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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 September 2017 (08.09.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/151287 A1

(51) International Patent Classification:
H04L 29/08 (2006.01) *H04L 12/18* (2006.01)

(21) International Application Number:
PCT/US2017/017181

(22) International Filing Date:
9 February 2017 (09.02.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/060,298 3 March 2016 (03.03.2016) US

(71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95054 (US).

(72) Inventors: **PRIEV, Avi**; P.O.B. 3173, Har Hotzvim, 91031 Jerusalem (IL). **POGORELIK, Oleg**; Alonim 12, 73133 Lapid (IL).

(74) Agent: **JORDAN, B. Delano**; Jordan IP Law, LLC, c/o CPA Global, 900 Second Avenue South, Suite 600, Minneapolis, Minnesota 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

WO 2017/151287 A1

(54) Title: EFFECTIVE HANDLING OF DISTRESS SIGNALS IN AN INTERNET OF THINGS ENVIRONMENT

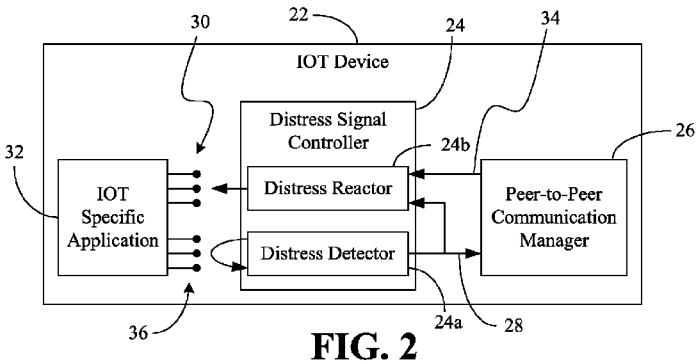


FIG. 2

(57) Abstract: Systems and methods may detect a condition with respect to a first device and generate a distress signal if the condition satisfies one or more safety criteria that are relevant to a second device. Additionally, the distress signal may be broadcasted, wherein the distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area. In one example, one or more local preventive actions may be triggered, via the application control(s), based on the distress signal.

EFFECTIVE HANDLING OF DISTRESS SIGNALS IN AN INTERNET OF THINGS ENVIRONMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims the benefit of priority to U.S. Non-Provisional Patent Application No. 15/060,298 filed on March 3, 2016.

TECHNICAL FIELD

Embodiments generally relate to distress signals. More particularly, embodiments relate to the effective handling of distress signals in an Internet of Things (IOT) environment.

BACKGROUND

The Internet of Things (IOT) may involve household devices such as thermostats, washers/dryers, and so forth, interactively reporting operational data to homeowners, utility companies, and other analytical services, wherein most modern IOT devices may be developed to support centralized control. Accordingly, when a particular IOT device has a message for one or more other IOT devices, the message may be passed through higher level control systems and that may delay or even drop the message if the system is busy or the other IOT device(s) are isolated (e.g., not connected to the centralized control). As a result, in some IOT systems, intercommunication between IOT peers is slow or impossible. Indeed, the intercommunication challenges may be heightened in systems involving complex heterogeneous IOT deployments. Moreover, in mission critical systems such as, for example, security installations, fire alarm systems, etc., such delays and/or disconnects may be unacceptable.

BRIEF DESCRIPTION OF THE DRAWINGS

The various advantages of the embodiments will become apparent to one skilled in the art by reading the following specification and appended claims, and by referencing the following drawings, in which:

FIG. 1 is an illustration of an example of an IOT environment according to an embodiment;

FIG. 2 is a block diagram of an example of an IOT device including a logic architecture according to an embodiment;

FIGs. 3A and 3B are flowcharts of examples of methods of operating a distress signal controller according to an embodiment;

FIG. 4 is a flowchart of an example of a distress signal processing scenario according to an embodiment;

FIG. 5 is a flowchart of an example of a distress signal generation scenario according to an embodiment; and

FIG. 6 is a block diagram of an example of an interoperable device according to an embodiment.

DESCRIPTION OF EMBODIMENTS

Turning now to FIG. 1, an IOT environment is shown in which a first device 10 and a second device 12 operate within proximity to one another. In the illustrated example, the first device 10 is a robotic cleaner and the second device 12 is a smart water tap that supplies water to an appliance 14 (e.g., washing machine), although other types and configurations of devices may be used. The illustrated appliance 14 has a leaking valve 16 that causes water 18 to be deposited on the floor. Because the first device 10 is cleaning the floor, the first device 10 may detect the water 18 on the floor and automatically recognize that the water 18 is a condition (e.g., "Broadcast Emergency when detect water in unusual place") that gives rise to a safety concern such as, for example, flooding, property damage, slippery walking conditions, etc. Moreover, the first device 10 may automatically determine that the condition is relevant to the second device 12, which functions as a source of water to the appliance 14, in the illustrated example. Accordingly, the first device 10 may broadcast a distress signal 20 that is received by the second device 12. The second device 12 may be configured to conduct one or more local preventive actions (e.g., "Close water on emergency") in response to the distress signal 20. The illustrated solution therefore enables the prevention of further possible damage.

As will be discussed in greater detail, the broadcast of the distress signal 20 may bypass one or more application controls of the first device 10, wherein the application controls may constitute a higher level communication path (e.g., uplink) to a centralized control system (e.g., server, analytical service, etc., not shown) also having a higher level communication path (e.g., downlink) to the second device 12.

The illustrated peer-to-peer connection between the first device 10 and the second device 12 may therefore eliminate/reduce delays and/or dropped messages if the centralized control system is busy, the first or second devices 10, 12 are disconnected from the centralized control system, and so forth. Moreover, as will be discussed in greater detail, the first device 10 and the second device 12 may use the same or different protocols to communicate with the centralized control system. In the case of different protocols, the devices 10, 12 may communicate with one another through a translation gateway and/or translation/pairing components disposed within the devices 10, 12 themselves.

Additionally, the distress signal 20 may be configured with a transmission range that is restricted to the local area of the first device 10 and the second device 12. Limiting the transmission range may simplify the interoperability solution because the second device 12 may only need to be concerned with distress signals originating from nearby devices. In this regard, the distress signal 20 may be transmitted wirelessly via, for example, Bluetooth (e.g., Bluetooth Core Specification Version 4.0, June 30, 2010, Bluetooth Special Interest Group/SIG), Wi-Fi (Wireless Fidelity, e.g., Institute of Electrical and Electronics Engineers/IEEE 802.11-2007, Wireless Local Area Network/LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications), radio frequency (RF), infrared (IR), optical (e.g., light emitting diode/LED), or other transmission.

In one example, the distress signal 20 is encoded with an interoperability message that indicates parameters such as, for example, the alarm type, severity level, size of the affected area, event label, source identifier (ID), location, time, etc., or any combination thereof. For example, the interoperability message might be Morse coded into the flashing of an LED on the first device 10, wherein the second device 12 may be configured to optically detect the flashing and decode the interoperability message. Other encoding techniques may also be used.

The first device 10 may also trigger local preventive actions (e.g., shutdown, travel to a safe area) based on the distress signal 20 and/or the condition(s) giving rise to the distress signal 20. In this regard, the first device 10 may also discontinue the broadcast of the distress signal 20 after a predetermined number of transmissions (e.g., three) in order to prevent collisions with other distress signals and/or confusion/false positives on the part of the first device 10. For example, if a third device (not shown) and the first device 10 concurrently broadcast distress signals,

discontinuing the broadcast signal 20 as described herein might enable both the first device 10 and the second device 12 to distinguish between the illustrated distress signal 20 and the distress signal (not shown) from the third device.

FIG. 2 shows an Internet of Things (IOT) device 22 that includes a logic architecture with a distress signal controller 24 (24a, 24b) and a peer-to-peer communication manager 26. In the illustrated example, the controller 24 includes a distress detector 24a to detect a condition with respect to the IOT device 22 and generate an outbound distress signal 28 if the condition satisfies one or more safety criteria (e.g., flooding, smoke, fire, earthquake, electrical short, etc.) that are relevant to a second device (not shown). In one example, the distress detector 24a polls one or more sensors 36 of the IOT device 22 in order to detect the condition.

Additionally, the peer-to-peer communication manager 26 may broadcast the outbound distress signal 28, wherein the outbound distress signal 28 bypasses one or more controls 30 of an IOT specific application 32. The application 32 may generally be part of a higher level uplink to a centralized control system (not shown). Moreover, the outbound distress signal 28 may have a transmission range that is restricted to a local area. For example, the peer-to-peer communication manager 26 may include one or more wireless physical transport components such as, for example, a Bluetooth radio, Wi-Fi radio, RF radio/antenna, IR transmitter, optical transmitter (e.g., LED), and so forth. In one example, the peer-to-peer communication manager 26 discontinues the broadcast of the outbound distress signal 28 after a predetermined number of transmissions.

The illustrated controller 24 also includes a distress reactor 24b to trigger, via the control(s) 30, one or more local preventive actions such as, for example, shutdown of the IOT device 22, reporting, etc., based on the outbound distress signal 28. Reporting (e.g., to a centralized control service) may be through a communication component (not shown) such as, for example, a Bluetooth radio or a Wi-Fi radio, wherein the component may be separate from or integrated with one or more physical transport components used by the peer-to-peer communication manager 26. The distress reactor 24b may also receive an inbound distress signal 34 originating from another nearby device (not shown), wherein the peer-to-peer communication manager 26 may capture the inbound distress signal 34 via, for example, Bluetooth radio, Wi-Fi radio, RF radio/antenna, IR transmitter, optical receiver, camera, etc. The outbound distress signal 28 and/or the inbound distress signal 34 may be encoded

with an interoperability message that indicates, for example, an alarm type, a severity level, a size of an affected area, an event label, a source ID, a location, a time, and so forth.

Additionally, if the IOT device 22 uses a different communication protocol than one or more other nearby devices (not shown), the peer-to-peer communication manager 26 might include a translation and/or pairing component to ensure that the outbound distress signal 28 is understood by the other nearby device(s) and/or the inbound distress signal 34 is understood by the illustrated IOT device 22. For example, a pairing phase may provide the devices in question with an opportunity to establish common parameters to be used during the real-time exchange of distress signals. The translation/pairing component may also access a local database that enables conversion between interoperability messages having different formats, wherein the database may be stored to the device 22 during manufacture and/or updated after deployment. In another example, the device 22 may communicate with other nearby devices through a translation gateway operating within physical proximity of the devices in question. Other solutions may also be used to support different communication protocols.

FIG. 3A shows a method 38 of operating a logic architecture including a distress signal controller. The method 38 may generally be implemented in a device such as, for example, the devices 10, 12 (FIG. 1) and/or the IOT device 22 (FIG. 2), already discussed. More particularly, the method 38 may be implemented in one or more modules as a set of logic instructions stored in a machine- or computer-readable storage medium such as random access memory (RAM), read only memory (ROM), programmable ROM (PROM), firmware, flash memory, etc., in configurable logic such as, for example, programmable logic arrays (PLAs), field programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), in fixed-functionality logic hardware using circuit technology such as, for example, application specific integrated circuit (ASIC), complementary metal oxide semiconductor (CMOS) or transistor-transistor logic (TTL) technology, or any combination thereof.

Illustrated processing block 40 provides for detecting a condition with respect to a first device. Block 40 may include, for example, polling one or more sensors (e.g., moisture sensors, temperature sensors, motion sensors, cameras, etc.) of the first device. A determination may be made at block 42 as to whether the condition

satisfies one or more safety criteria (e.g., flooding, smoke, fire, earthquake, electrical short, etc.) that are relevant to a second device. If so, illustrated block 44 generates a first distress signal. As already noted, the first distress signal may be encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source ID, a location or a time.

Block 46 may broadcast the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area. Illustrated block 48 triggers, via the one or more application controls, one or more local preventive actions based on the first distress signal. Additionally, the broadcast of the first distress signal may be discontinued after a predetermined number of transmissions at block 50. If a safety criteria is not satisfied at block 42, the illustrated method 38 terminates.

FIG. 3B shows another method 52 of operating a logic architecture including a distress signal controller. The method 52 may generally be implemented in a device such as, for example, the devices 10, 12 (FIG. 1) and/or the IOT device 22 (FIG. 2), already discussed. More particularly, the method 52 may be implemented in one or more modules as a set of logic instructions stored in a machine- or computer-readable storage medium such as RAM, ROM, PROM, firmware, flash memory, etc., in configurable logic such as, for example, PLAs, FPGAs, CPLDs, in fixed-functionality logic hardware using circuit technology such as, for example, ASIC, CMOS or TTL technology, or any combination thereof.

Illustrated processing block 54 provides for receiving a second distress signal associated with a third device. Additionally, block 56 may trigger, via the one or more application controls, one or more local preventive actions based on the second distress signal.

FIG. 4 shows a distress signal processing scenario in which a peer-to-peer communication manager such as, for example, the communication manager 26 (FIG. 2) receives a distress signal at a beginning block 60. A distress reactor such as, for example, the distress reactor 24b (FIG. 2), may determine at block 62 whether the distress signal is new. If so, the distress reactor may process the distress signal at block 64 and determine at block 66 whether a local preventive action is associated with the distress signal. Block 66 may take into consideration the various interoperability message attributes (e.g., alarm type, severity level, size of the affected area, event label, source ID, location, time) that may be embedded into the distress

signal as well as any known actions (e.g., close on water emergency) linked to the attributes. If an action is identified, an IOT specific action such as, for example, the application 32 (FIG. 2), may perform the selected preventive action at block 68 and terminate the process at block 70.

If it is determined at block 62 that the distress signal is not new, the distress reactor may drop the signal at block 72 and terminate the process at block 70. Additionally, if it is determined at block 66 that there are no local preventive actions associated with the distress signal, the distress reactor may terminate the process at block 70.

FIG. 5 shows a distress signal generation scenario in which an IOT specific action such as, for example, the application 32 (FIG. 2), identifies a condition with respect to an IOT device at a beginning block 74. A distress detector such as, for example, the distress detector 24a (FIG. 2) may obtain information relevant to the condition by, for example, polling one or more sensors on the IOT device in question. The distress detector may determine whether the condition is critical (e.g., the condition satisfies one or more safety criteria) at block 76. If so, the distress detector may generate a distress signal at block 78, wherein a peer-to-peer communication manager such as, for example, the communication manager 26 (FIG. 2) may issue a distress signal broadcast at a block 80 and terminate at block 82. Additionally, if it is determined at block 76 that the condition is critical, a distress reactor such as, for example, the distress reactor 24b (FIG. 2), may perform a selected distress reactor action (e.g., trigger a local preventive action) at block 84. The IOT specific application may perform the local preventive action at block 86 and terminate at block 82. If it is determined at block 76 that the condition is not critical, the distress detector may simply terminate at block 82.

FIG. 6 shows an interoperable device 90 such as, for example, a robotic cleaner, smart water tap/valve, etc. The device 90 may be readily substituted for the devices 10, 12 (FIG. 1) and/or the IOT device 22 (FIG. 2), already discussed. In the illustrated example, the device 90 includes a battery 92 to supply power to the device 90 and a processor 94 having an application 95 (e.g., IOT specific application) and an integrated memory controller (IMC) 96, which may communicate with system memory 98. The system memory 98 may include, for example, dynamic random access memory (DRAM) configured as one or more memory modules such as, for

example, dual inline memory modules (DIMMs), small outline DIMMs (SODIMMs), etc.

The illustrated device 90 also includes an input output (IO) module 100 implemented together with the processor 94 on a semiconductor die (not shown) as a system on chip (SoC), wherein the IO module 100 functions as a host device and may communicate with, for example, a peer-to-peer communication manager 102 and mass storage 104 (e.g., flash memory, block storage, solid state disk/SSD, etc.). The IO module 100 may include logic 106 (e.g., implemented in logic instructions, configurable logic, fixed-functionality logic hardware, etc., or any combination thereof) that detects a condition with respect to the device 90 and generates an outbound distress signal if the condition satisfies one or more safety criteria that are relevant to a second device. Additionally, the logic 106 may broadcast the outbound distress signal via the peer-to-peer communication manager 102, wherein the outbound distress signal bypasses one or more application controls of the device 90 and has a transmission range that is restricted to a local area.

Moreover, the logic 106 may trigger, via the one or more application controls, one or more local preventive actions based on the outbound distress signal. In one example, the logic 106 receives, via the peer-to-peer communication manager 102, an inbound distress signal and triggers, via the one or more application controls, one or more local preventive actions based on the inbound distress signal. Thus, the logic 106 may implement one or more aspects of the method 38 (FIG. 3A) and/or the method 52 (FIG. 3B), already discussed.

Additional Notes and Examples:

Example 1 may include an interoperable first device comprising a peer-to-peer communication manager, one or more application controls, and logic, implemented at least partly in one or more of configurable logic or fixed-functionality logic hardware, to detect a condition with respect to the first device, generate a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device, and broadcast, via the peer-to-peer communication manager, the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

Example 2 may include the first device of Example 1, wherein the logic is to trigger, via the one or more application controls, one or more local preventive actions based on the first distress signal.

Example 3 may include the first device of Example 1, wherein the logic is to receive a second distress signal associated with a third device, and trigger one or more local preventive actions based on the second distress signal.

Example 4 may include the first device of Example 1, further including one or more sensors, wherein the logic is to poll at least one of the one or more sensors to detect the condition.

Example 5 may include the first device of Example 1, wherein the first distress signal is to be encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

Example 6 may include the first device of any one of Examples 1 to 5, wherein the logic is to discontinue the broadcast of the first distress signal after a predetermined number of transmissions.

Example 7 may include a distress signal controller apparatus comprising logic, implemented at least partly in one or more of configurable logic or fixed-functionality logic hardware, to detect a condition with respect to a first device, generate a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device, and broadcast the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

Example 8 may include the apparatus of Example 7, wherein the logic is to trigger one or more local preventive actions based on the first distress signal.

Example 9 may include the apparatus of Example 7, wherein the logic is to receive a second distress signal associated with a third device, and trigger one or more local preventive actions based on the second distress signal.

Example 10 may include the apparatus of Example 7, wherein the logic is to poll one or more sensors of the first device to detect the condition.

Example 11 may include the apparatus of Example 7, wherein the first distress signal is to be encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

Example 12 may include the apparatus of any one of Examples 7 to 11, wherein the logic is to discontinue the broadcast of the first distress signal after a predetermined number of transmissions.

Example 13 may include a method of operating a distress signal controller, comprising detecting a condition with respect to a first device, generating a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device, and broadcasting the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

Example 14 may include the method of Example 13, further including triggering, via the one or more application controls, one or more local preventive actions based on the first distress signal.

Example 15 may include the method of Example 13, further including receiving a second distress signal associated with a third device, and triggering, via the one or more application controls, one or more local preventive actions based on the second distress signal.

Example 16 may include the method of Example 13, wherein detecting the condition includes polling one or more sensors of the first device.

Example 17 may include the method of Example 13, wherein the first distress signal is encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

Example 18 may include the method of any one of Examples 13 to 17, further including discontinuing the broadcasting of the first distress signal after a predetermined number of transmissions.

Example 19 may include at least one non-transitory computer readable storage medium comprising a set of instructions, which when executed by a first device, cause the first device to detect a condition with respect to the first device, generate a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device, and broadcast the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

Example 20 may include the at least one non-transitory computer readable storage medium of Example 19, wherein the instructions, when executed, further cause the first device to trigger, via the one or more application controls, one or more local preventive actions based on the first distress signal.

Example 21 may include the at least one non-transitory computer readable storage medium of Example 19, wherein the instructions, when executed, cause the first device to receive a second distress signal associated with a third device, and trigger, via the one or more application controls, one or more local preventive actions based on the second distress signal.

Example 22 may include the at least one non-transitory computer readable storage medium of Example 19, wherein the instructions, when executed, cause the first device to poll one or more sensors of the first device to detect the condition.

Example 23 may include the at least one non-transitory computer readable storage medium of Example 19, wherein the first distress signal is to be encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

Example 24 may include the at least one non-transitory computer readable storage medium of any one of Examples 19 to 23, wherein the instructions, when executed, cause the first device to discontinue the broadcast of the first distress signal after a predetermined number of transmissions.

Example 25 may include a distress signal controller apparatus comprising means for detecting a condition with respect to a first device, means for generating a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device, and means for broadcasting the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

Example 26 may include the apparatus of Example 25, further including means for triggering, via the one or more application controls, one or more local preventive actions based on the first distress signal.

Example 27 may include the apparatus of Example 25, further including means for receiving a second distress signal associated with a third device, and means for triggering, via the one or more application controls, one or more local preventive actions based on the second distress signal.

Example 28 may include the apparatus of Example 25, wherein detecting the condition is to include polling one or more sensors of the first device.

Example 29 may include the apparatus of Example 25, wherein the first distress signal is to be encoded with an interoperability message that indicates one or

more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

Example 30 may include the apparatus of any one of Examples 25 to 29, further including means for discontinuing the broadcasting of the first distress signal after a predetermined number of transmissions.

Techniques described herein may therefore improve real time effectiveness in the handling of critical events in IOT systems and provide a lower cost solution. Moreover, scalable IOT solutions may be established with no bottlenecks or mandatory human involvement. Additionally, techniques may support larger and more complex heterogeneous IOT environments, while providing effortless integration between peers and ease of integration into to existing IOT devices and ecosystems.

Embodiments are applicable for use with all types of semiconductor integrated circuit ("IC") chips. Examples of these IC chips include but are not limited to processors, controllers, chipset components, programmable logic arrays (PLAs), memory chips, network chips, systems on chip (SoCs), SSD/NAND controller ASICs, and the like. In addition, in some of the drawings, signal conductor lines are represented with lines. Some may be different, to indicate more constituent signal paths, have a number label, to indicate a number of constituent signal paths, and/or have arrows at one or more ends, to indicate primary information flow direction. This, however, should not be construed in a limiting manner. Rather, such added detail may be used in connection with one or more exemplary embodiments to facilitate easier understanding of a circuit. Any represented signal lines, whether or not having additional information, may actually comprise one or more signals that may travel in multiple directions and may be implemented with any suitable type of signal scheme, e.g., digital or analog lines implemented with differential pairs, optical fiber lines, and/or single-ended lines.

Example sizes/models/values/ranges may have been given, although embodiments are not limited to the same. As manufacturing techniques (e.g., photolithography) mature over time, it is expected that devices of smaller size could be manufactured. In addition, well known power/ground connections to IC chips and other components may or may not be shown within the figures, for simplicity of illustration and discussion, and so as not to obscure certain aspects of the embodiments. Further, arrangements may be shown in block diagram form in order

to avoid obscuring embodiments, and also in view of the fact that specifics with respect to implementation of such block diagram arrangements are highly dependent upon the platform within which the embodiment is to be implemented, i.e., such specifics should be well within purview of one skilled in the art. Where specific details (e.g., circuits) are set forth in order to describe example embodiments, it should be apparent to one skilled in the art that embodiments can be practiced without, or with variation of, these specific details. The description is thus to be regarded as illustrative instead of limiting.

The term "coupled" may be used herein to refer to any type of relationship, direct or indirect, between the components in question, and may apply to electrical, mechanical, fluid, optical, electromagnetic, electromechanical or other connections. In addition, the terms "first", "second", etc. may be used herein only to facilitate discussion, and carry no particular temporal or chronological significance unless otherwise indicated.

Those skilled in the art will appreciate from the foregoing description that the broad techniques of the embodiments can be implemented in a variety of forms. Therefore, while the embodiments have been described in connection with particular examples thereof, the true scope of the embodiments should not be so limited since other modifications will become apparent to the skilled practitioner upon a study of the drawings, specification, and following claims.

CLAIMS

We claim:

1. An interoperable first device comprising:

a peer-to-peer communication manager;

one or more application controls; and

logic, implemented at least partly in one or more of configurable logic or fixed-functionality logic hardware, to:

detect a condition with respect to the first device,

generate a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device, and

broadcast, via the peer-to-peer communication manager, the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

2. The first device of claim 1, wherein the logic is to trigger, via the one or more application controls, one or more local preventive actions based on the first distress signal.

3. The first device of claim 1, wherein the logic is to:

receive a second distress signal associated with a third device, and

trigger one or more local preventive actions based on the second distress signal.

4. The first device of claim 1, further including one or more sensors, wherein the logic is to poll at least one of the one or more sensors to detect the condition.

5. The first device of claim 1, wherein the first distress signal is to be encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

6. The first device of any one of claims 1 to 5, wherein the logic is to discontinue the broadcast of the first distress signal after a predetermined number of transmissions.

7. A distress signal controller apparatus comprising:

logic, implemented at least partly in one or more of configurable logic or fixed-functionality logic hardware, to:

detect a condition with respect to a first device,

generate a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device, and

broadcast the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

8. The apparatus of claim 7, wherein the logic is to trigger one or more local preventive actions based on the first distress signal.

9. The apparatus of claim 7, wherein the logic is to:

receive a second distress signal associated with a third device, and

trigger one or more local preventive actions based on the second distress signal.

10. The apparatus of claim 7, wherein the logic is to poll one or more sensors of the first device to detect the condition.

11. The apparatus of claim 7, wherein the first distress signal is to be encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

12. The apparatus of any one of claims 7 to 11, wherein the logic is to discontinue the broadcast of the first distress signal after a predetermined number of transmissions.

13. A method of operating a distress signal controller, comprising:

detecting a condition with respect to a first device;

generating a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device; and

broadcasting the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

14. The method of claim 13, further including triggering, via the one or more application controls, one or more local preventive actions based on the first distress signal.

15. The method of claim 13, further including:

receiving a second distress signal associated with a third device; and

triggering, via the one or more application controls, one or more local preventive actions based on the second distress signal.

16. The method of claim 13, wherein detecting the condition includes polling one or more sensors of the first device.

17. The method of claim 13, wherein the first distress signal is encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

18. The method of any one of claims 13 to 17, further including discontinuing the broadcasting of the first distress signal after a predetermined number of transmissions.

19. At least one non-transitory computer readable storage medium comprising a set of instructions, which when executed by a first device, cause the first device to:

detect a condition with respect to the first device;

generate a first distress signal if the condition satisfies one or more safety criteria that are relevant to a second device; and

broadcast the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area.

20. The at least one non-transitory computer readable storage medium of claim 19, wherein the instructions, when executed, further cause the first device to trigger, via the one or more application controls, one or more local preventive actions based on the first distress signal.

21. The at least one non-transitory computer readable storage medium of claim 19, wherein the instructions, when executed, cause the first device to:

receive a second distress signal associated with a third device; and

trigger, via the one or more application controls, one or more local preventive actions based on the second distress signal.

22. The at least one non-transitory computer readable storage medium of claim 19, wherein the instructions, when executed, cause the first device to poll one or more sensors of the first device to detect the condition.

23. The at least one non-transitory computer readable storage medium of claim 19, wherein the first distress signal is to be encoded with an interoperability message that indicates one or more of an alarm type, a severity level, a size of an affected area, an event label, a source identifier, a location or a time.

24. The at least one non-transitory computer readable storage medium of any one of claims 19 to 23, wherein the instructions, when executed, cause the first device to discontinue the broadcast of the first distress signal after a predetermined number of transmissions.

25. A distress signal controller apparatus comprising means for performing the method of any one of claims 13 to 17.

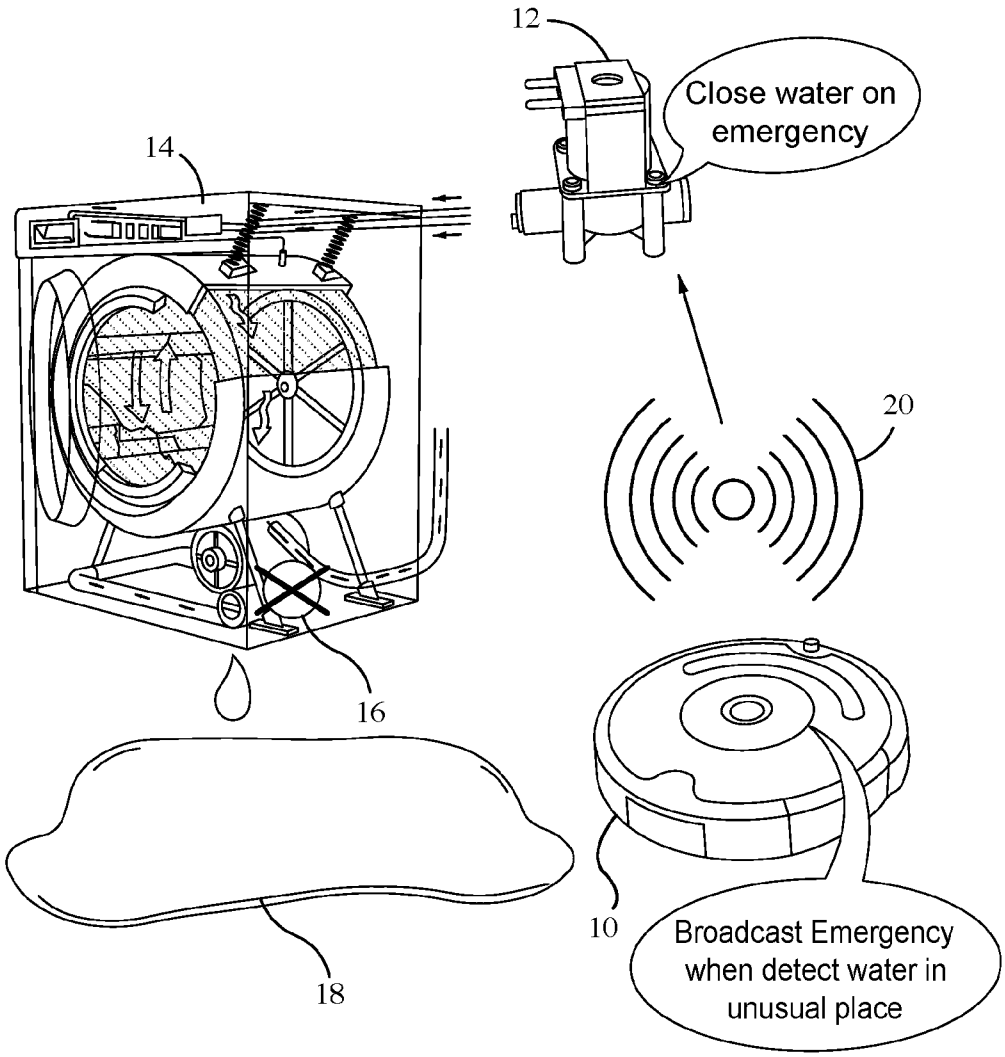

12
Close water on emergency
14
20
16
10
Broadcast Emergency when detect water in unusual place
18

FIG. 1

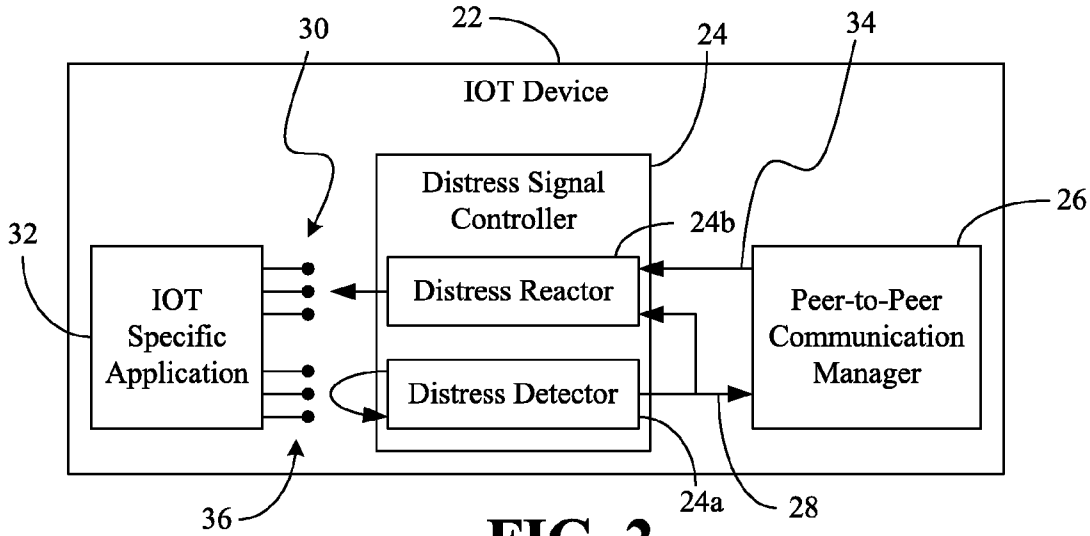

30
22
24
34
IOT Device
Distress Signal Controller
24b
26
32
IOT Specific Application
Distress Reactor
Peer-to-Peer Communication Manager
Distress Detector
36
24a
28

FIG. 2

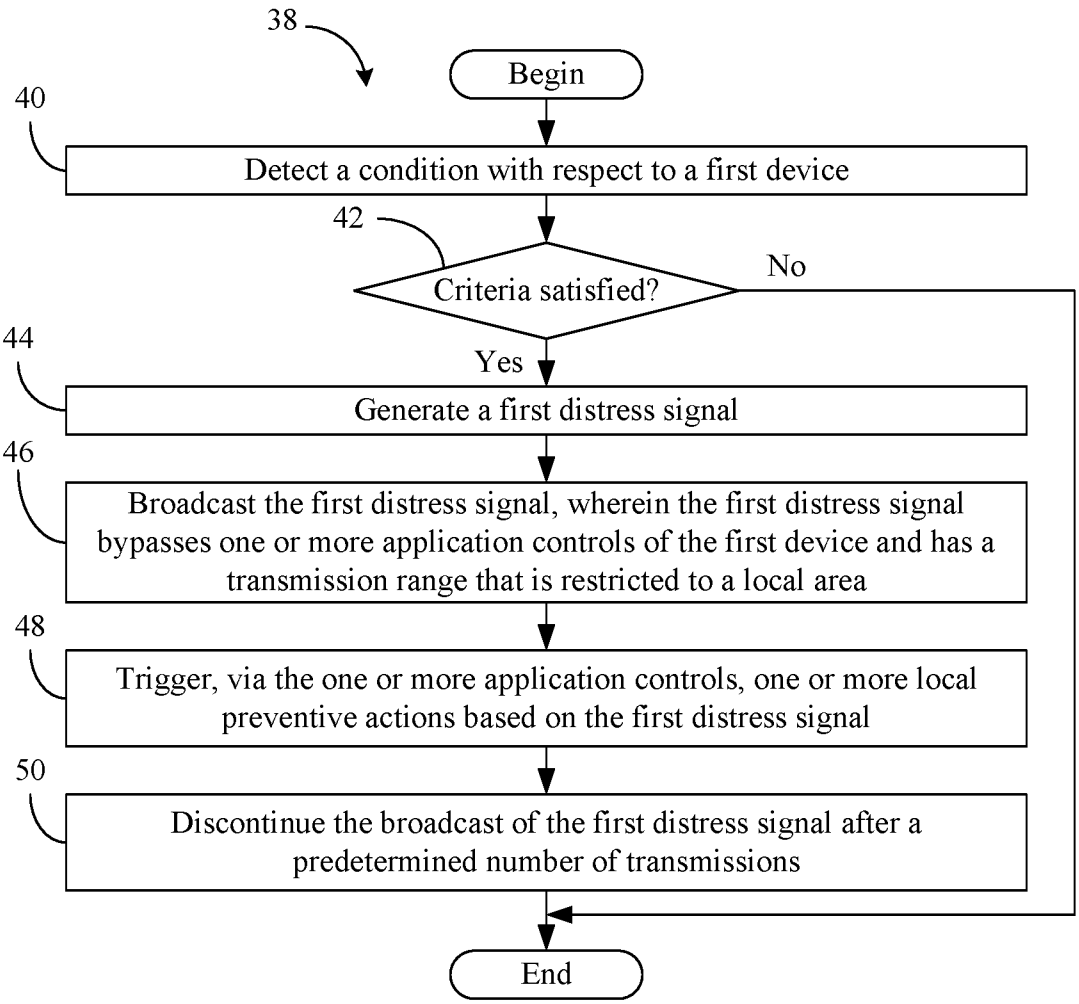

38
Begin
40
Detect a condition with respect to a first device
42
Criteria satisfied?
No
Yes
44
Generate a first distress signal
46
Broadcast the first distress signal, wherein the first distress signal bypasses one or more application controls of the first device and has a transmission range that is restricted to a local area
48
Trigger, via the one or more application controls, one or more local preventive actions based on the first distress signal
50
Discontinue the broadcast of the first distress signal after a predetermined number of transmissions
End

FIG. 3A

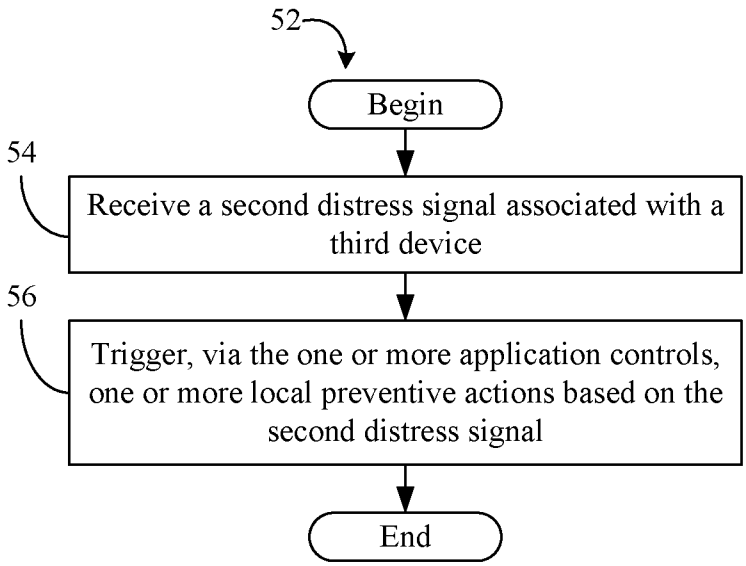

52
Begin
54
Receive a second distress signal associated with a third device
56
Trigger, via the one or more application controls, one or more local preventive actions based on the second distress signal
End

FIG. 3B

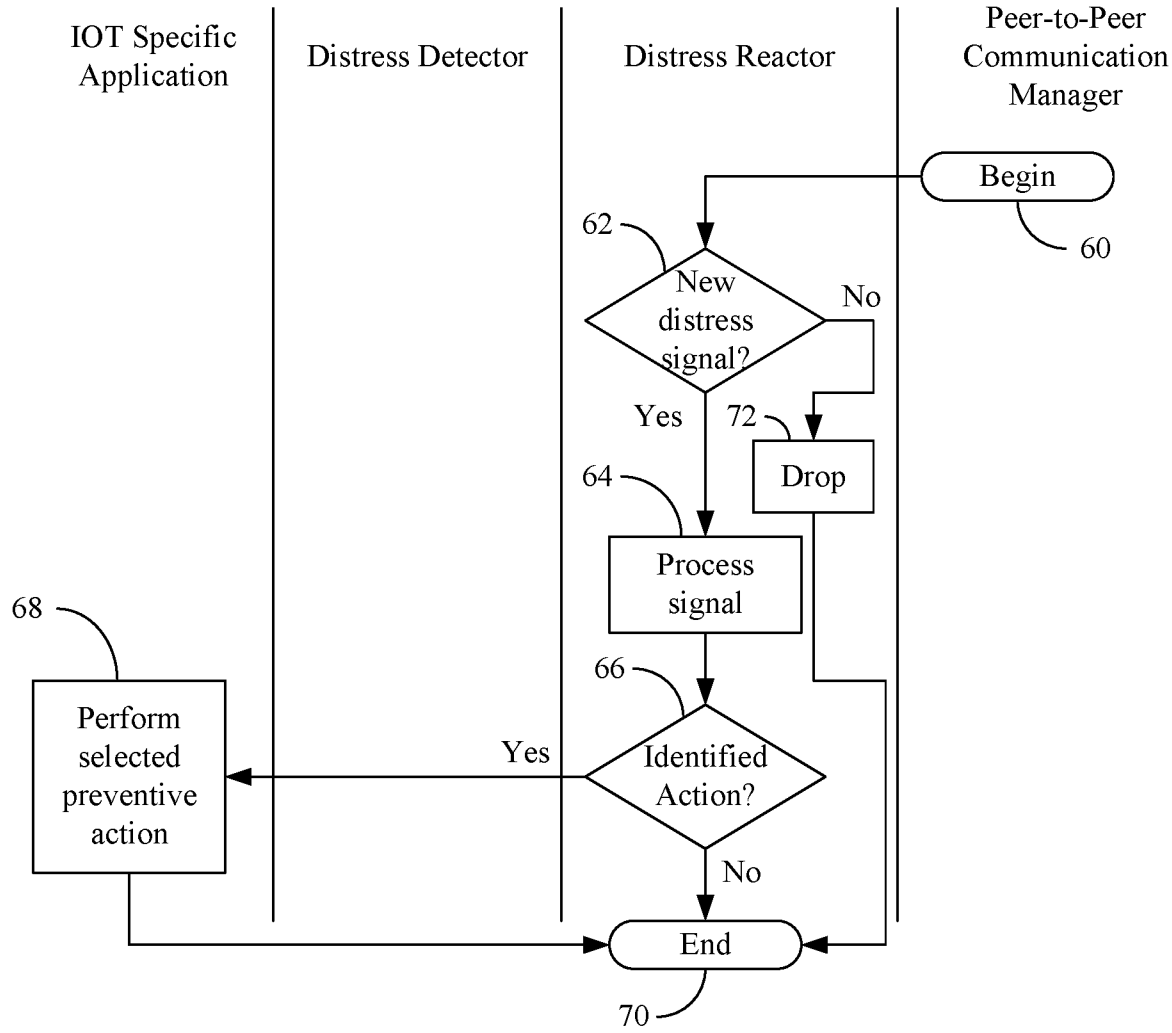

IOT Specific Application
Distress Detector
Distress Reactor
Peer-to-Peer Communication Manager
Begin
60
62
New distress signal?
No
Yes
72
Drop
64
Process signal
66
Identified Action?
Yes
No
68
Perform selected preventive action
End
70

FIG. 4

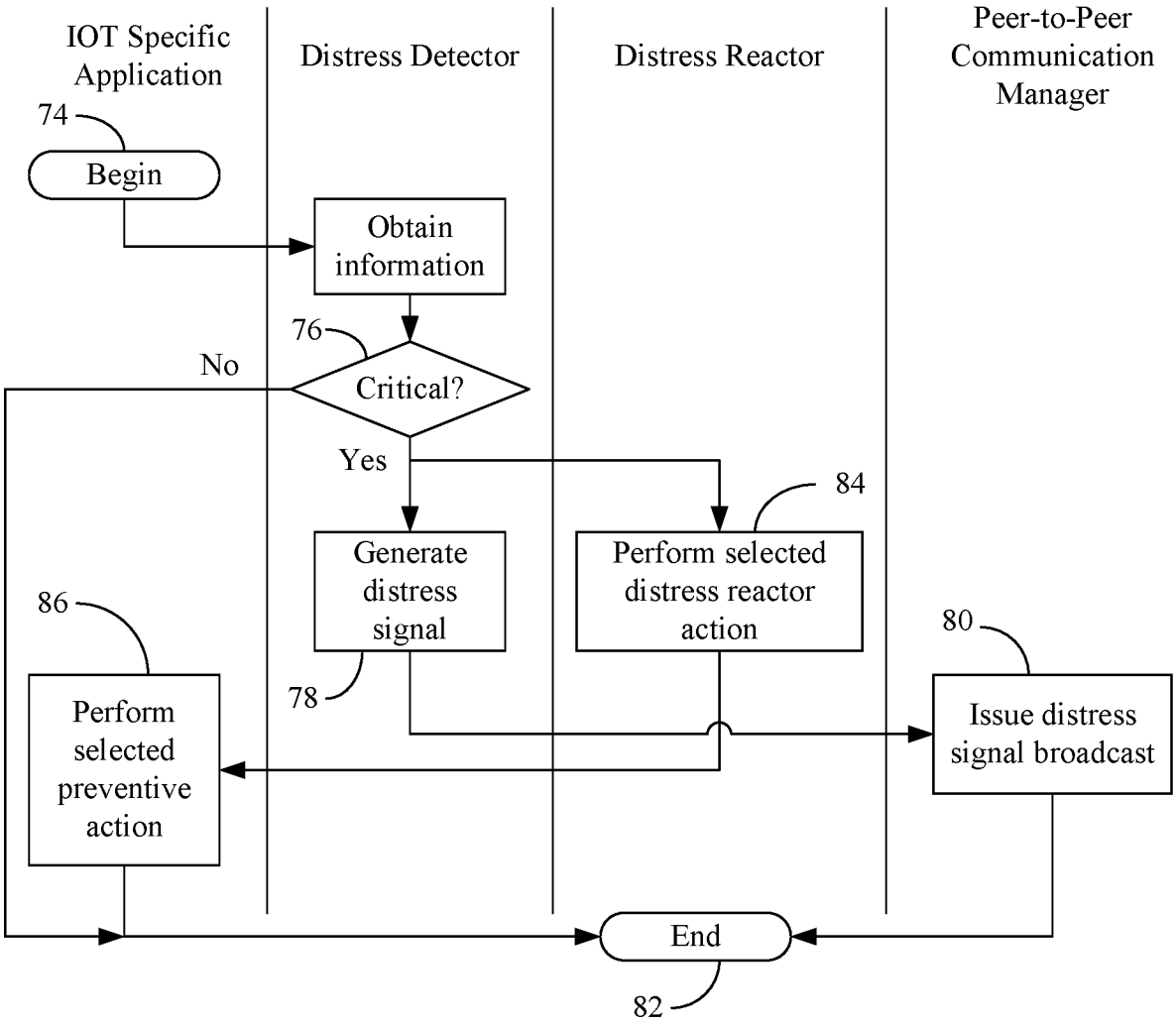

IOT Specific Application
Distress Detector
Distress Reactor
Peer-to-Peer Communication Manager
74
Begin
Obtain information
76
Critical?
No
Yes
84
Generate distress signal
Perform selected distress reactor action
86
80
78
Perform selected preventive action
Issue distress signal broadcast
End
82

FIG. 5

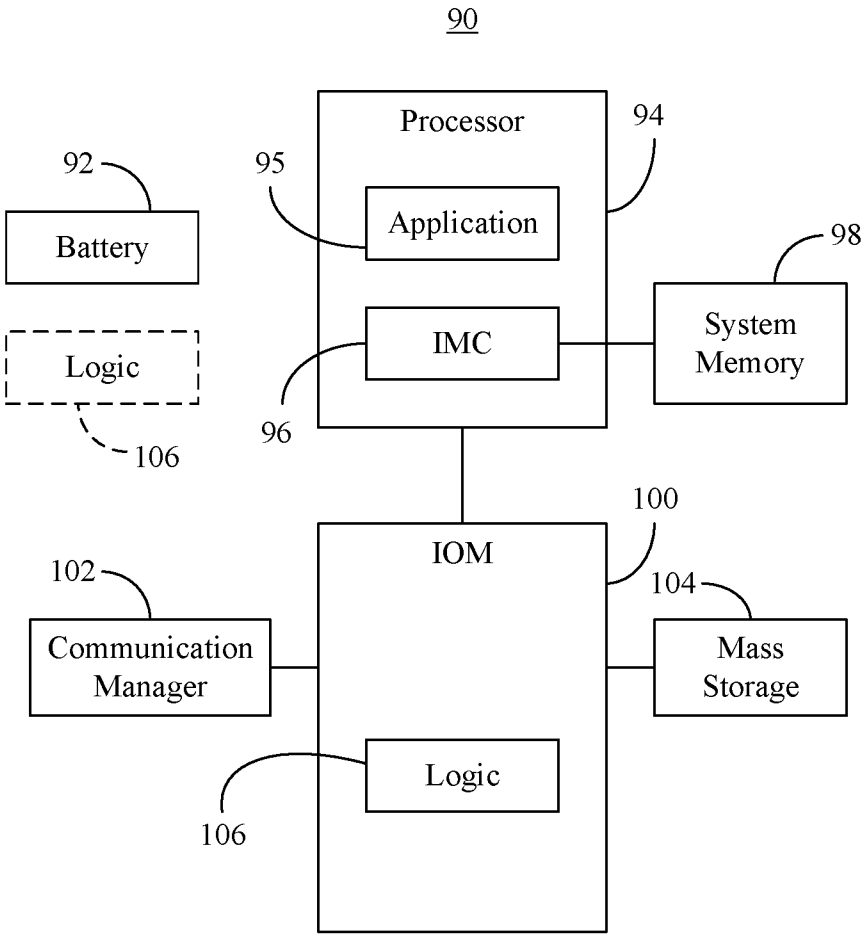

90
Processor
94
92
95
Application
Battery
98
System Memory
IMC
Logic
96
106
100
IOM
102
104
Communication Manager
Mass Storage
Logic
106

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/017181

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08(2006.01)i, H04L 12/18(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 29/08; G06F 15/16; G05B 13/02; H04L 12/26; G08B 21/02; G08B 3/00; H04W 4/00; G06F 21/00; H04L 12/18

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: iot (internet of things), detect, failure, device, condition, distress, signal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015-0019710 A1 (NEURA, INC.) 15 January 2015 See paragraphs [0037]-[0038], [0084], [0133]; and figures 3, 8.	1-25
Y	US 2012-0047551 A1 (SUDHIR B. PATTAR et al.) 23 February 2012 See paragraphs [0004], [0058].	1-25
A	US 2014-0320311 A1 (OLYMPUS CORPORATION) 30 October 2014 See paragraphs [0021]-[0029]; and figures 1-2.	1-25
A	US 2015-0022337 A1 (LEEO, INC.) 22 January 2015 See paragraphs [0156]-[0170]; and figures 15-18.	1-25
A	US 2014-0244001 A1 (QUALCOMM INCORPORATED) 28 August 2014 See paragraphs [0026]-[0047]; and figures 1A-1E.	1-25

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 May 2017 (08.05.2017)	**15 May 2017 (15.05.2017)**

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

Authorized officer
KIM, Seong Woo
Telephone No. +82-42-481-3348

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2017/017181

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015-0019710 A1	15/01/2015	CN 105579993 A	11/05/2016
		CN 105579994 A	11/05/2016
		CN 105683847 A	15/06/2016
		EP 3019919 A1	18/05/2016
		EP 3019969 A2	18/05/2016
		EP 3019970 A1	18/05/2016
		US 09372922 B2	21/06/2016
		US 2015-0019553 A1	15/01/2015
		US 2015-0019714 A1	15/01/2015
		WO 2015-006044 A2	15/01/2015
		WO 2015-006044 A3	19/03/2015
		WO 2015-006045 A1	15/01/2015
		WO 2015-006080 A1	15/01/2015
US 2012-0047551 A1	23/02/2012	CN 102687547 A	19/09/2012
		CN 102687547 B	02/09/2015
		EP 2520110 A1	07/11/2012
		JP 2013-516149 A	09/05/2013
		JP 2015-122752 A	02/07/2015
		JP 5678094 B2	25/02/2015
		KR 10-2012-0099794 A	11/09/2012
		KR 10-2014-0074357 A	17/06/2014
		TW 201141124 A	16/11/2011
		TW I519098 B	21/01/2016
		WO 2011-082150 A1	07/07/2011
US 2014-0320311 A1	30/10/2014	US 09247375 B2	26/01/2016
US 2015-0022337 A1	22/01/2015	US 08947230 B1	03/02/2015
		US 09070272 B2	30/06/2015
		US 09235975 B2	12/01/2016
		US 09257030 B2	09/02/2016
		US 09324227 B2	26/04/2016
		US 2015-020614 A1	22/01/2015
		US 2015-020615 A1	22/01/2015
		US 2015-021465 A1	22/01/2015
		US 2015-022340 A1	22/01/2015
		US 2015-022351 A1	22/01/2015
		US 2015-022352 A1	22/01/2015
		US 2015-022356 A1	22/01/2015
		US 2015-022357 A1	22/01/2015
		WO 2015-009350 A1	22/01/2015
US 2014-0244001 A1	28/08/2014	CN 105009548 A	28/10/2015
		EP 2959663 A1	30/12/2015
		JP 2016-513434 A	12/05/2016
		KR 10-2015-0123850 A	04/11/2015
		WO 2014-131035 A1	28/08/2014