISTRIBUTED CONTROL

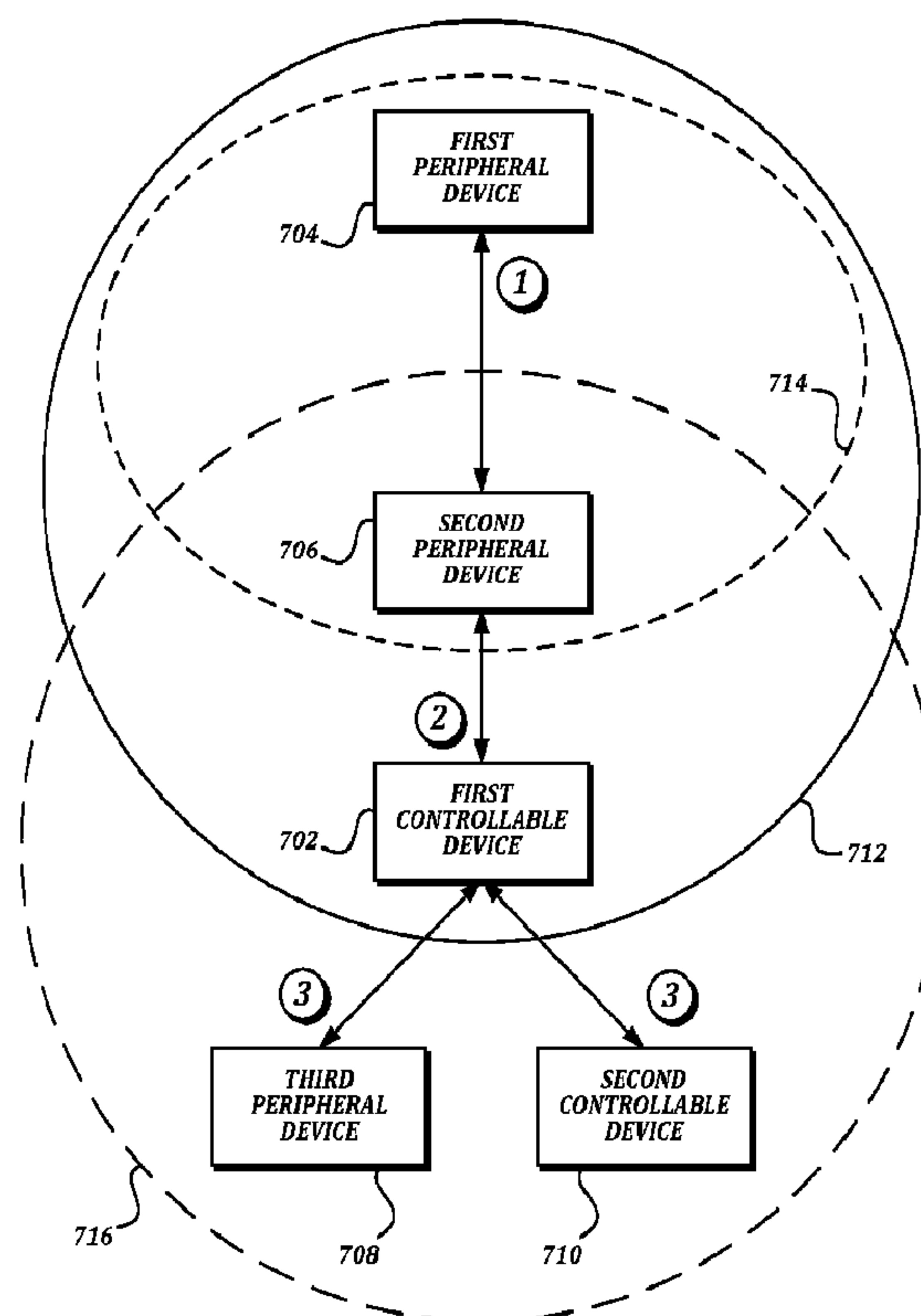


FIG. 7A

(57) Abrégé/Abstract:

Systems involving distributed control functions are described herein. Each member or device within the system has responsibility for controlling part of the system's behavior, and includes logic to determine what action, if any, will follow as a response to

(57) **Abrégé(suite)/Abstract(continued):**

determining information or receiving information from other members or devices within the system. A change of status of one member of a system may provide a basis for action by another member of the system. Status may be the result of sensing a condition of the environment, sensing the condition of a component, receiving the output of a conventional sensor, and/or sensing the condition of a link between components. In some embodiments, action taken by a member of the system may include collecting data during law enforcement activities.

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

(19) World Intellectual Property
Organization
International Bureau(10) International Publication Number
WO 2016/064893 A1(43) International Publication Date
28 April 2016 (28.04.2016)

(51) International Patent Classification:

H04W 4/00 (2009.01) *H04N 21/436* (2011.01)
H04N 21/422 (2011.01) *H04N 21/4363* (2011.01)

(21) International Application Number:

PCT/US2015/056490

(22) International Filing Date:

20 October 2015 (20.10.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/066,083 20 October 2014 (20.10.2014) US
 62/192,466 14 July 2015 (14.07.2015) US

(71) Applicant: **TASER INTERNATIONAL, INC.** [US/US];
17800 North 85th Street, Scottsdale, AZ 85255 (US).(72) Inventors: **WAGNER, Daniel, J.**; c/o TASER International, Inc., 17800 North 85th Street, Scottsdale, AZ 85255 (US). **HANCHETT, Mark, A.**; c/o TASER International, Inc., 17800 North 85th Street, Scottsdale, AZ 85255 (US). **KLOC, Aaron, J.**; c/o TASER International, Inc., 17800 North 85th Street, Scottsdale, AZ 85255 (US). **CONANT,****Tyler**; c/o TASER International, Inc., 17800 North 85th Street, Scottsdale, AZ 85255 (US).(74) Agent: **LETHAM, Lawrence, D.**; TASER International, Inc., 17800 North 85th Street, Scottsdale, AZ 85255 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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,

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR DISTRIBUTED CONTROL

(57) Abstract: Systems involving distributed control functions are described herein. Each member or device within the system has responsibility for controlling part of the system's behavior, and includes logic to determine what action, if any, will follow as a response to determining information or receiving information from other members or devices within the system. A change of status of one member of a system may provide a basis for action by another member of the system. Status may be the result of sensing a condition of the environment, sensing the condition of a component, receiving the output of a conventional sensor, and/or sensing the condition of a link between components. In some embodiments, action taken by a member of the system may include collecting data during law enforcement activities.

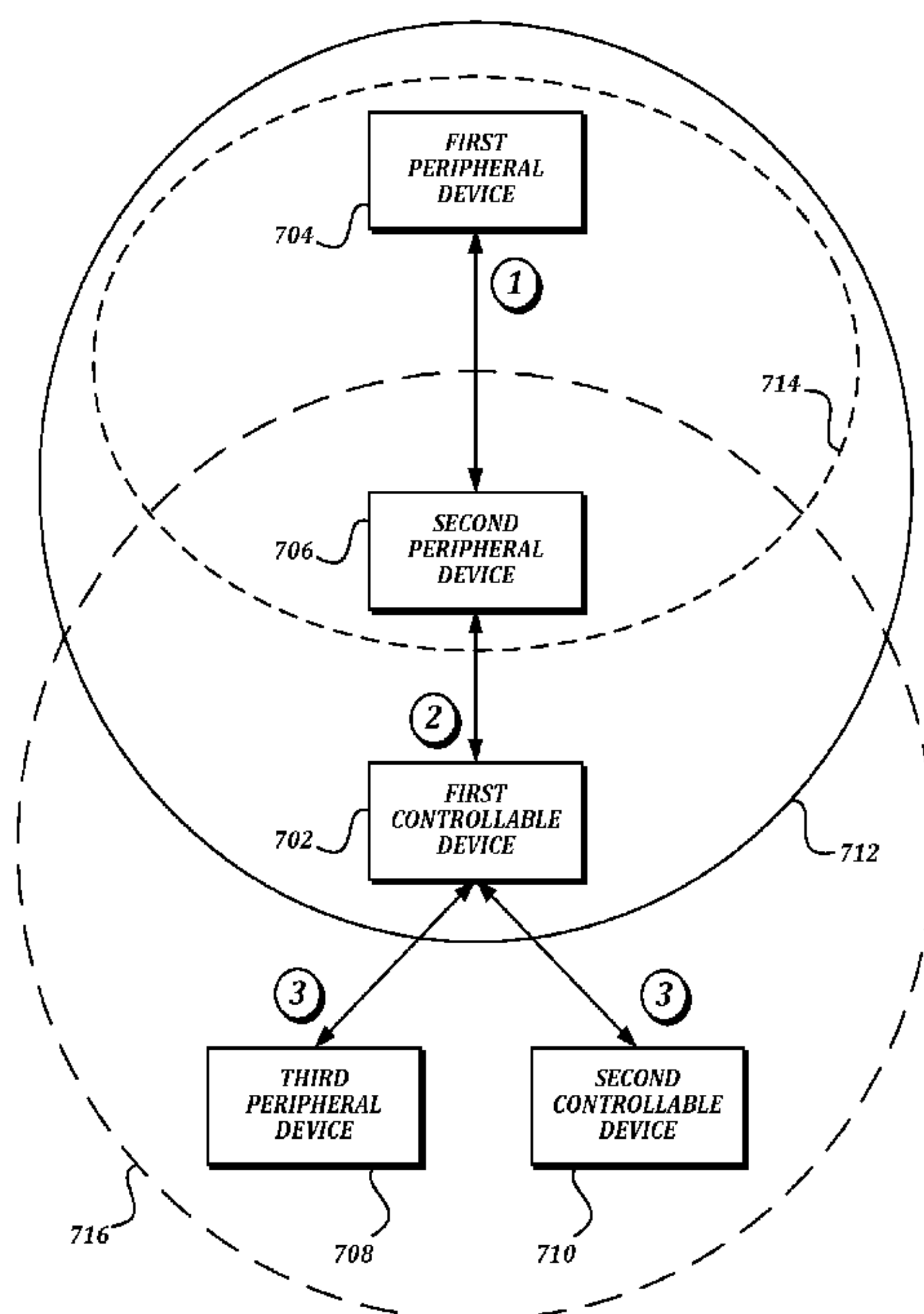


FIG. 7A

WO 2016/064893 A1

WO 2016/064893 A1



SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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

SYSTEMS AND METHODS FOR DISTRIBUTED CONTROL

CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims the benefit of Provisional Application No. 62/066083,
5 filed October 20, 2014, and Provisional Application No. 62/192466, filed July 14, 2015,
the entire disclosures of which are hereby incorporated by reference herein.

BACKGROUND

Existing techniques for controlling devices in a system, such as wearable cameras
10 operating in a law enforcement context, have various shortcomings. For example, some
existing systems require a recording state of a camera to be manually changed by its user.
This can lead to video not being recorded for important incidents because a user is too
distracted by urgent events that require attention to operate the camera, or for other
reasons. What is needed are effective systems and methods for distributed control of
15 wearable cameras and other controllable devices that do not require manual control by a
user, but instead allow settings on the controllable devices to be changed in response to
events that can automatically be detected.

SUMMARY

20 This summary is provided to introduce a selection of concepts in a simplified
form that are further described below in the Detailed Description. This summary is not
intended to identify key features of the claimed subject matter, nor is it intended to be
used as an aid in determining the scope of the claimed subject matter.

In some embodiments, a system comprising a first peripheral device and a
25 controllable device is provided. The first peripheral device is configured to broadcast a
first notification indicating an availability of first information generated by the first
peripheral device, and to transmit the first information in response to a request for the
first information. The controllable device is configured to receive the first notification
from the first peripheral device; in response to the first notification, transmit a request for
30 the first information to the first peripheral device; and in response to the first information
received from the first peripheral device, change at least one setting of the controllable
device based on the first information.

In some embodiments, a controllable device is provided. The controllable device comprises a short-range wireless interface and a notification processing engine. The notification processing engine is configured to receive a first notification from a first peripheral device via the short-range wireless interface; and in response to a
5 determination that the controllable device should process the first notification, change at least one setting of the controllable device based on the first notification.

In some embodiments, a method of processing received signals for control of a controllable device is provided. The method comprises receiving, by the controllable device, a first notification from a first peripheral device; and in response to determining
10 that the controllable device should process the first notification, changing at least one setting of the controllable device based on the first notification.

DESCRIPTION OF THE DRAWINGS

The foregoing aspects and many of the attendant advantages of this invention will
15 become more readily appreciated as the same become better understood by reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

FIGURE 1 is a high-level schematic diagram that illustrates communication between various components of an exemplary embodiment of a system according to
20 various aspects of the present disclosure;

FIGURE 2 is a block diagram that illustrates an exemplary embodiment of a controllable device according to various aspects of the present disclosure;

FIGURE 3 is a block diagram that illustrates components of an exemplary embodiment of a controllable camera device according to various aspects of the present
25 disclosure;

FIGURE 4 is a block diagram that illustrates an exemplary embodiment of a peripheral device according to various aspects of the present disclosure;

FIGURE 5 is a block diagram that illustrates a light bar peripheral device according to various aspects of the present disclosure;

30 FIGURE 6 is a block diagram that illustrates an exemplary embodiment of a command peripheral device according to various aspects of the present disclosure;

FIGURES 7A-7C are high-level schematic diagrams of exemplary embodiments of communication between devices according to various aspects of the present disclosure;

FIGURES 8A-8C are a flowchart that illustrates an exemplary embodiment of a method of transmitting and processing event notifications according to various aspects of the present disclosure;

FIGURE 9 is a flowchart that illustrates a procedure for transmitting a notification
5 from a device according to various aspects of the present disclosure; and

FIGURE 10 is a block diagram that illustrates aspects of an exemplary computing device appropriate for use as a computing device of the present disclosure.

DETAILED DESCRIPTION

10 In a system involving central control functions, the central (or federated) part of the system issues commands to other parts of the system and those parts take action in accordance with the received commands. The part that makes decisions and issues commands may be referred to as the master. The part or parts that perform commands may be referred to as slaves. By contrast, in a system involving distributed control
15 functions such as the systems described herein, each member or device within the system that has responsibility for controlling part of the system's behavior includes logic to determine what action, if any, will follow as a response to determining information (e.g., passage of time, results of computation) or receiving information (e.g., one or more notice(s) of change(s) in status(es)). In systems that involve distributed control functions,
20 a change of status of one member of a system may provide a basis for action by another member of the system. Status may be the result of sensing a condition of the environment, sensing the condition of a component, receiving the output of a conventional sensor, and/or sensing the condition of a link between components. When a member of a system receives an indication that status has changed, action taken in
25 response may be determined by logic implemented in that member of the system.

A condition of a component may include a physical condition including but not limited to temperature, physical location or movement, configuration, capacity to perform, response time, forecast of capability, operating mode, faults encountered, inputs received, received messages, and results of computation. A condition of a link between
30 components may include but is not limited to an operating electrical parameter, a description of establishing connection, a disconnection, a mode of communication, a network capacity, a latency, a description of a queue or buffer, a description of message

routing, an extent of noise, a time allotment, and a description of a node (e.g., control, dormant, active, in range).

In some embodiments, recorded data is collected during law enforcement activities (e.g., traffic stops, incidents where police are dispatched to investigate or
5 enforce the law, unmanned traffic monitoring). This class of embodiments will be used below to describe systems, methods, and communication that may be implemented in an analogous manner in a system used for other purposes, for example, any quantity of users who desire to record data during their chosen activities (e.g., first responders, surgical teams, sports teams, military operatives, security officers, social event managers, news
10 reporting, film production, music production, classroom instruction, consumer surveys, group interviews). An officer is a user as discussed below.

FIGURE 1 is a high-level schematic diagram that illustrates communication between various components of an exemplary embodiment of a system according to various aspects of the present disclosure. In some embodiments, the system 100 is
15 configured to allow for distributed control of various devices within the system 100.

In general, a user 92, such as a law enforcement officer, may be associated with one or more devices. The devices may include, but are not limited to, a camera 106, a weapon 108, and various devices associated with a vehicle 94 such as a light bar device 110. The camera 106 may be, for example, a wearable camera that records video
20 and/or audio data when activated. The weapon 108 may be, for example, a conducted energy weapon (CEW) that transmits notifications regarding events such as firing events, cartridge loading, holster removal, and/or the like. The light bar device 110 may detect changes in state such as activation of the light bar on the vehicle 94, which is usually associated with an emergency situation. Other devices, such as a dashboard camera, a
25 heart rate sensor device, a holster sensor device, and/or the like may also be included in the system 100 but are not illustrated in FIGURE 1.

In some embodiments, at least some of the devices may have limited communication functionality. For example, devices may have short-range wireless communication abilities, but some devices may only be able to perform a direct long-
30 range transmission or reception of information, such as to an evidence management system 102, when physically connected to an evidence collection dock 104 that communicates with the evidence management system 102 via a broadband network 90 such as a LAN, a WAN, and/or the Internet. Accordingly, technical problems arise when

attempting to control the devices in an automated manner, at least in that no reliable communication path from a central control device to the controllable devices is available. In some embodiments, a personal assistant computing device 107 is provided. The personal assistant computing device 107 is illustrated as a smartphone computing device, but in some embodiments may be a laptop computing device, a tablet computing device, or any other suitable computing device capable of being carried by the user 92 or a vehicle 94 associated with the user 92 and capable of performing the actions described herein. The personal assistant computing device 107 may be capable of short-range communication with the other devices in the system 100, and may also be capable of long range communication with the evidence management system 102, a dispatch system, or any other system. In some embodiments, the personal assistant computing device 107 has the components and capabilities of a peripheral device 706 and/or a controllable device 702 as discussed below. Further aspects of these devices and their capabilities will be discussed below.

FIGURE 2 is a block diagram that illustrates an exemplary embodiment of a controllable device according to various aspects of the present disclosure. As illustrated, the controllable device 702 includes a short-range wireless interface 202. The short-range wireless interface 202 may be configured to use any suitable wireless networking technology capable of wirelessly exchanging data with other devices within range of the controllable device 702, including but not limited to Bluetooth (including Bluetooth Low Energy), ZigBee, NFC, and/or the like.

As illustrated, the controllable device 702 also includes a notification generation engine 204, an information transmission engine 206, a notification repeater engine 208, and a notification processing engine 210. In general, the term "engine" as used herein refers to logic embodied in hardware or software instructions, which can be written in a programming language, such as C, C++, COBOL, JAVA™, PHP, Perl, HTML, CSS, JavaScript, VBScript, ASPX, Microsoft .NET™ languages such as C#, and/or the like. An engine may be compiled into executable programs or written in interpreted programming languages. Engines may be callable from other engines or from themselves. Generally, the engines described herein refer to modules that can be merged with other engines to form a single engine, or can be divided into multiple sub-engines. The engines may be embodied in any type of circuit such as an FPGA or an ASIC; and/or may be stored in any type of computer-readable medium or computer storage device and

be stored on and executed by one or more general purpose computers, thus creating a special purpose computer configured to provide the engine. Accordingly, the devices and systems illustrated herein include one or more computing devices configured to provide the illustrated engines, though the computing devices themselves have not been illustrated
5 in every case for the sake of clarity.

In some embodiments, the notification generation engine 204 is configured to create and transmit new notifications based on information obtained by components of the controllable device 702. In some embodiments, the information transmission engine 206 is configured to respond to requests for information associated with
10 notifications after notifications have been transmitted by the notification generation engine 204 and received by other devices. In some embodiments, the notification repeater engine 208 is configured to create and transmit notifications based on notifications received by the controllable device 702 from other devices. In some
15 embodiments, the notification processing engine 210 is configured to analyze notifications received from other devices via the short-range wireless interface 202, and to determine whether a setting of the controllable device 702 should be changed in response to the notifications. In some embodiments, the notification processing engine 210 is also configured to filter notifications for selective retransmission. Further
description of the configuration of and actions performed by these components is
20 provided below.

One of ordinary skill in the art will recognize that, though components common to all controllable devices are illustrated in FIGURE 2, in some embodiments, particular controllable devices may include additional components. For example, FIGURE 3 is a block diagram that illustrates components of an exemplary embodiment of a controllable
25 camera device according to various aspects of the present disclosure. In some embodiments, the controllable camera device 752 is a wearable camera that provides a point of view associated with the user 92. In some embodiments, the controllable camera device 752 may be attached to another device carried by the user 92, such as a weapon.

Because the controllable camera device 752 is a type of controllable device 702, it
30 includes a short-range wireless interface 202, a notification generation engine 204, an information transmission engine 206, a notification repeater engine 208, and a notification processing engine 210 as described above. Further, as with any camera, the controllable camera device 752 includes at least a video sensor 302, and may also include

an audio sensor 306. Data collected by the video sensor 302 and the audio sensor 306 may be stored in a video data store 322 and an audio data store 324, respectively, though in some embodiments the audio and video information is stored together in a single data store and/or in a combined data file. One example of an appropriate video sensor is a charge-coupled device (CCD), though any other digital image sensor, such as a complementary metal-oxide-semiconductor (CMOS) sensor, an active pixel sensor, or any other type of digital image sensor could be used instead. Any type of microphone may be used as an audio sensor 306.

As understood by one of ordinary skill in the art, a "data store" as described herein may be any suitable device configured to store data for access by a computing device. One example of a data store suitable for use with the high capacity needs of the evidence management system 102 is a highly reliable, high-speed relational database management system (RDBMS) executing on one or more computing devices and accessible over a high-speed network. However, any other suitable storage technique and/or device capable of quickly and reliably providing the stored data in response to queries may be used, such as a key-value store, an object database, and/or the like. Further, for the evidence management system 102, the computing device providing the data store may be accessible locally instead of over a network, or may be provided as a cloud-based service. A data store may also include data stored in an organized manner on a computer-readable storage medium, as described further below. One example of a data store suitable for use with the needs of the controllable camera device 752, which includes reliable storage but also low overhead, is a file system or database management system that stores data in files (or records) on a computer-readable medium such as flash memory, random access memory (RAM), hard disk drives, and/or the like. One of ordinary skill in the art will recognize that separate data stores described herein may be combined into a single data store, and/or a single data store described herein may be separated into multiple data stores, without departing from the scope of the present disclosure.

The controllable camera device 752 also includes a camera control engine 304. The camera control engine 304 is configured to change settings of the controllable camera device 752 and thereby cause the controllable camera device 752 to perform camera functions. For example, the camera control engine 304 may cause the video sensor 302 and audio sensor 306 to begin obtaining data, and may cause the video and/or audio data to be saved in a video data store 322 and/or audio data store 324 after

receiving it from the sensor. The camera control engine 304 may receive commands to start, pause, or stop the video recording from a physical user interface device of the controllable camera device 752, or may automatically start, pause, or stop the video recording in response to an instruction received from, for example, the notification
5 processing engine 200 related to a notification received via the short-range wireless interface 202. The camera control engine 304 may also change settings on the video sensor 302 and/or audio sensor 306 in response to such instructions, such as an image quality, a white balance setting, a gain, and/or any other video or audio recording setting. Starting video recording may include transitioning from a pre-trigger mode, wherein
10 video data and/or audio data is saved in a pre-trigger buffer such as a ring buffer, to a post-trigger mode wherein video data and/or audio data is saved in the video data store 322 and/or the audio data store 324. Likewise, stopping video recording may include transitioning from the post-trigger mode to the pre-trigger mode.

In some embodiments, the camera control engine 304 may record events relating
15 to starting, pausing, or stopping the video recording, as well as the settings for the video sensor 302 and audio sensor 306, in an audit trail data store 316. In some embodiments, the camera control engine 304 may embed the sensor configuration information in the data stored in the video data store 322 and/or audio data store 324, along with other information about the state of the controllable camera device 752. The notification
20 processing engine 210 may likewise store records of received notifications and/or information, and the notification generation engine 204 may likewise store records of generated notifications and/or information, in the audit trail data store 316, the video data store 322, and/or the audio data store 324.

The controllable camera device 752 may also include a number of general
25 components, including a motion sensor 338, a physical dock interface 332, and a battery sensor 334. The motion sensor 338, such as a multi-axis accelerometer, produces information that may be used by other components. For example, the notification generation engine 204 may use the motion sensor 338 to detect a certain types of motion, such as running, falling, and/or the like, and to generate notifications announcing when
30 particular types of motion are detected.

The physical dock interface 332 is configured to mate with a physical connector on the evidence collection dock 104. In some embodiments, the physical dock interface 332 may include a female 2.5mm socket, which mates with a male 2.5mm plug

of the evidence collection dock 104. Once docked, the controllable camera device 752 may then transfer data to the evidence management system 102 via the connection using any suitable data transmission protocol. In some embodiments, power may be transferred to the controllable camera device 752 via the physical dock interface 332 instead of or in addition to the data transfer. In some embodiments, other connection hardware that can provide both power and data connectivity may be used, such as a USB connector, a USB Type-C connector, a Firewire connector, and/or the like.

The battery sensor 334 is another example of an internal system that may generate events that are monitored by the notification generation engine 204 for the generation of notifications. For example, the battery sensor 334 may detect a low battery state, a battery overheating state, and/or the like, and may provide alerts to the notification generation engine 204 for the generation of notifications. Other well-known internal device systems, such as a file system controller, a free-fall sensor, and/or the like, may similarly provide alerts to the notification generation engine 204, but are not illustrated here.

FIGURE 4 is a block diagram that illustrates an exemplary embodiment of a peripheral device according to various aspects of the present disclosure. As illustrated, the peripheral device 706 includes a short-range wireless interface 402, a notification generation engine 404, a notification repeater engine 406, and an information transmission engine 408. One of ordinary skill in the art will recognize that these components are similar to the short-range wireless interface 202, notification generation engine 204, notification repeater engine 208, and information transmission engine 206 illustrated and described above with respect to the controllable device 702. As such, a detailed description of the similar components in the peripheral device 706 is not provided here for the sake of brevity. The peripheral device 706 and the controllable device 702 have some overlapping capabilities (as discussed in more detail below), and so include similar components. However, the peripheral device 706 is generally used as a source of notifications based on events detected by or generated by components of the peripheral device 706, and is not generally controllable based on received notifications. Accordingly, the peripheral device 706 is missing the notification processing engine 210 that is present in the controllable device 702. This allows for the simplification of the hardware used in a peripheral device 706, thus reducing cost and improving battery life.

One of ordinary skill in the art will recognize that, though components common to all peripheral devices are illustrated in FIGURE 4, in some embodiments, particular peripheral devices may include additional components. As one example, FIGURE 5 is a block diagram that illustrates a light bar peripheral device 756 according to various aspects of the present disclosure. The light bar peripheral device 756 is suitable for associating with a light bar 110 of a vehicle 94, and will help make information about the status of the light bar 110 available within the system 100. The light bar peripheral device 756 is a type of peripheral device 706, and so it includes a short-range wireless interface 402, a notification generation engine 404, a notification repeater engine 406, and an information transmission engine 408 as described above.

The light bar peripheral device 756 also includes a light bar status sensor 502. The light bar status sensor 502 is configured to determine at least a state of the lights on the light bar 110 and/or the status of any other hardware associated with the light bar 110, including but not limited to a siren, a camera, and/or the like. The light bar status sensor 502 detects when a state of the light bar 110 changes (e.g., the lights are turned on or off), and is configured to transmit alerts regarding the state changes to the notification generation engine 404. In some embodiments, the notification generation engine 404 receives the alerts from the light bar status sensor 502 and generates notifications when appropriate. The content of the notification generated by the notification generation engine 404 may merely indicate that the status of the light bar 110 has changed, as opposed to also including an indication of the actual status. In response to receiving such a notification, another device may request information that includes the actual status of the light bar 110 from the light bar peripheral device 756. To respond to the request, the information transmission engine 408 may use the light bar status sensor 502 to determine the state of the light bar 110 (e.g., lights on, lights off, a particular pattern being displayed by the lights, and/or the like) for transmission as information associated with the notification.

As will be recognized by one of ordinary skill in the art, although a light bar peripheral device 756 is illustrated and described in FIGURE 5, many other types of peripheral devices 706 and controllable devices 702 not illustrated in the drawings may be used within the system 100. These devices will include the common features of the peripheral device 706 and/or the controllable device 702, as well as additional sensors appropriate for detecting relevant statuses of the components of the particular device.

For example, in some embodiments, a weapon peripheral device may be provided. A weapon provides force for self-defense, defense of others, and/or defense of property. For example, a weapon may include conventional circuits and/or mechanisms for cutting (e.g., hand knife, jaws of life), propelling a projectile (e.g., hand gun, shotgun), releasing
5 noxious material (e.g., pepper spray), and/or causing involuntary muscle contractions (e.g., conducted electrical weapons (CEWs) such as those marketed by TASER International Inc.). A weapon peripheral device may include sensors for determining a change in status of a safety device, detecting a discharge of the weapon, detecting a change in loading status of the weapon, and/or the like. As a similar example, a weapon
10 holster peripheral device may be provided. The weapon holster may be configured to carry a weapon when not in use, and the weapon holster peripheral device may include a sensor configured to detect when the weapon is placed into or removed from the holster.

As another example, in some embodiments, a personal assistant device may be configured as a peripheral device. A personal assistant device, such as the personal
15 assistant device 107 illustrated in FIGURE 1, may include any personal computer system that performs user-selected programs and supports communication with other officers (e.g., officers not co-located with the officer, officers operating dispatch or inventory functions, and/or the like) and/or communicates with other members of the system (e.g., forwards notices, batches notices to forward, derives a new notice from one or more other
20 notices). For example, a personal assistant may be packaged as or with the functions of a laptop computing device, a wrist-worn computing device, a tablet computing device, a body-worn computing device, a smartphone, and/or the like. Communication may include any conventional technologies (e.g., cellular phone service, text and data messaging, email, voice over IP, push-to-talk, video over cellular, video over IP, and/or
25 the like). Communication may use conventional public or private media (e.g., public cellular phone service, local area service, reserved channels, private trunk service, emergency services radio bands, and/or the like). In some embodiments, the personal assistant device may be configured as a controllable device, as opposed to a peripheral device.

30 As yet another example, a personal monitor peripheral device may be provided. A personal monitor peripheral device may include any apparatus for monitoring and/or recording physical and biological aspects of the user 92 (e.g., location, orientation, position, acceleration, ambient temperature, body temperature, voice, heart rate,

indications of stress, and/or the like). Sensors that generate inputs to a personal monitor peripheral device may be of any conventional technology (e.g., analog voltage or current, frequency, pulse position, optical transducers, hall effect, magnetic induction, acceleration, temperature, audio, and/or the like). In some embodiments, a personal monitor peripheral device permits assessment of a user's present level of physiological stress, psychological stress, and/or capacity to perform his or her duties within the policies and procedures prescribed by his or her superiors. A personal monitor peripheral device may be packaged to be worn on the wrist, chest, waist, and/or head. A personal monitor peripheral device with separable components may communicate among its components using conventional short range communication technology (e.g., Bluetooth, Zigbee, and/or the like).

As still another example, a vehicle monitor peripheral device may be provided. A vehicle monitor peripheral device includes any apparatus for monitoring and/or recording physical aspects of a vehicle (e.g., location, orientation, position, acceleration, ambient temperature, speed, direction, engine performance, supplies of consumables, operating temperature, emissions, operation of integral and accessory equipment, and/or the like). Sensors that generate inputs to a vehicle monitor peripheral device may be of any conventional technology (e.g., analog voltage or current, frequency, pulse position, optical transducers, hall effect, magnetic induction, acceleration, temperature, audio, and/or the like). Any conventional integrated or after-market installation for sensing, monitoring and recording technologies may be used. Some operating mode sensors may include a light bar operating mode sensor be packaged with a light bar; a siren operating mode sensor packaged with a siren; a combined siren and light bar operating mode sensor (if the siren and light bar themselves are combined; vehicle lighting operating mode sensor(s) (e.g., head lights, tail lights, directional and emergency flashers, passenger compartment lighting) packaged with suitable lighting assemblies and/or subassemblies; engine operating mode sensors integrated with engine controls such as ECMs; and/or the like.

In some embodiments, vehicle environment monitors may be provided as peripheral devices or controllable devices. A vehicle environment monitor may include enhanced monitoring and/or recording sensors that expands an unaided user's awareness (e.g., night vision cameras, ultrasound detecting microphones, gunshot detection/location sensor, and/or the like). Other types of sensors that may be provided by a vehicle

environment monitor include, but are not limited to: scanners for hidden weapons; sensors for illegal substances such as drugs; breathalyzer devices; still cameras for capturing portraits, scenes, documents, licenses, contraband, or counterfeit goods; video cameras adapted for investigations of particular areas (e.g., under-car or confined space cameras); explosives sensors; and/or the like. Some vehicle environment monitors may also provide analyzed data that goes beyond mere recording. Analysis may include recognition, correlation, and/or prediction based on information monitored or recorded from any source, such as other sensors within the system 100. Analysis of video or still photographs may be used for recognition of car make and model and identification of the owner of the vehicle and owner of the vehicle license. Analysis of audio and video may be used for recognition and identification of voices, faces, body dimensions, birth marks, tattoos, clothing, currency, drivers' licenses, and/or documents. Predictions may include conventional algorithms for the prediction of crime, for example, predictions based on locations of persons, locations of vehicles, recent dispatches, and recent sniffed, snooped, or analyzed network packets.

In some embodiments, some peripheral devices may be configured to generate notifications as desired by a user, as opposed to automatically in response to data generated by a sensor. As an example, FIGURE 6 is a block diagram that illustrates an exemplary embodiment of a command peripheral device 602 according to various aspects of the present disclosure. Again, the command peripheral device 602 is a type of peripheral device 706, and so it includes a short-range wireless interface 402, a notification generation engine 404, a notification repeater engine 406, and an information transmission engine 408 as described above. In contrast to the above, the command peripheral device 602 includes a user interface engine 604. The user interface engine 604 is configured to generate a user interface for accepting commands from a user intended for a controllable device. In this way, notifications may be generated within the system 100 that are not in response to a sensed status change, but are instead intentionally created by a user. When a command is received by the user interface engine 604, the notification generation engine 404 generates a notification and optionally generates information for propagation through the system 100 in a manner similar to other notifications and information.

In some embodiments, the command peripheral device 602 may be an interactive device carried by the user 92 or the vehicle 94, such as a smart phone, a tablet computing

device, a laptop computing device, and/or the like. In some embodiments, the command peripheral device 602 may be a desktop computing device or a server computing device located remotely from the user 92 and operated by a dispatcher or other such user. In such embodiments, the command peripheral device 602 may include a long-range
5 network interface, such as a wired network interface, a WiFi network interface, an LTE network interface, and/or the like. The notification in such embodiments would be sent in a targeted manner to another device with a long-range network interface, such as the personal assistant device 107, which may then propagate the notification and/or information throughout the rest of the system 100 as any other notification and/or
10 information is propagated.

FIGURES 7A-7C are high-level schematic diagrams of exemplary embodiments of communication between devices according to various aspects of the present disclosure. In FIGURE 7A, a setting is changed on a first controllable device 702 in response to a notification generated on a first peripheral device 704. The first peripheral device 704
15 detects an event that causes a notification to be generated. At a first point in a communication sequence, the first peripheral device 704 generates a notification and transmits the notification to one or more devices within a short-range wireless communication range 714 of the first peripheral device 704. As illustrated, a second peripheral device 706 is within the communication range 714, but the first controllable
20 device 702 is not. As discussed in further detail below, the notification may include all of the information needed to describe the event, or the second peripheral device 706 may, upon receiving the notification, request further information from the first peripheral device 704.

At a second point in the communication sequence, the second peripheral
25 device 706 retransmits the notification originally generated by the first peripheral device 704 to other devices within a communication range 712 of the second peripheral device 706. For example, the first controllable device 702 is within the communication range 712 of the second peripheral device 706. Accordingly, the first controllable device receives the notification from the second peripheral device 706. As discussed in further
30 detail below, in some embodiments the notification transmitted by the second peripheral device 706 may be the same notification as that originally transmitted by the first peripheral device 704 and so appears to the first controllable device 702 as having been transmitted by the first peripheral device 704. In some embodiments, the second

peripheral device 706 may generate a new notification based on the notification received from the first peripheral device 704, and transmit that new notification to the first controllable device 702. As above, all of the information needed by the first controllable device 702 to change its setting may be included in the notification, or the first
5 controllable device 702 may request further information from the second peripheral device 706 upon receiving the notification. In the second case, the second peripheral device 706 may respond to the request for further information with the information it retrieved from the first peripheral device 704. The first controllable device 702 may then change one or more of its settings based on the notification and/or the information.

10 At a third point in the communication sequence, the first controllable device 702 may itself retransmit the notification in order to ensure the broadest possible propagation of the notification despite only using short-range wireless technology. Accordingly, the notification retransmitted by the first controllable device 702 may be received by other devices within a communication range 716 of first controllable device 702, such as a third
15 peripheral device 708 and a second controllable device 710. As described above, the retransmitted notification could match the original notification, or could be a new notification based on the original notification. In some embodiments, any retransmitted notification is be ignored by the original peripheral device or controllable device, even if the original device is within communication range and receives the retransmitted
20 notification. This may help to avoid exponential growth of transmitted notifications, and may save battery life on the original device by not having to fully process as many incoming notifications.

As stated above, any suitable short-range wireless communication technology may be used for the communication. In some embodiments, if Bluetooth or Bluetooth
25 Low Energy is used, the devices may form piconets and scatternets. For example, the communication range 714 may represent a piconet comprising the first peripheral device 704 and the second peripheral device 706, communication range 712 may represent a piconet comprising the second peripheral device 706 and the first controllable device 702, and communication range 716 may represent a piconet comprising the first
30 controllable device 702, the third peripheral device 708, and the second controllable device 710. As such, communication ranges 712, 714, and 716 may be joined by their common devices to form a scatternet.

In FIGURE 7A, generic peripheral devices and controllable devices are discussed in order to illustrate the general types of communication that occur in some typical embodiments. FIGURE 7B illustrates a similar communication topology, but describes the participating devices with more particularity in order to demonstrate a practical example of communication according to various aspects of the present disclosure. In
5 FIGURE 7B, an event is detected by a vehicle monitor peripheral device 754. For example, the vehicle monitor peripheral device 754 may be installed in a vehicle 94, and may include a sensor that monitors the state of the trunk of the vehicle 94. Upon detecting that the trunk has been opened from a closed state, the vehicle monitor
10 peripheral device 754 generates a notification.

At the first point in the communication sequence, the vehicle monitor peripheral device 754 transmits the notification to devices within its communication range 764, including light bar peripheral device 756 (but not first wearable camera device 752). Once the light bar peripheral device 756 receives the notification, it may request further
15 information from the vehicle peripheral device 754 based on the content of the notification. In some embodiments, the notification may simply be an alert similar to a "door ajar" warning, and so a type included in the notification indicating the "door ajar" alert may be adequate for controllable devices to make decisions regarding what settings to change. However, in some embodiments, more information may be made available by
20 the vehicle monitor peripheral device 754 to indicate, for example, which component of the vehicle 94 is ajar and generating the alert. If the light bar peripheral device 756 determines from the notification that further information is available, then it retrieves the information from the vehicle monitor peripheral device 754.

The first wearable camera device 752 may not be within the communication
25 range 764 of the vehicle monitor peripheral device 754 for a variety of reasons. For example, the user 92 may have travelled away from the vehicle 94, and therefore may not be close enough to the vehicle monitor peripheral device 754. As another example, a line of sight between the vehicle monitor peripheral device 754 and the first wearable camera device 752 may be blocked by the seats of the vehicle 94, the engine of the vehicle 94, or
30 by some other item that blocks low-powered short-range wireless communication between the devices despite their relatively close proximity.

At a second point in the communication sequence after the light bar peripheral device 756 has received the notification, it retransmits the notification to other devices

within its communication range 762, such as the first wearable camera device 752. As before, the first wearable camera device 752 may request further information from the light bar peripheral device 756 if it is available. Thereafter, the first wearable camera device 752 may check or change a recording state of its camera in response to the received notification. For example, opening the trunk may indicate that the user 92 is retrieving a weapon, a testing kit, or other items used when responding to an incident that should be recorded. As such, the first wearable camera device 752 may begin recording if recording was not already happening. As another example, closing the trunk may indicate that the items have been replaced by the user 92 and the incident is over, and so the recording could be stopped.

At a third point in the communication sequence, the first wearable camera device 752 itself retransmits the notification to other devices within its communication range 765. These devices may include a weapon holster peripheral device 758 and/or a personal assistant device 760. The notification is not itself relevant to the weapon holster peripheral device 758, but it provides the weapon holster peripheral device 758 the opportunity to retransmit the notification. Likewise, the personal assistant device 760 may not change a setting based on the notification, but it may record the notification, retransmit the notification via a wide-area network in order to notify a dispatch system of the event, ignore the notification completely, or take any other appropriate action.

FIGURE 7C illustrates another similar communication topology, in order to describe communication between other particular participating devices as another practical example of communication according to various aspects of the present disclosure. In FIGURE 7C, a command peripheral device 766 receives an input via a user interface that causes a notification and optionally information to be generated representing a command. For example, a dispatcher may be sending a user 92 to the scene of an incident, and using the user interface engine of the command peripheral device 766, the dispatcher causes the notification and optionally information to be generated that will cause the camera 752 of the user 92 to be activated.

At the first point in the communication sequence, the command peripheral device 766 transmits the notification and optionally the information to the personal assistant device 760 of the user 92. The communication range 764 of the command peripheral device 766 may indicate a wireless communication range in which the personal assistant device 760 is reachable, or it may indicate a network connection between the

command peripheral device 766 and the personal assistant device 760 that traverses two or more networking technologies. For example, the command peripheral device 766 may transmit the notification to the personal assistant device 760 over a wide area network such as the Internet. The command peripheral device 766 may be connected to the Internet via a wired network, and the personal assistant device 760 may be connected to the Internet via WiFi, 3G, 4G, LTE, or any other suitable long-range wireless networking technology.

From this point, the notification propagates similar to the notifications in the previously described examples. At the second point in the communication sequence, the personal assistant device 760 acts as a peripheral device or a controllable device, and transmits the notification to devices within a communication range 762 of the personal assistant device 760, such as the first wearable camera device 752. If the first wearable camera device 752 determines that there is further information associated with the notification, it retrieves the information from the personal assistant device 760. The first wearable camera device 752 then changes a setting based on the notification and/or the information. If the notification is as described above and associated with a command to start recording, the first wearable camera device 752 will start recording based on the notification and/or the information.

At a third point in the communication sequence, the first wearable camera device 752 may retransmit the notification to other devices within a communication range 765 of the first wearable camera device, such as a weapon holster peripheral device 758 and/or a second personal assistant device 756 associated with another user. In some embodiments wherein the original notification was addressed specifically to the first wearable camera device 752, the first wearable camera device 752 may not retransmit the notification because it is only relevant to the first wearable camera device 752. Even in such embodiments, other peripheral devices 706 or controllable devices 702 may be able to take action in response to the start of recording if the first wearable camera device 752 generates and transmits a new notification related to its own change in recording state.

FIGURES 8A-8C are a flowchart that illustrates an exemplary embodiment of a method of transmitting and processing event notifications according to various aspects of the present disclosure. From a start block, the method 800 proceeds to block 802, where a first peripheral device 706 detects an event. As discussed above, a wide variety of

events may be detected by peripheral devices, depending on the type of peripheral device. For example, a safety sensor of a weapon peripheral device may detect changes in state of a weapon safety. As another example, a light bar sensor of a vehicle monitor peripheral device may detect a change in state of the light bar as an event. As yet another example,
5 a command peripheral device may detect an event based upon an entry received by its user interface engine. As will be understood by one of ordinary skill in the art, other types of events may also be detected by the peripheral devices described above or by other types of peripheral devices.

At block 804, a notification generation engine 404 of the first peripheral
10 device 706 generates a first notification in response to the event. In some embodiments, the first notification includes a header having a standard layout that includes at least some information relating to the event and/or the first peripheral device 706, such as one or more of a session identifier (described further below); information identifying a type, manufacturer, model, and/or serial number of the first peripheral device 706; information
15 identifying a type of the event; and/or an indication regarding whether more information will be made available. In some embodiments, the first notification may also include a payload with more data based on the type of the event.

At optional block 806, the notification generation engine 404 generates a first
information in response to the event. The first information is kept separate from the first
20 notification, and is stored by the first peripheral device 706 until it is requested by a device that receives the first notification. The actions of optional block 806 may be performed in embodiments wherein more information is needed to describe the event than will fit in a single notification packet; in embodiments wherein the information is desired to be communicated via a secure channel instead of via a public broadcast; in
25 embodiments wherein the size of the first notification is intended to be minimized; or in any other suitable embodiment. The actions of block 806 are optional because in some embodiments, none of these goals is desired, and all of the data needed to adequately describe the event fits in the first notification. For example, if the first peripheral device 706 is a heartrate monitor device, a value indicating a current heartrate or heartrate
30 range would not be sensitive information and would likely fit within the notification packet, and so the actions of optional block 806 may not be necessary.

Next, at procedure block 808, a notification transmission engine 404 of the first peripheral device 706 transmits the notification. In some embodiments, the transmission

may be a broadcast receivable by any devices within communication range of the first peripheral device 706. In some embodiments, the transmission may be directed to one or more particular devices by virtue of a previously configured setting such as a pairing between the particular devices and the first peripheral device 706. Any suitable
5 procedure for transmitting the notification may be used, including the procedure 900 illustrated in FIGURE 9 and described in further detail below.

At block 810, the notification is received by at least one of a controllable device 702 or a second peripheral device 706. The method 800 then proceeds to a decision block 812, after which the remainder of the method 800 changes based on
10 whether the notification was received by a controllable device 702 or a second peripheral device 706. The remainder of method 800 assumes that the notification was received by exactly one controllable device 702 or second peripheral device 706 for ease of discussion only. One of ordinary skill in the art will recognize that, in some embodiments, the same transmitted notification could be received by both a controllable
15 device 702 and a second peripheral device 706, could be received by multiple controllable devices 702, or could be received by multiple other peripheral devices 706, and that portions of the remainder of the method 800 may therefore be conducted concurrently by multiple receiving devices.

If the notification was received by a second peripheral device 706, then the result
20 of the decision block 812 is NO, and the method 800 proceeds to optional block 814. At optional block 814, a notification repeater engine 406 of the second peripheral device 706 retrieves the first information from the first peripheral device 406. The actions of block 814 are optional because, in some embodiments, there may not be first information to retrieve from the first peripheral device 406. In some embodiments, the notification
25 repeater engine 406 will request information from the first peripheral device 406 regardless of whether information is present to be retrieved. In some embodiments, the notification repeater engine 406 may determine whether or not to request information from the first peripheral device 406 based on the first notification. For example, the notification repeater engine 406 may check for an explicit indication regarding the
30 presence or absence of information to be retrieved in the first notification, may check a type of the first notification, may check a type of device that transmitted the first notification, and/or may use any other suitable technique.

At procedure block 816, the notification repeater engine 406 of the second peripheral device 706 retransmits the notification. Again, any suitable transmission technique may be used, including the procedure 900 described in further detail below. In some embodiments, the notification repeater engine 406 may create a new notification,
5 and the original notification and information may be retrievable from the second peripheral device 406 as further information associated with the new notification. In some embodiments, the notification repeater engine 406 may retransmit the notification that matches the first notification, either exactly or with enough alterations such that a receiving device will contact the second peripheral device instead of the first peripheral
10 device for the further information. The method 800 then proceeds to an end block and terminates.

Returning to decision block 812, if the first notification was received by a controllable device 702, then the result at decision block 812 is YES, and the method 800 proceeds to a continuation terminal ("terminal A"). From terminal A (FIGURE 8B), the
15 method 800 proceeds to block 818, where a notification processing engine 210 of the controllable device 702 determines whether a related notification has already been processed. In some embodiments, the controllable device 702 is likely to receive duplicate notifications, because the notifications may be transmitted repeatedly for the same event to help overcome intermittent losses in connectivity (as discussed further
20 below). To detect duplicate notifications, the controllable device 702 may save session identifiers that have previously been processed and ignore notifications after the first for a given session identifier; the controllable device 702 may ignore all notifications from a given device for a predetermined amount of time after processing a first notification; the controllable device 702 may create a fingerprint of each processed notification to
25 compare to newly received notifications; or may use any other suitable technique.

At decision block 820, the method 800 branches based on the determination regarding whether a related notification had already been processed. If a related notification had been processed, then the received notification is a duplicate and the result of the determination at decision block 820 is YES. Thereafter, the method 800 proceeds
30 to an end block and terminates. Otherwise, if no related notification had been processed, then the received notification is not a duplicate and the result of the determination at decision block 820 is NO. The method 800 then proceeds to block 822, where the notification processing engine 210 authenticates the first peripheral device 706.

Authentication of the first peripheral device 706 is desirable in order to avoid allowing unauthorized malicious notifications to cause unwanted changes in settings of the controllable device 702.

Any suitable technique for authentication may be used. In some embodiments, the controllable device 702 stores a whitelist of serial numbers or other identifiers of peripheral devices 706 for which notifications will be processed, and authentication comprises ensuring that the peripheral device 706 is on the whitelist. In some embodiments, the controllable device 702 may establish an encrypted connection with the peripheral device 706 using any suitable cryptographic communication technique, including but not limited to a Diffie-Hellman elliptical curve technique and/or the like. The controllable device 702 may assume that, if the peripheral device 706 implements the cryptographic communication technique and can establish the encrypted connection, then the peripheral device 706 is authenticated. In some embodiments, this encrypted connection or tunnel may be used to exchange further information between the peripheral device 706 and the controllable device 702. In some embodiments, a digital signature or other certificate stored on the peripheral device 706 is checked by the controllable device 702 for validity in order to authenticate the peripheral device.

Assuming the first peripheral device 706 was properly authenticated, the method 800 proceeds to block 824, where the notification processing engine 210 determines whether further information should be retrieved from the first peripheral device 706. Similar to the discussion above with respect to the actions of the notification repeater engine 406 of the second peripheral device, the notification processing engine 210 may use any suitable technique for determining whether further information should be retrieved from the first peripheral device 706. In some embodiments, the notification processing engine 210 will request information from the first peripheral device 406 regardless of whether information is present to be retrieved. In some embodiments, the notification processing engine 210 may determine whether or not to request information from the first peripheral device 706 based on the first notification. For example, the notification processing engine 210 may check for an explicit indication regarding the presence or absence of information to be retrieved in the first notification, may check a type of the first notification, may check a type of device that transmitted the first notification, and/or may use any other suitable technique. In some embodiments, the notification processing engine 210 may check a whitelist of devices from which

information will be requested. The whitelist may define one or more "sets" of devices to which the controllable device 702 belongs, such as a user or officer set, a vehicle set, a group set, a station set, and/or the like.

At decision block 826, the method 800 branches based on the determination
5 regarding whether further information should be retrieved from the first peripheral device 706. If it had been determined that further information should be retrieved from the first peripheral device 706, then the result of the determination at decision block 826 is YES, and the method 800 proceeds to block 828. At block 828, the notification processing engine 210 retrieves the information from the first peripheral device 706 using
10 any suitable technique. In some embodiments, the notification may be a Bluetooth Low Energy advertisement message, and the notification processing engine 210 may retrieve the information by transmitting a scan request packet to the first peripheral device 706. In some embodiments, a tunnel may be established between the first peripheral device 706 and the controllable device 702, and the further information may be retrieved
15 using a serial transmission protocol. The method 800 then proceeds to a continuation terminal ("terminal B"). Returning to decision block 826, if it had been determined that further information should not be retrieved from the first peripheral device 706, then the result of the determination at decision block 826 is NO, and the method 800 proceeds directly to terminal B.

20 From terminal B (FIGURE 8C), the method 800 proceeds to block 830, where the notification processing engine 210 changes at least one configuration setting of the controllable device 702 based on the notification and/or the information. As one example, if the controllable device 702 is a controllable camera device 752, then the notification processing engine 210 may cause the camera control engine 304 to change a
25 recording state of the video sensor 302 and/or audio sensor 306 to start, pause, or stop recording based on the notification and/or the information. As another example, if the controllable camera device 752 is equipped with or can otherwise access a long-range wireless interface, the notification processing engine 210 may cause transmission of a live video or audio stream from the controllable camera device 752 to the evidence
30 management system 102 or other remote device to be started or stopped.

Further, in some embodiments changing a configuration setting may include storing or transmitting data associated with the notification and/or the information. For example, if the controllable device 702 includes a long-range wireless interface, the

notification processing engine 210 may cause the controllable device 702 to transmit an SMS, an email, an API call, or any other data transmission based on the notification and/or the information to a remote device. As another example, the notification processing engine 210 may record and aggregate metadata based on the received
5 notifications and/or information, including but not limited to identities of users associated with the notifications (in order to be able to count a total number of users within the system's communication range); a type of the peripheral device that transmitted the notification and its status (in order to be able to count, for example, a total number of activated cameras or weapons drawn in an area); a distance of the peripheral device from
10 the controllable device 702 based on the signal strength; and or the like.

Also, though single notifications are described above, in some embodiments the notification processing engine 210 may use multiple notifications and/or multiple pieces of retrieved information to make the decision regarding the change in a setting. For example, if the notification and information indicate that the trunk of a vehicle 94
15 associated with the user 92 is open, the notification processing engine 210 may cause other information to be retrieved to determine whether the light bar or siren is active, or whether the vehicle 94 is moving, before causing a change in video or audio recording state. As another example, if several notifications and/or pieces of retrieved information indicate that a weapon has been removed from a holster and the trunk is open, then the
20 video recording state may not be changed (due to the likelihood that the user 92 is merely placing the weapon in the trunk as opposed to using the weapon to apply force. As still another example, if several notifications and or pieces of retrieved information indicate that the user 92 has returned to the driver's seat of the vehicle 94 and that the user's holster is empty, then the notification processing engine 210 may cause a warning
25 message to be transmitted or displayed.

At optional block 832, the notification processing engine 210 stores an indication of the notification and/or the information (depending on whether additional information was retrieved) in an audit trail data store 316 of the controllable device 702. The actions at block 832 are optional because not all embodiments of a controllable device 702 will
30 include an audit trail data store 316, but may instead apply the configuration setting change without storing a record of the change, the notification, or the information. In some embodiments, instead of storing the notification and/or the information in an audit trail data store 316, the notification processing engine 210 may add data from the

notification and/or the information to data recorded by the controllable device 702 or metadata associated with data recorded by the controllable device 702, including but not limited to metadata associated with video data or audio data.

5 The method 800 then proceeds to decision block 834, where a determination is made regarding whether the controllable device 702 should retransmit the notification and/or the information. In some embodiments, the controllable device 702 may retransmit all notifications, as does the peripheral device 706. In some embodiments, the controllable device 702 may filter some notifications and may not retransmit them. For example, in some embodiments, the notification processing engine 210 may detect that a
10 notification was addressed specifically to the controllable device 702, and may therefore not retransmit it because it will not be relevant to other devices. As another example, in some embodiments, the notification processing engine 210 may not retransmit notifications of certain types or from certain types of devices.

If the determination at decision block 834 is that the controllable device 702
15 should retransmit the notification, then the result of decision block 834 is YES, and the method 800 proceeds to procedure block 836, where a notification repeater engine 208 of the controllable device 702 retransmits the notification. Again, any suitable transmission technique may be used, including the procedure 900 described in further detail below. In some embodiments, the notification repeater engine 208 may create a new notification,
20 and the original notification and information may be retrievable from the controllable device 702 as further information associated with the new notification. In some embodiments, the notification repeater engine 208 may retransmit the notification that matches the first notification, either exactly or with enough alterations such that a receiving device will contact the first peripheral device instead of the controllable
25 device 702 for the further information. The method 800 then proceeds to optional block 838. Returning to decision block 834, if the determination is that the controllable device 702 should not retransmit the notification, then the result of decision block 834 is NO, and the method 800 proceeds directly to optional block 838.

At optional block 838, the controllable device 702 transmits notifications and/or
30 information from the audit trail data store 316 to an evidence management system 102. The information may be transmitted from the audit trail data store 316 to the evidence management system 102 using any suitable technique, including via an evidence collection dock 104 or via an ad-hoc wireless communication path. In some

embodiments, urgent notifications and/or information may be transmitted to the evidence management system 102 via the ad-hoc wireless communication path, including via a coordinator computing device, as soon as possible after the receipt of the notification and/or information whether or not it is stored in the audit trail data store 316. The actions
5 described at block 838 are optional because not all embodiments transmit information to an evidence management system 102, nor do all embodiments include an audit trail data store 316. The method 800 then proceeds to an end block and terminates.

FIGURE 9 is a flowchart that illustrates a procedure for transmitting a notification from a device according to various aspects of the present disclosure. As discussed above,
10 the procedure 900 is suitable for use by a peripheral device 706 or a controllable device 702, as discussed in blocks 808, 816, and 836 of the method 800 described above. Because similar steps would be performed by either device at any of these blocks 808, 816, and 836, separate descriptions of each block are not provided.

The technique described in the procedure 900 has many advantages. For example,
15 the procedure 900 can overcome issues with intermittent connectivity, which may be caused by an intermittent lack of line of sight between devices, devices intermittently moving out of communication range of each other, and/or the like. For example, if a low-power short-range wireless communication technique is used, the line of sight may be blocked by the user's body, the frame of a vehicle, and/or the like. As another example,
20 the devices may travel into and out of range of each other during an activity such as a foot pursuit, a traffic stop, and/or the like. As another example of an advantage, the short periods for which notifications are transmitted helps to strike a balance that reduces power consumption and thereby increases battery life. As yet another example of an advantage, the use of sessions (as described below) may help allow receiving devices to
25 ignore duplicate notifications, thereby further reducing processing and power drains.

From a start block, the procedure 900 advances to block 902, where the device creates a new session for the notification. In some embodiments, the new session is identified by a session identifier. In some embodiments, creating the new session may simply increment a session identifier value based on a previous session identifier value
30 for the device. In some embodiments, the device may randomly choose a session identifier or use an unpredictable but deterministic sequence of session identifier values, such as the output of a pseudo-random number generator for a given seed, so that a

receiving device can compare the session identifier value to an expected next session identifier value for authentication purposes.

At block 904, the device transmits the notification to other devices within communication range of the device. In some embodiments, the notification may be a
 5 broadcast transmission or otherwise unaddressed, such that any device within communication range may receive and process the notification. In some embodiments, the notification may be addressed or otherwise directed to one or more particular devices, such as devices that had previously been paired to the transmitting device, devices that are the particular target of the notification, and/or the like. In some embodiments, the
 10 notification may be transmitted using a radio frequency communication technique. In some embodiments, the radio frequency used may be in the 2.4 GHz band in order to avoid interference with police bands used for other equipment. In some embodiments, the notification may be transmitted using a short-range wireless networking technology, such as Bluetooth or Bluetooth Low Energy. In some embodiments, wired
 15 communication and/or long-range wireless communication may be used to implement at least part of the communication path used to transmit the notification. For example, the transmitting device may be a command peripheral device 602 operated by a dispatcher on a wired network, and the notification may be addressed to a peripheral device 706 or a controllable device 702 in the field, such as a smart phone device or a controllable camera
 20 device 752 having a long-range wireless interface such as LTE or WiFi.

In some embodiments, the notification may be included in a Bluetooth Low Energy advertisement message as defined by the respective protocol. Some portions of the message format may be defined by the systems designer (e.g., the predefined sequence of information in the payload, the quantity of bits predefined to convey various
 25 information in the payload, and/or the like). In some embodiments, the format described below in Table 1 may be used. Other embodiments, according to various aspects of the present disclosure, may use a different sequence of information in the payload. Still other embodiments, according to various aspects of the present disclosure, use different quantities of bits for information in the payload. Shorter payloads permit more messages
 30 to be sent and received per unit time.

TABLE 1

Bit Position	Name	Description and Alternatives
1 - 8	Preamble	Tunes receiver; defined by protocol
9 - 40	Access address	Distinguishes an intended message from noise; defined by protocol
41 - 48	Header	Packet type defined by protocol
49 - 56	Length	Number of bits in the Payload
57 - 353	Payload	See following rows
57 - 88	Sender manufacturer	A code number, a more meaningful coded text abbreviation
89 - 100	Sender model	A code number, a more meaningful coded text abbreviation
101 - 148	Sender serial number	A binary integer, a code comprising digits, a code comprising characters
149 - 164	Sender faults	A set of binary true/false values each conveying a predetermined fault condition in the transmitting device
165 - 180	Session identifier	A binary integer
181 - 200	Status	A set of bits providing data that carries status information regarding the device (or an event detected by the device)
201 - 353	reserved	May be omitted from the message
353 - 376	CRC	Cyclic redundancy check code for the message or for one or more suitable portions of the message (e.g., header, length, payload, portion of the payload)

After transmitting the notification, the procedure 900 waits for a predetermined amount of time. The amount of time for which the procedure 900 waits may be configurable by an administrator or designer of the system in order to balance battery life with a likelihood of successful communication (shorter wait times increase the likelihood of successful communication, but reduce battery life). In some embodiments, the amount of time may be a value in the range of 1-10 seconds, such as 5 seconds. In some embodiments, an extra random delay interval between 0 and 10 ms may be added to the amount of time to help avoid collisions between notifications.

After waiting, the procedure 900 then proceeds to a decision block 906, where a determination is made regarding whether a predetermined amount of time has elapsed since the creation of the new session. In some embodiments, the predetermined amount of time may be configurable by an administrator or designer of the system; in some
5 embodiments, the predetermined amount of time may be a value in the range of 20-60 seconds, such as 30 seconds. Again, longer sessions increase likelihood of successful communication, but reduce battery life on both the transmitter and receiver.

If the predetermined amount of time has not elapsed since the creation of the new session, then the result of the determination at decision block 906 is NO, and the
10 procedure 900 returns to block 904. Otherwise, if the predetermined amount of time has elapsed, then the result of the determination at decision block 906 is YES, and the procedure 900 advances to block 908, where the device ends the new session associated with the notification. Once the new session ends, no more transmissions will be made using the session identifier. In some embodiments, the end of a session also stops the
15 transmission of further notifications until the procedure 900 is executed a subsequent time. In some embodiments, events other than the elapsing of the predetermined amount of time may cause session to end. For example, in some embodiments, a new event that supersedes the previous event, such as another change in camera or light bar state, or crossing an additional heart rate threshold, may cause the session to end so that a new
20 session can be started. As another example, in some embodiments, a confirmed receipt by a targeted recipient device may cause the session to end.

The procedure 900 then proceeds to an end block and terminates.

FIGURE 10 is a block diagram that illustrates aspects of an exemplary computing device appropriate for use as a computing device of the present disclosure. While
25 multiple different types of computing devices were discussed above, the exemplary computing device 1000 describes various elements that are common to many different types of computing devices. While FIGURE 10 is described with reference to a computing device that is implemented as a device on a network, the description below is applicable to servers, personal computers, mobile phones, smart phones, tablet
30 computers, embedded computing devices, and other devices that may be used to implement portions of embodiments of the present disclosure. Moreover, those of ordinary skill in the art and others will recognize that the computing device 1000 may be any one of any number of currently available or yet to be developed devices.

In its most basic configuration, the computing device 1000 includes at least one processor 1002 and a system memory 1004 connected by a communication bus 1006. Depending on the exact configuration and type of device, the system memory 1004 may be volatile or nonvolatile memory, such as read only memory ("ROM"), random access
5 memory ("RAM"), EEPROM, flash memory, or similar memory technology. Those of ordinary skill in the art and others will recognize that system memory 1004 typically stores data and/or program modules that are immediately accessible to and/or currently being operated on by the processor 1002. In this regard, the processor 1002 may serve as
10 a computational center of the computing device 1000 by supporting the execution of instructions.

As further illustrated in FIGURE 10, the computing device 1000 may include a network interface 1010 comprising one or more components for communicating with other devices over a network. Embodiments of the present disclosure may access basic services that utilize the network interface 1010 to perform communications using
15 common network protocols. The network interface 1010 may also include a wireless network interface configured to communicate via one or more wireless communication protocols, such as WiFi, 2G, 3G, LTE, WiMAX, Bluetooth, and/or the like. As will be appreciated by one of ordinary skill in the art, the network interface 1010 illustrated in
FIGURE 10 may represent one or more wireless interfaces or physical communication
20 interfaces described and illustrated above with respect to particular components of the system 100.

In the exemplary embodiment depicted in FIGURE 10, the computing device 1000 also includes a storage medium 1008. However, services may be accessed using a computing device that does not include means for persisting data to a local
25 storage medium. Therefore, the storage medium 1008 depicted in FIGURE 10 is represented with a dashed line to indicate that the storage medium 1008 is optional. In any event, the storage medium 1008 may be volatile or nonvolatile, removable or nonremovable, implemented using any technology capable of storing information such as, but not limited to, a hard drive, solid state drive, CD ROM, DVD, or other disk storage,
30 magnetic cassettes, magnetic tape, magnetic disk storage, and/or the like.

As used herein, the term "computer-readable medium" includes volatile and non-volatile and removable and non-removable media implemented in any method or technology capable of storing information, such as computer readable instructions, data

structures, program modules, or other data. In this regard, the system memory 1004 and storage medium 1008 depicted in FIGURE 10 are merely examples of computer-readable media.

Suitable implementations of computing devices that include a processor 1002,
5 system memory 1004, communication bus 1006, storage medium 1008, and network interface 1010 are known and commercially available. For ease of illustration and because it is not important for an understanding of the claimed subject matter, FIGURE 10 does not show some of the typical components of many computing devices. In this regard, the computing device 1000 may include input devices, such as a keyboard,
10 keypad, mouse, microphone, touch input device, touch screen, tablet, and/or the like. Such input devices may be coupled to the computing device 1000 by wired or wireless connections including RF, infrared, serial, parallel, Bluetooth, USB, or other suitable connections protocols using wireless or physical connections. Similarly, the computing device 1000 may also include output devices such as a display, speakers, printer, etc.
15 Since these devices are well known in the art, they are not illustrated or described further herein.

While illustrative embodiments have been illustrated and described, it will be appreciated that various changes can be made therein without departing from the spirit and scope of the invention.

CLAIMS

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A system, comprising:
 - a first peripheral device, configured to:
 - broadcast a first notification indicating an availability of first information generated by the first peripheral device; and
 - transmit the first information in response to a request for the first information; and
 - a controllable device, configured to:
 - receive the first notification from the first peripheral device;
 - in response to the first notification, transmit a request for the first information to the first peripheral device; and
 - in response to the first information received from the first peripheral device, change at least one setting of the controllable device based on the first information.
2. The system of Claim 1, wherein the system further comprises a second peripheral device;
 - wherein the second peripheral device is not within communication range of the controllable device;
 - wherein the first peripheral device is within communication range of the controllable device and the second peripheral device; and
 - wherein the first peripheral device is configured to:
 - receive a second notification broadcast by the second peripheral device indicating an availability of second information generated by the second peripheral device;
 - in response to the second notification, transmit a request for the second information to the second peripheral device; and
 - broadcast a third notification indicating an availability of the second information.

3. The system of Claim 2, wherein the controllable device is further configured to:

receive the third notification from the first peripheral device;

in response to the third notification, transmit a request for the second information to the first peripheral device; and

in response to the second information received from the first peripheral device, change at least one setting of the controllable device based on the second information.

4. The system of any of Claims 1-3, wherein the first information is generated by a sensor of the first peripheral device, and wherein the sensor includes at least one of a heart rate sensor, a motion sensor, a holster removal sensor, a weapon status sensor, a light bar status sensor, a door sensor, a trunk sensor, and a camera status sensor.

5. The system of any of Claims 1-4, wherein changing at least one setting of the controllable device includes changing a recording state of a camera of the controllable device.

6. The system of any of Claims 1-5, wherein the controllable device is further configured to store the first information for subsequent transmission to an evidence management system.

7. The system of Claim 6, wherein the controllable device includes a camera, and wherein storing the first information for subsequent transmission to an evidence management system includes inserting the first information in metadata associated with video data generated by the camera.

8. The system of any of Claims 1-7, wherein the controllable device is further configured to broadcast a fourth notification indicating an availability of the first information generated by the first peripheral device.

9. The system of any of Claims 1-8, wherein the controllable device is further configured to authenticate the first peripheral device in response to receiving the first notification.

10. The system of Claim 9, wherein authenticating the first peripheral device includes determining whether the first peripheral device is on a whitelist.

11. The system of Claim 9, wherein authenticating the first peripheral device includes establishing an encrypted communication channel between the first peripheral device and the controllable device.

12. The system of any of Claims 1-11, further comprising a command peripheral device configured to:

broadcast a fifth notification based on a command generated by a user input received by the command peripheral device.

13. The system of any of Claims 1-12, wherein broadcasting the first notification indicating an availability of the first information generated by the first peripheral device includes repeatedly transmitting the first notification for a predetermined amount of time.

14. A controllable device, comprising:

a short-range wireless interface; and

a notification processing engine configured to:

receive a first notification from a first peripheral device via the short-range wireless interface; and

in response to a determination that the controllable device should process the first notification, change at least one setting of the controllable device based on the first notification.

15. The controllable device of Claim 14, wherein changing at least one setting of the controllable device based on the first notification includes:

transmitting a request for first information associated with the first notification to the first peripheral device via the short-range wireless interface;

receiving the first information from the first peripheral device via the short-range wireless interface; and

changing at least one setting of the controllable device based on the first information.

16. The controllable device of Claim 15, wherein the first information was generated by a second peripheral device and retransmitted by the first peripheral device.

17. The controllable device of Claim 15, wherein the first information is generated by a sensor of the first peripheral device, and wherein the sensor includes at least one of a heart rate sensor, a motion sensor, a holster removal sensor, a weapon status sensor, a light bar status sensor, a door sensor, a trunk sensor, and a camera status sensor.

18. The controllable device of any of Claims 14-17, further comprising a camera, and wherein changing at least one setting of the controllable device based on the first notification includes changing a recording state of the camera.

19. The controllable device of any of Claims 14-18, further comprising an audit trail data store, and wherein the notification processing engine is further configured to store an indication of the first notification in the audit trail data store.

20. The controllable device of any of Claims 14-19, further comprising a camera, and wherein the notification processing engine is further configured to store the first information in metadata associated with video data generated by the camera.

21. The controllable device of any of Claims 14-20, further comprising a notification repeater engine configured to transmit, via the short-range wireless interface, a second notification based on the first notification.

22. The controllable device of any of Claims 14-21, further comprising an authentication engine configured to authenticate the first peripheral device in response to receiving the first notification.

23. The controllable device of Claim 22, wherein authenticating the first peripheral device includes determining whether the first peripheral device is on a whitelist.

24. The controllable device of Claim 22, wherein authenticating the first peripheral device includes establishing an encrypted communication channel between the first peripheral device and the controllable device.

25. A method of processing received signals for control of a controllable device, the method comprising:

receiving, by the controllable device, a first notification from a first peripheral device; and

in response to determining that the controllable device should process the first notification, changing at least one setting of the controllable device based on the first notification.

26. The method of Claim 25, wherein changing at least one setting of the controllable device based on the first notification includes:

transmitting a request for first information associated with the first notification to the first peripheral device;

receiving the first information from the first peripheral device; and

changing at least one setting of the controllable device based on the first information.

27. The method of Claim 26, wherein the first information was generated by a second peripheral device and retransmitted by the first peripheral device.

28. The method of Claim 26, wherein the first information is generated by a sensor of the first peripheral device, and wherein the sensor includes at least one of a heart rate sensor, a motion sensor, a holster removal sensor, a weapon status sensor, a light bar status sensor, a door sensor, a trunk sensor, and a camera status sensor.

29. The method of any of Claims 25-28, wherein changing at least one setting of the controllable device based on the first notification includes changing a recording state of a camera.

30. The method of any of Claims 25-29, further comprising storing, by the controllable device, an indication of the first notification for subsequent transmission to an evidence management system.

31. The method of any of Claims 25-30, further comprising storing an indication based on the first notification in metadata associated with video data.

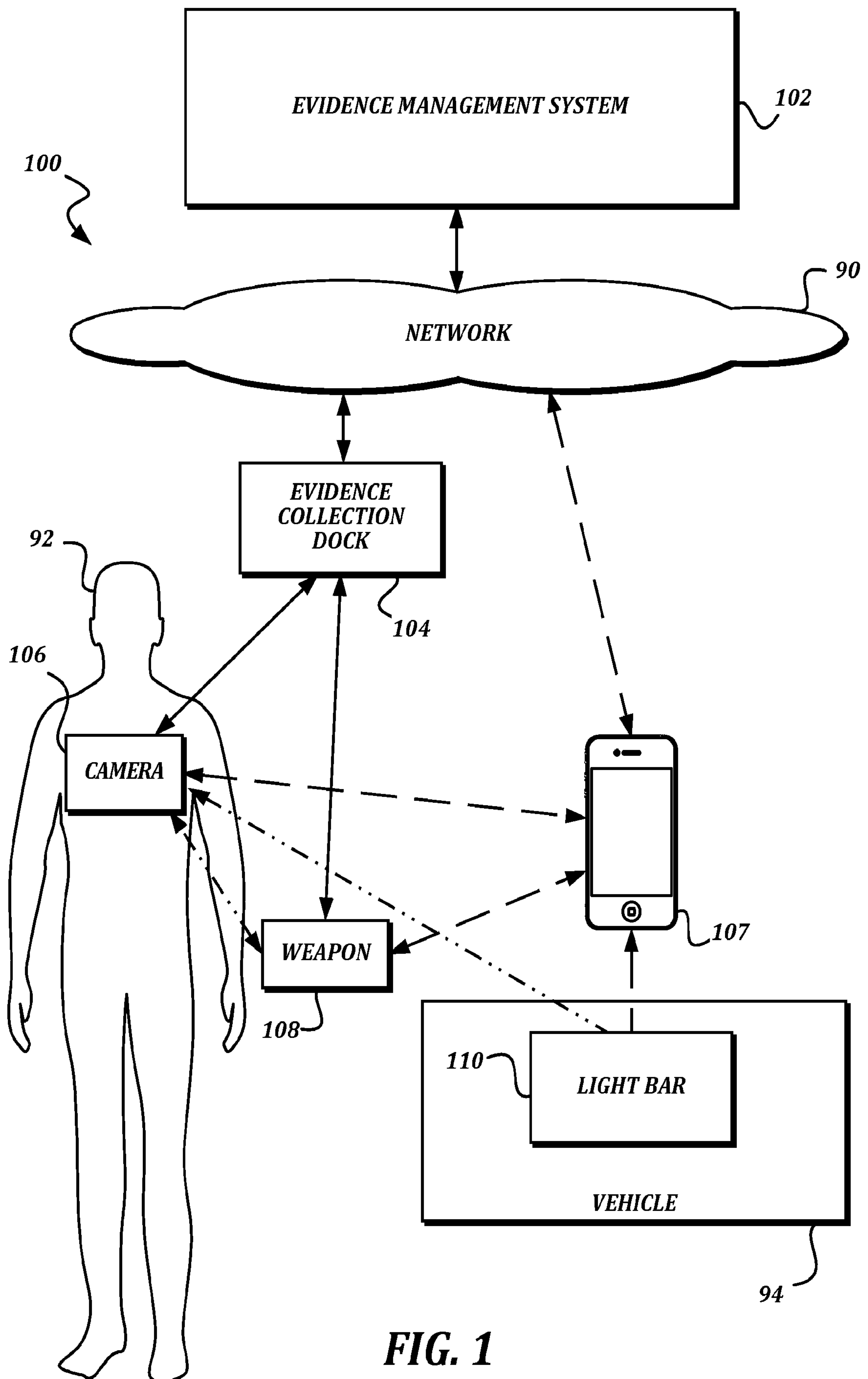
32. The method of any of Claims 25-31, further comprising transmitting, by the controllable device, a second notification based on the first notification.

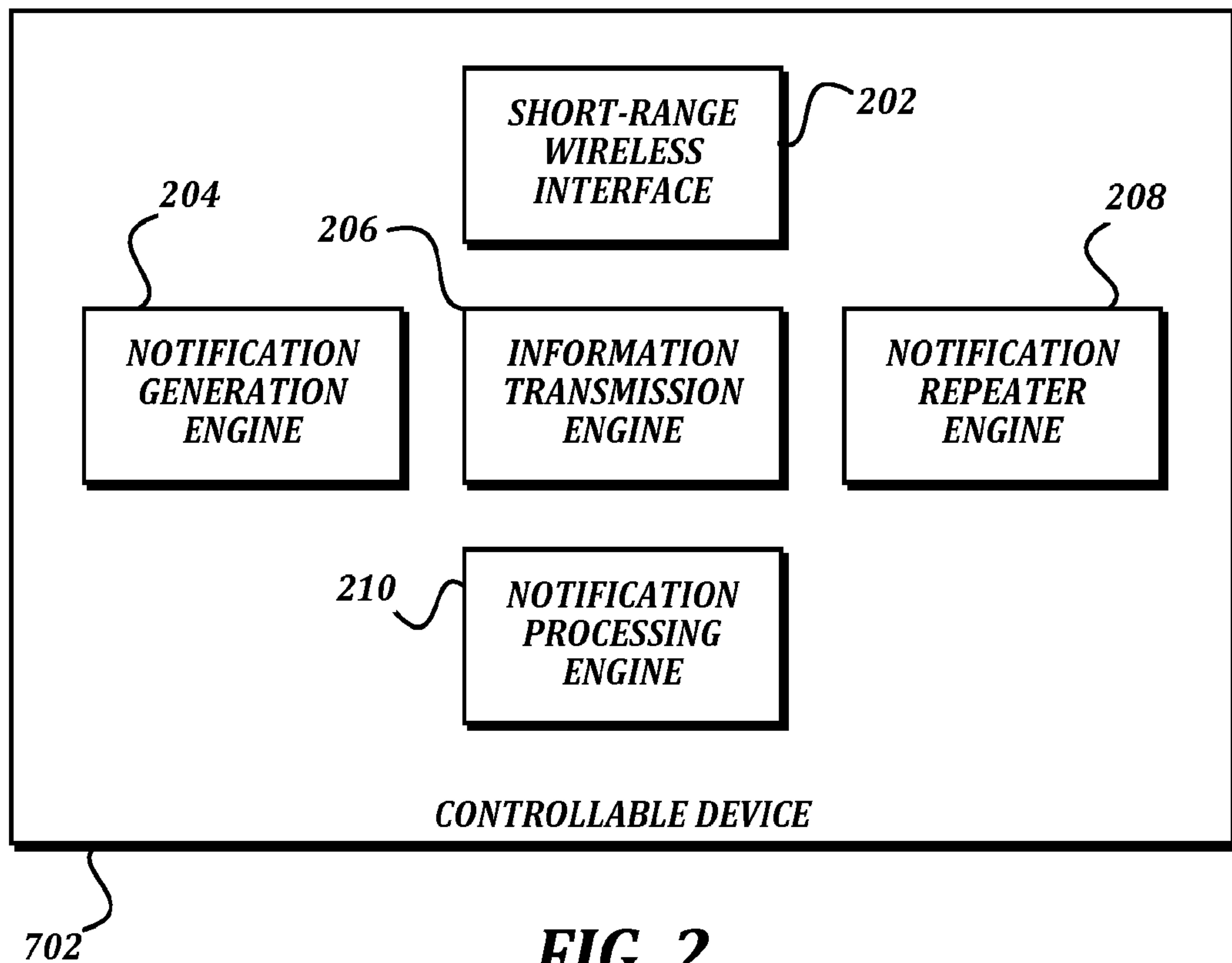
33. The method of any of Claims 25-32, further comprising authenticating the first peripheral device in response to receiving the first notification.

34. The method of Claim 33, wherein authenticating the first peripheral device includes determining whether the first peripheral device is on a whitelist.

35. The method of Claim 33, wherein authenticating the first peripheral device includes establishing an encrypted communication channel between the first peripheral device and the controllable device.

1/13

**FIG. 1**

2/13**FIG. 2**

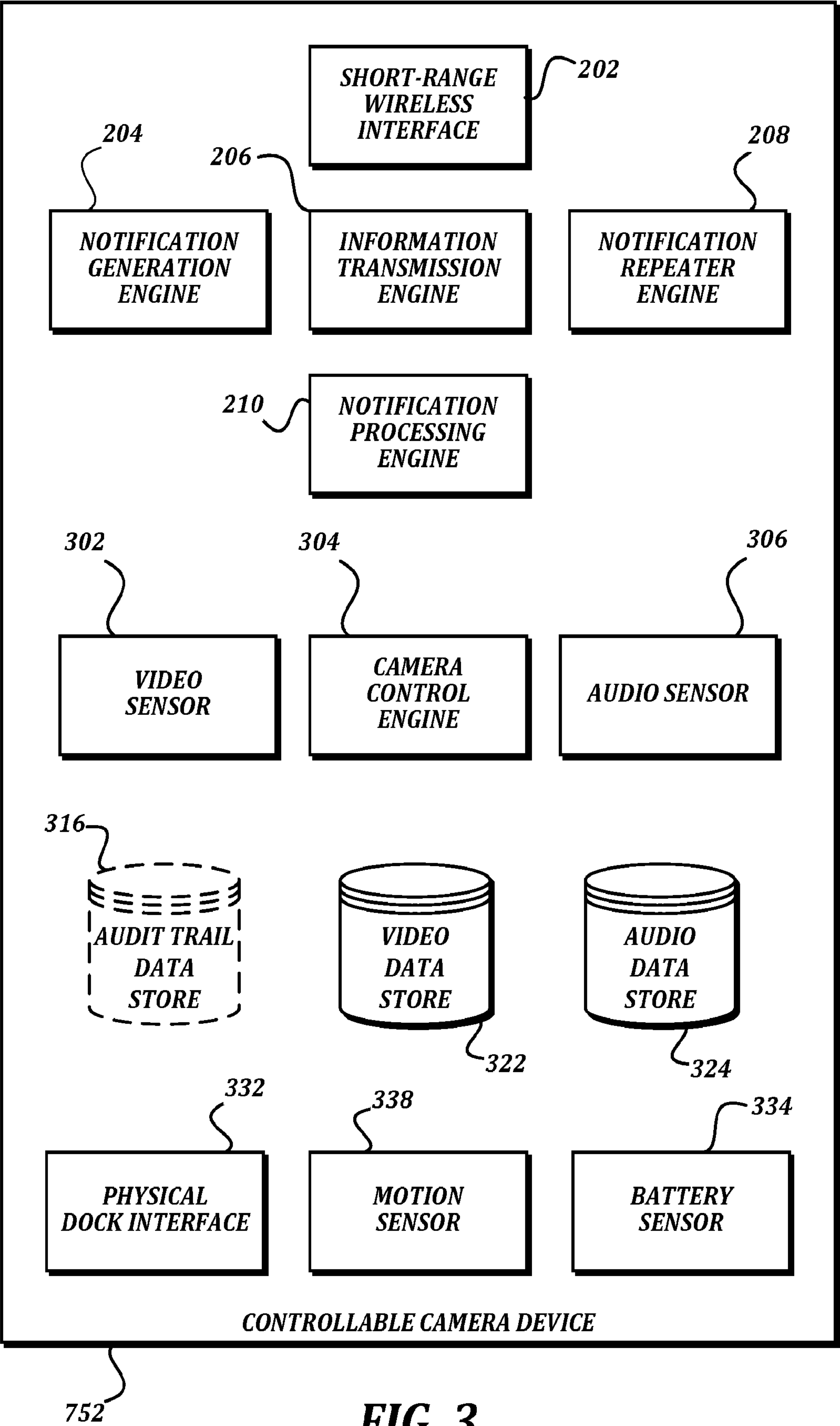
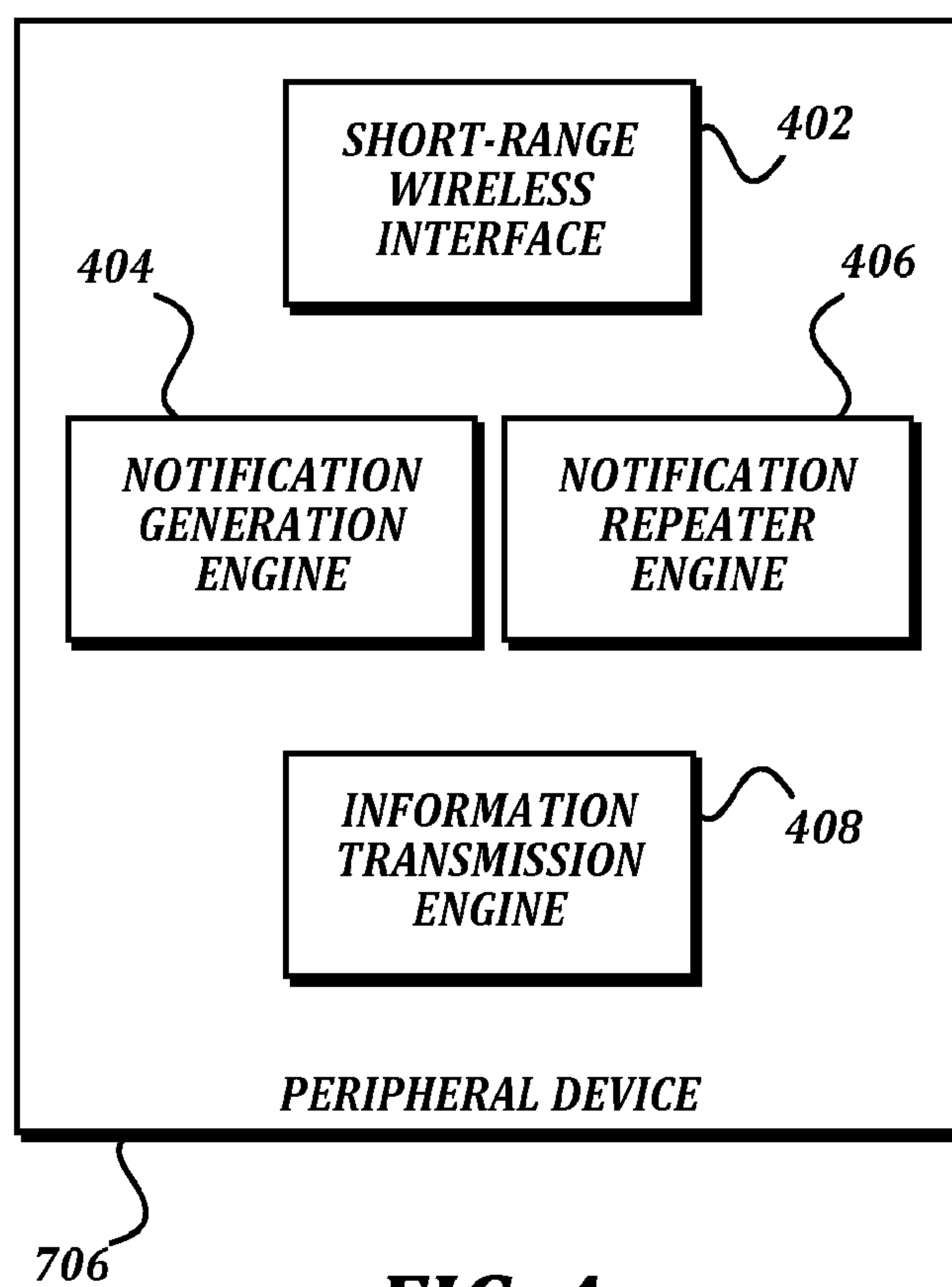
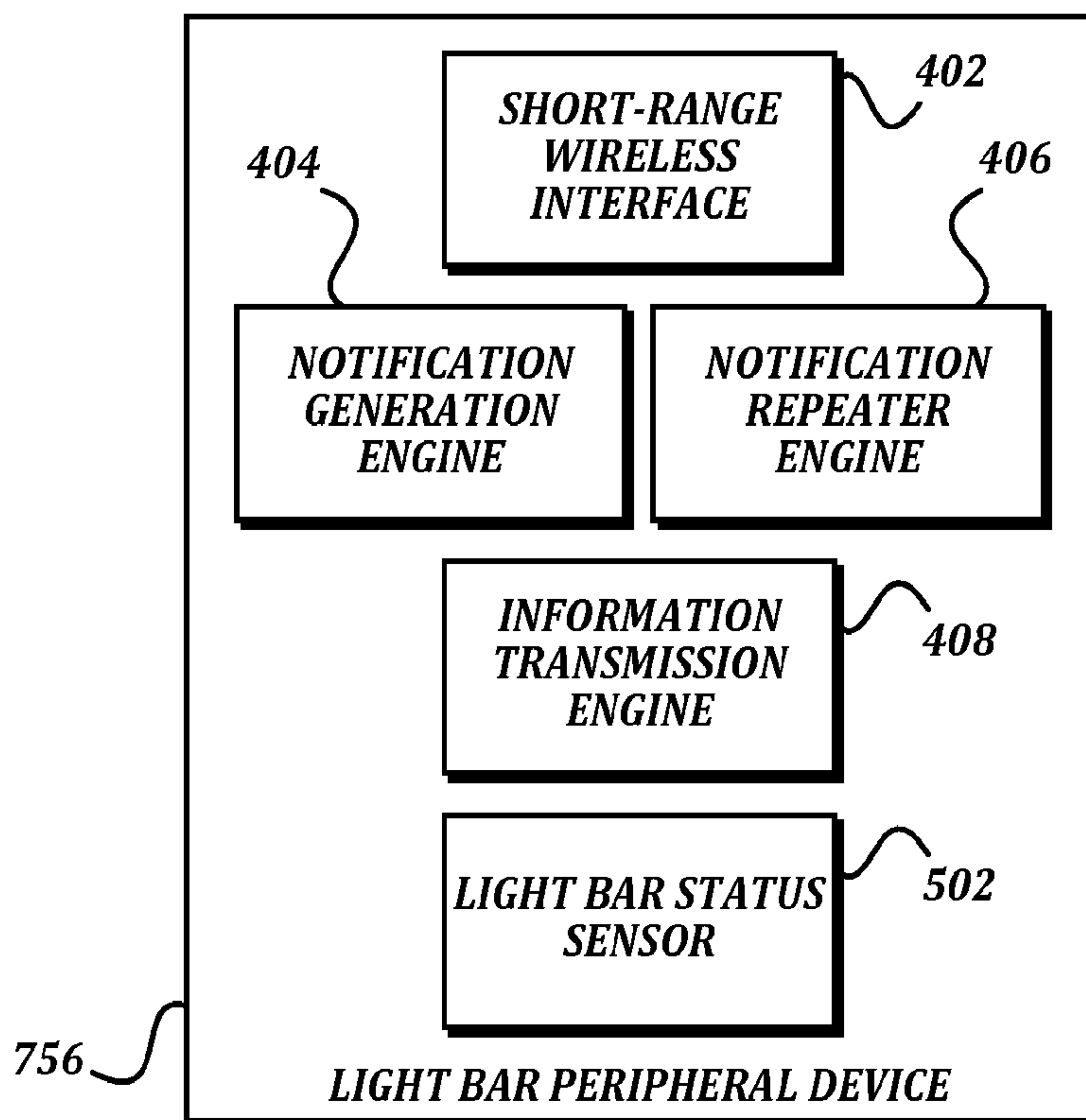
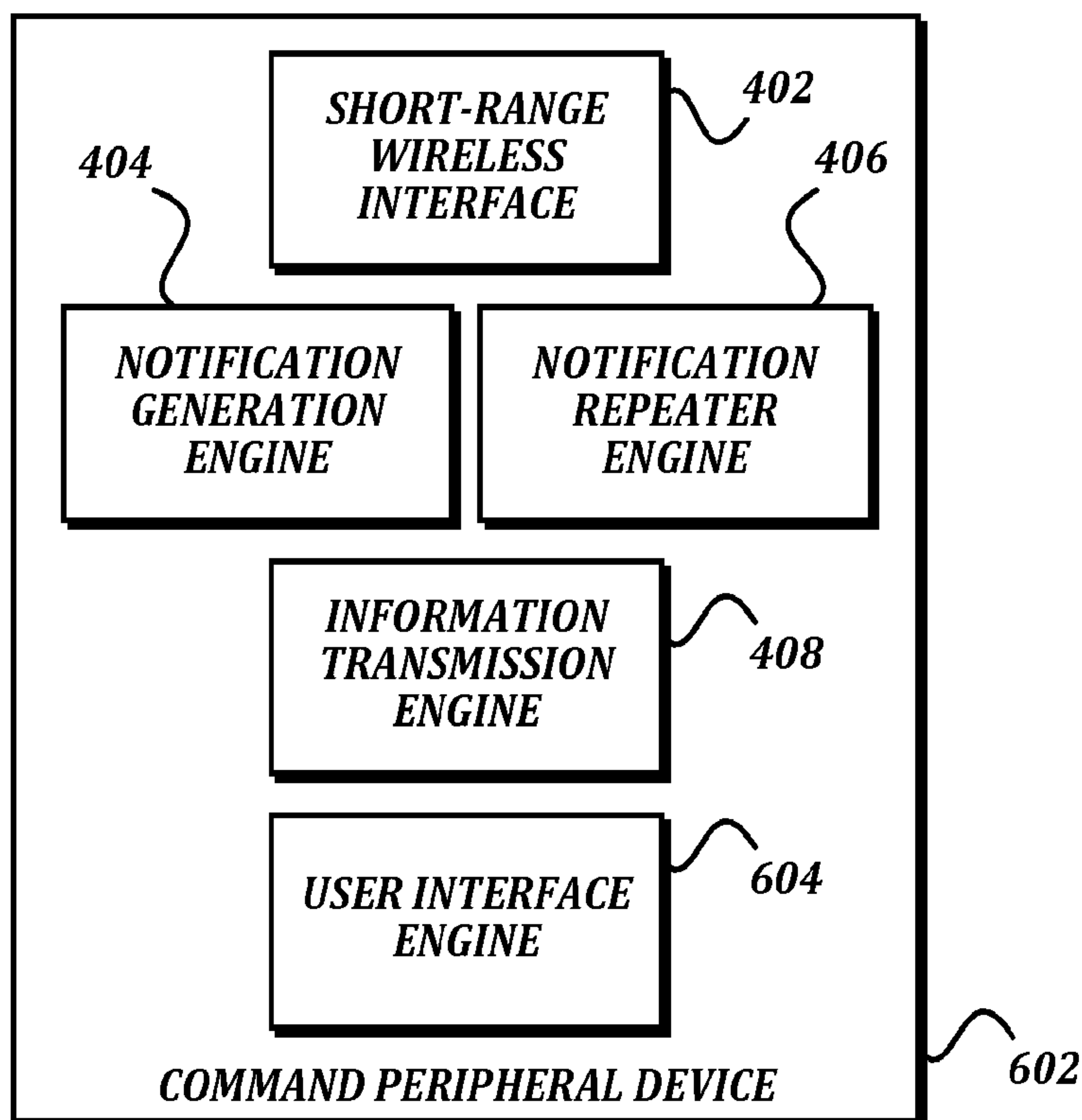


FIG. 3

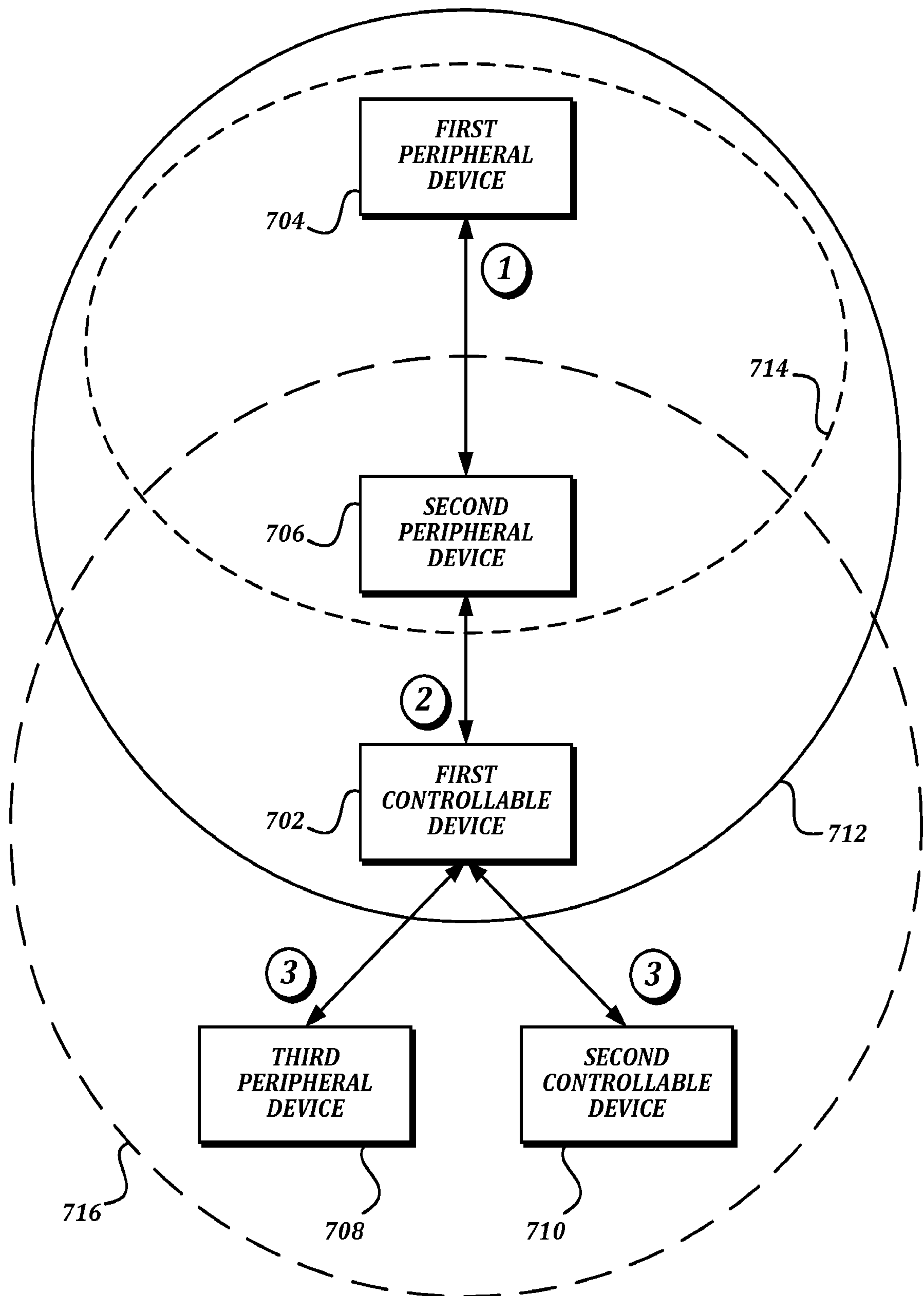
4/13

**FIG. 4**

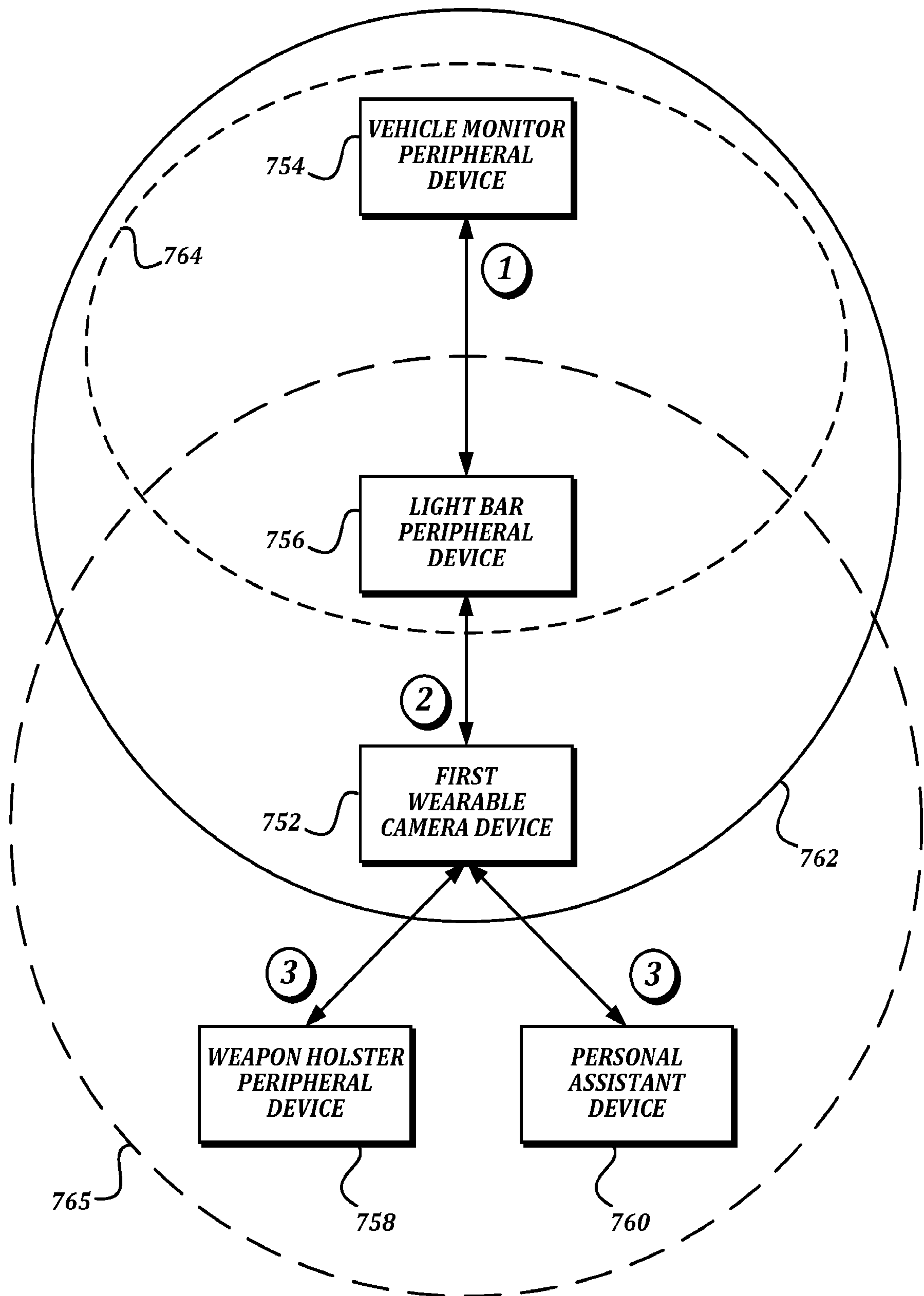
5/13

**FIG. 5****FIG. 6**

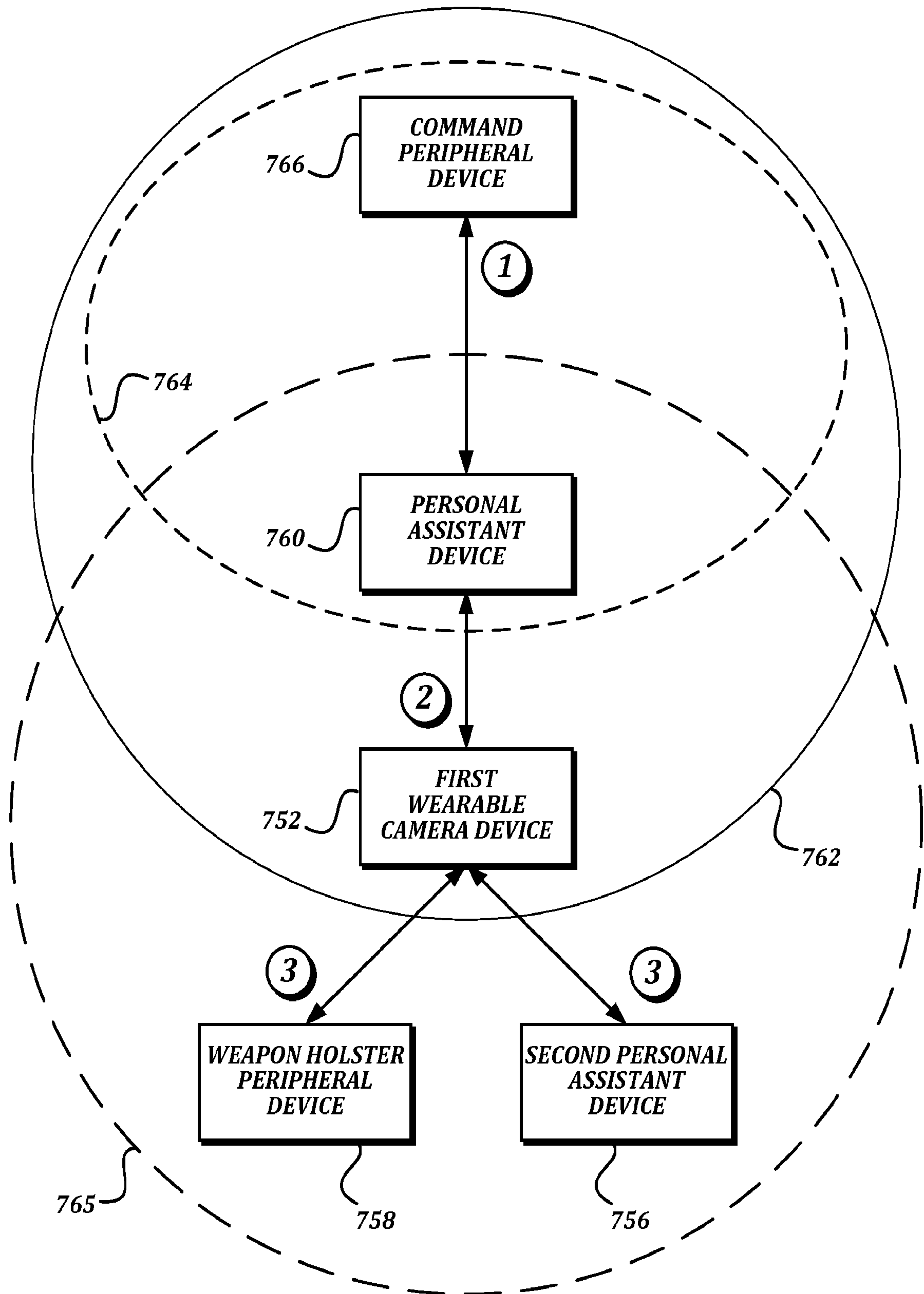
6/13

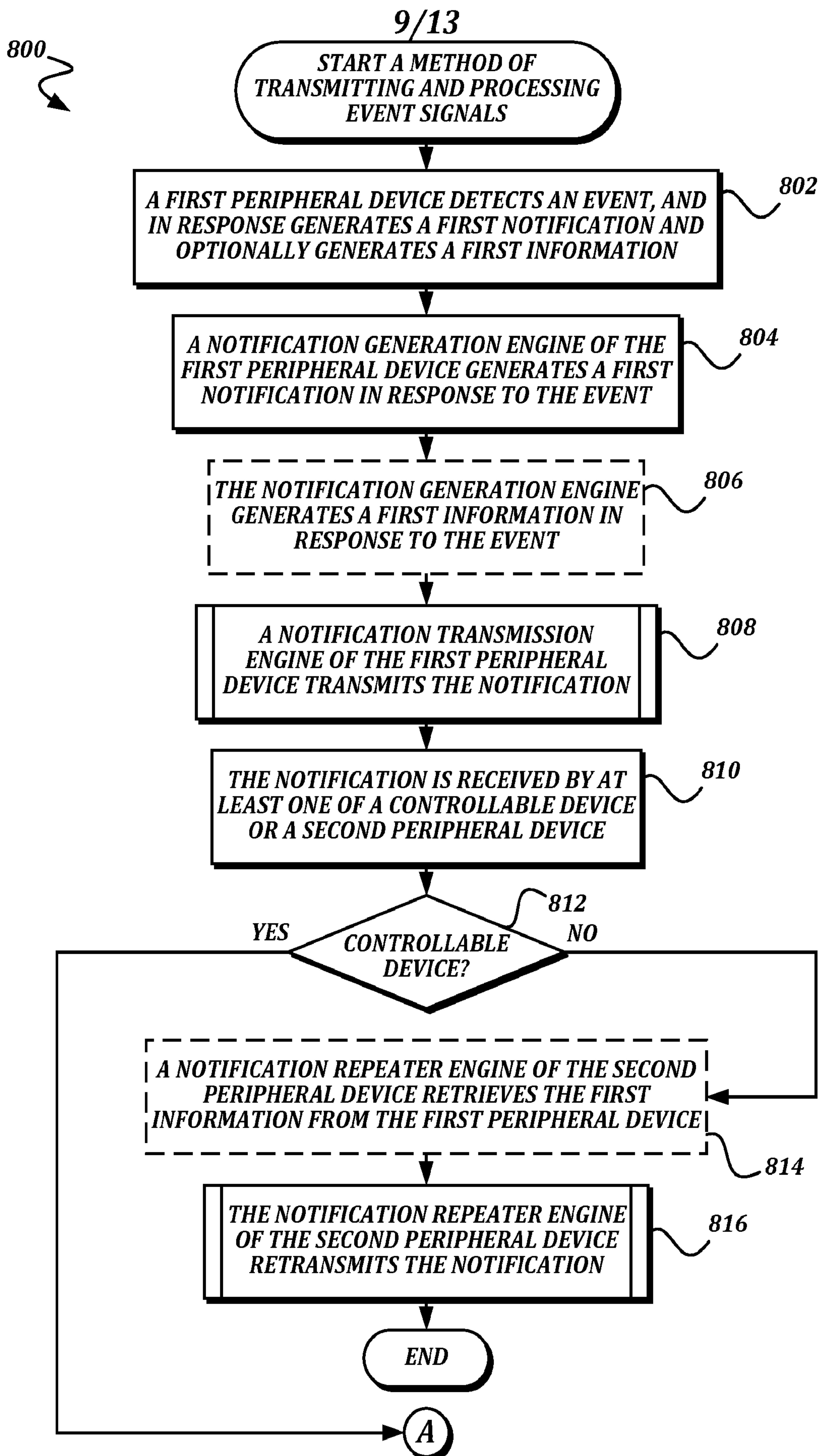
**FIG. 7A**

7/13

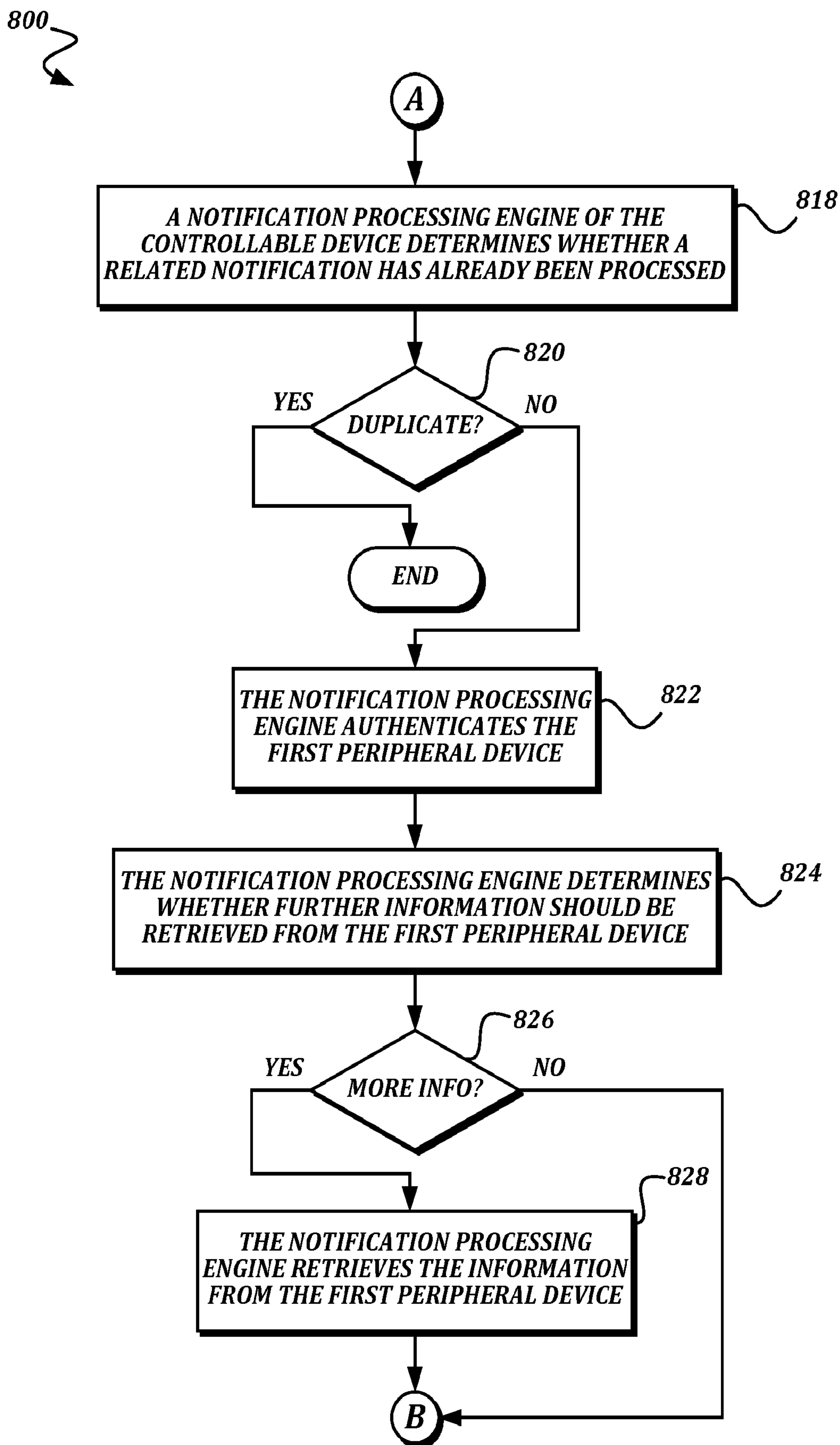
**FIG. 7B**

8/13

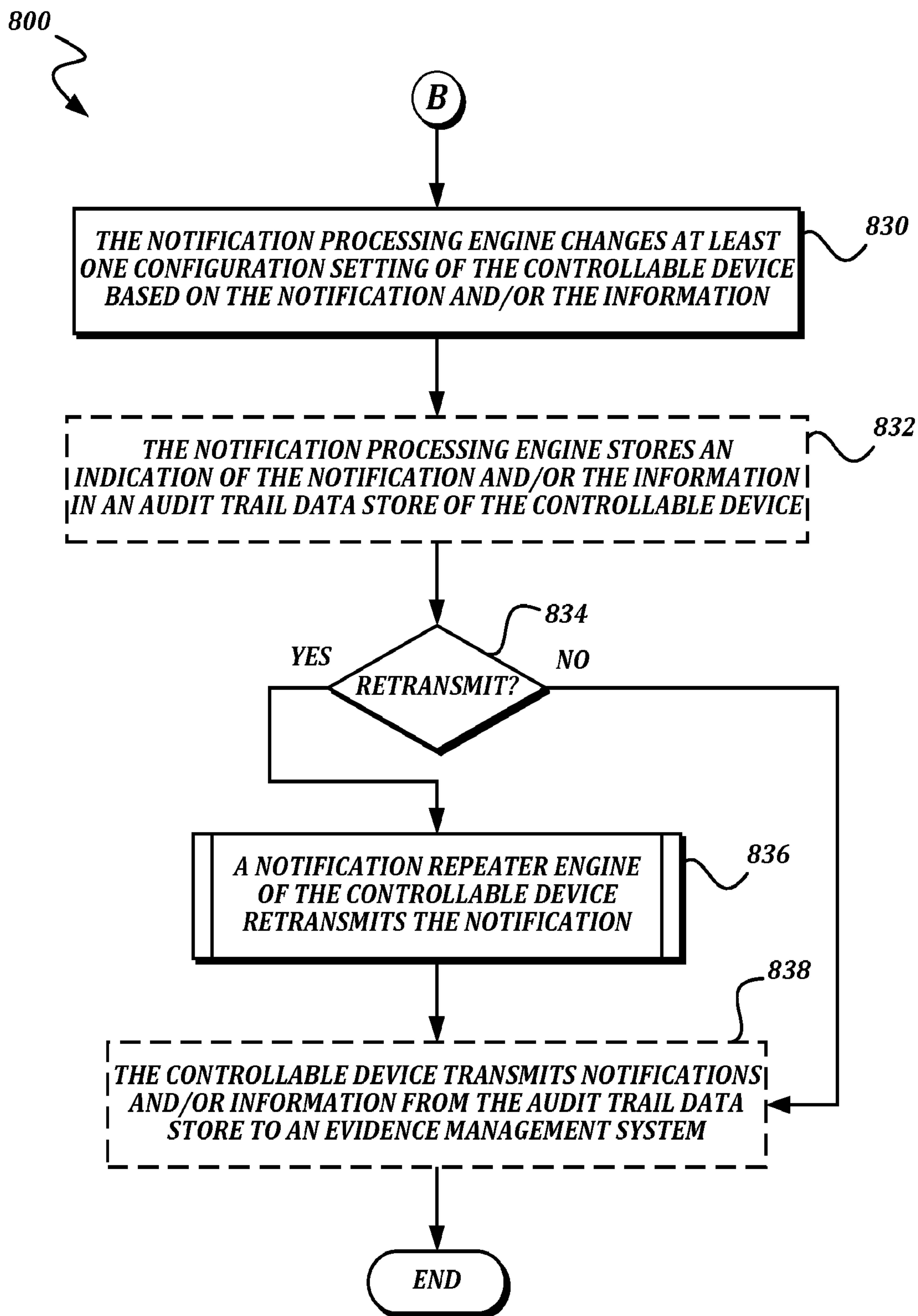
**FIG. 7C**



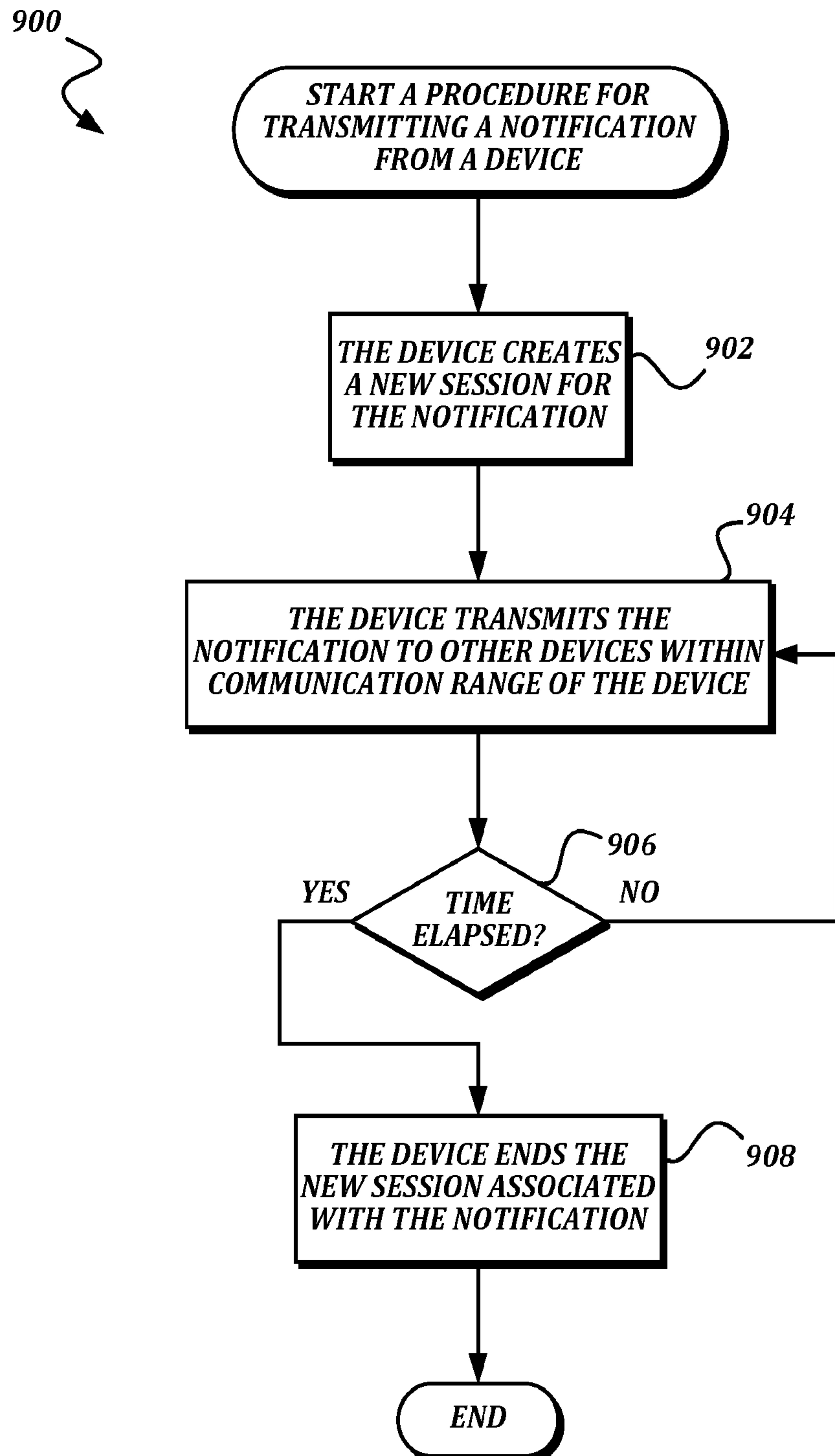
10/13

**FIG. 8B**

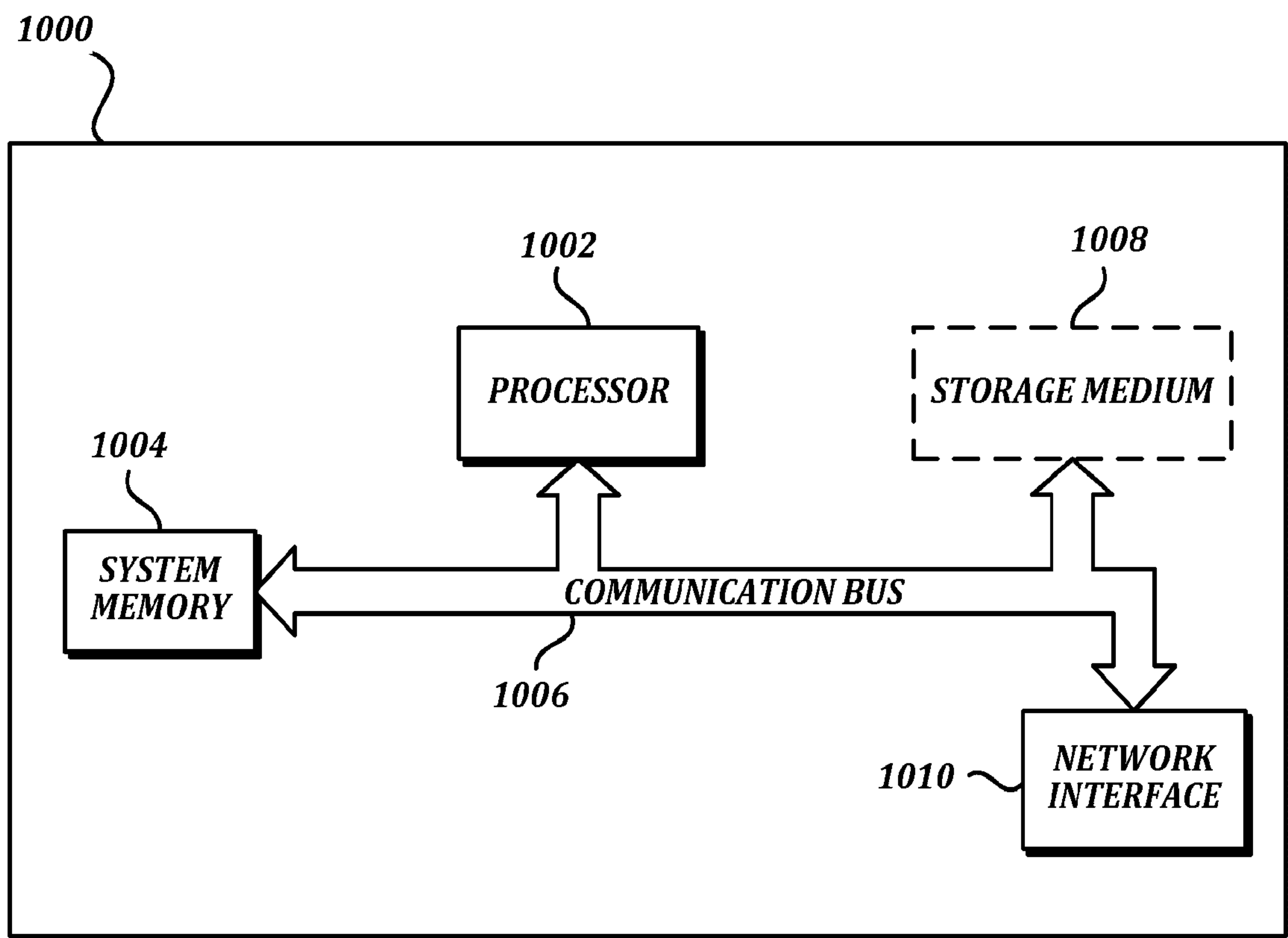
11/13

**FIG. 8C**

12/13

**FIG. 9**

13/13

**FIG. 10**

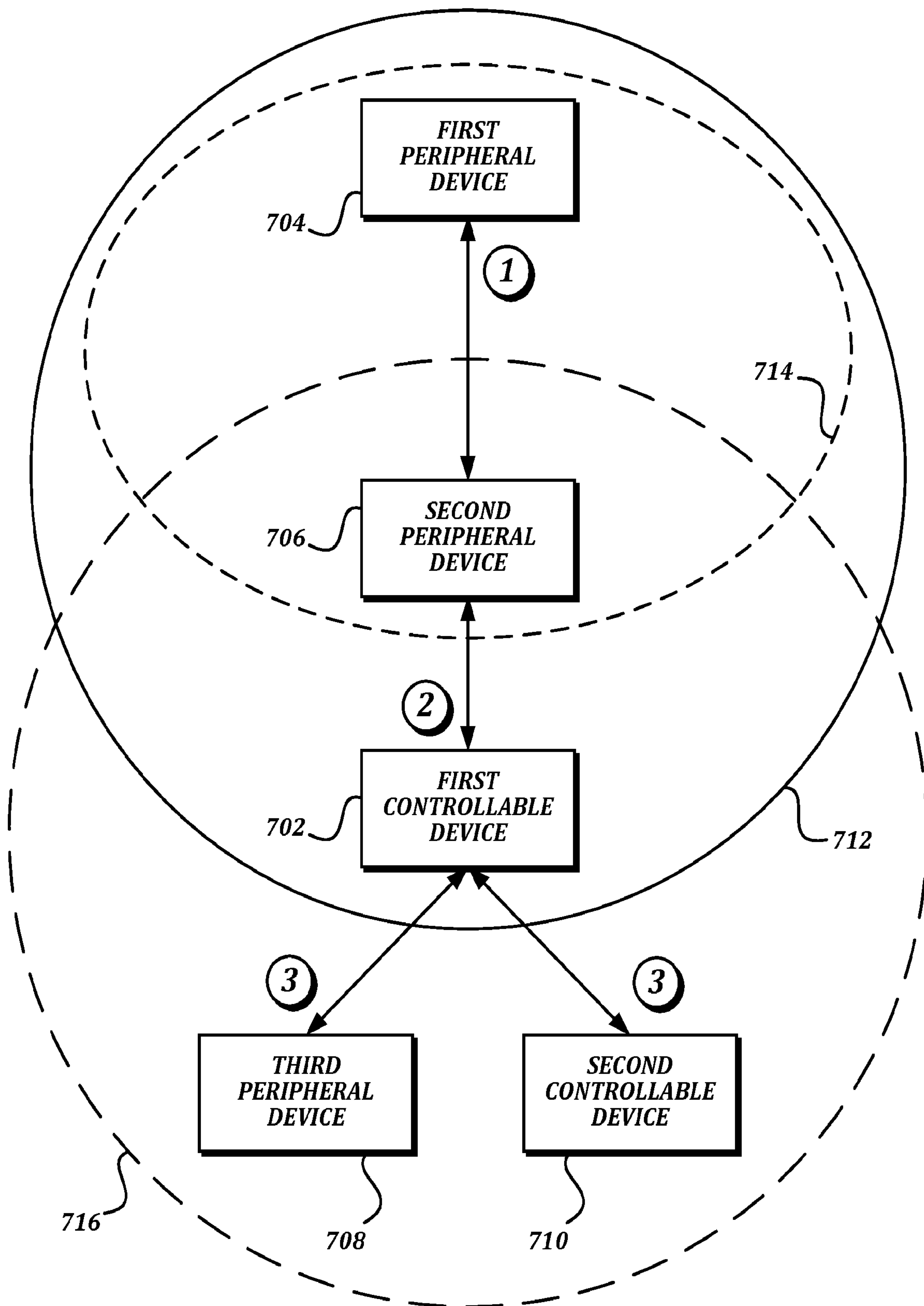


FIG. 7A