



(51) International Patent Classification:

G05B 15/02 (2006.01) G06K 9/32 (2006.01)
F24F 11/00 (2006.01) G06N 5/04 (2006.01)
G05B 1/00 (2006.01) G06Q 10/06 (2012.01)

(21) International Application Number:

PCT/US2017/025181

(22) International Filing Date:

30 March 2017 (30.03.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/316,468 31 March 2016 (31.03.2016) US

(71) Applicant: JOHNSON CONTROLS TECHNOLOGY COMPANY [US/US]; 49200 Halyard Drive, Plymouth, Michigan 48170 (US).

(72) Inventors: **SINHA, Sudhi**; c/o Johnson Controls Technology Company, 49200 Halyard Drive, Plymouth, Michigan 48170 (US). **PARK, Youngchoon**; c/o Johnson Controls Technology Company, 49200 Halyard Drive, Plymouth, Michigan 48170 (US). **GUSTAFSON, Kyle Richard**; c/o Johnson Controls Technology Company, 49200 Halyard Drive, Plymouth, Michigan 48170 (US). **PLOEGERT, Justin J.**; c/o Johnson Controls Technology Company, 49200 Halyard Drive, Plymouth, Michigan 48170 (US). **PAULSON, Erik**; c/o Johnson Controls Technology Company, 49200 Halyard Drive, Plymouth, Michigan 48170 (US).

(74) Agents: SWIETLIK, Matthew J. et al.; Foley & Lardner LLP, 3000 K Street NW, Suite 600, Washington, District of Columbia 20007 (US).

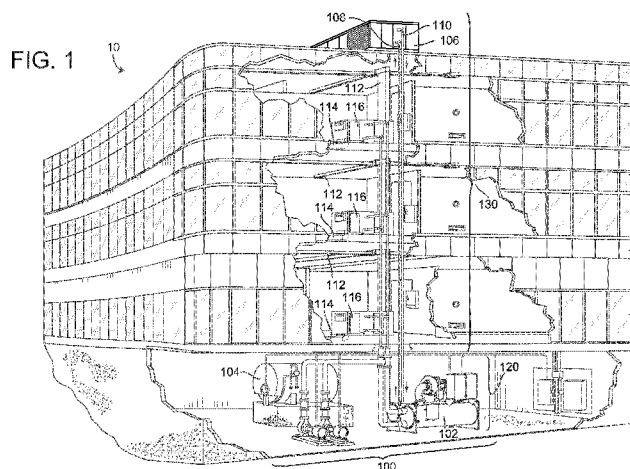
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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))

(54) Title: HVAC DEVICE REGISTRATION IN A DISTRIBUTED BUILDING MANAGEMENT SYSTEM



(57) Abstract: A method for registering an HVAC device in a distributed building management system (BMS). The method includes requesting a token. The token is configured to authorize a registration of the HVAC device. The method further includes receiving the token at a registration service, and receiving a unique ID associated with the HVAC device at the registration service. The method also includes registering the device into a document database of the registration service and generating a device shadow associated with the HVAC device. The method also includes storing the device shadow in the distributed BMS.

HVAC DEVICE REGISTRATION IN A DISTRIBUTED BUILDING MANAGEMENT SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of and priority to U.S. Provisional Patent Application No. 62/316,468 filed March 31, 2016, the entirety of which is incorporated by reference herein.

BACKGROUND

[0002] The present disclosure relates generally to the field of building management systems. A building management system (BMS) is, in general, a system of devices configured to control, monitor, and manage equipment in or around a building or building area. A BMS can include, for example, an HVAC system, a security system, a lighting system, a fire alerting system, any other system that is capable of managing building functions or devices, or any combination thereof.

[0003] In some BMS environments, the individual devices may be smart devices capable of communicating via an internet connection. This may be known as an Internet of Things (IoT) based BMS. In an IoT based BMS, devices may be added over time. However, adding device requires registration of the device into the IoT environment. The newly added device should be registered and verified to ensure that proper security precautions are taken due to the device's connection to the internet. Further, proper registration is needed to ensure that the added device can be integrated into the IoT environment, such that it can operate with the other devices within the IoT environment.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 is a drawing of a building equipped with an HVAC system, according to some embodiments.

[0005] FIG. 2 is a block diagram of a waterside system which may be used as part of the HVAC system of FIG. 1, according to some embodiments.

[0006] FIG. 3 is a block diagram of an airside system which may be used as part of the HVAC system of FIG. 1, according to some embodiments.

[0007] FIG. 4 is a block diagram of a system of smart connected HVAC equipment and a monitoring and service provider recommendation (MSPR) platform that leverages data from the smart connected HVAC equipment to provide service provider recommendations, according to some embodiments.

[0008] FIG. 5 is a block diagram illustrating the MSPR platform communicating directly with people, smart connected devices, buildings, and businesses, according to some embodiments.

[0009] FIG. 6 is a block diagram illustrating a smart connected device communicating with a building infrastructure, a building owner, a MSPR platform, an equipment manufacturer, a facility manager, a contractor, and other connected devices/controllers, according to some embodiments.

[0010] FIG. 7 is a flowchart illustrating multiple stages for implementing the MSPR platform including connected equipment, connected buildings, and connected business, according to some embodiments.

[0011] FIG. 8 is a block diagram illustrating a traditional customer relationship in the HVAC industry, according to some embodiments.

[0012] FIG. 9 is a block diagram illustrating a manufacturer-centric customer relationship made possible by the MSPR platform, according to some embodiments.

[0013] FIG. 10 is a block diagram illustrating a process for providing temporary access credentials to a contractor for accessing a smart connected device to obtain data from the device and perform remote diagnostics, according to some embodiments.

[0014] FIG. 11 is a block diagram illustrating the components of an ecosystem in which the MSPR platform may be implemented, according to some embodiments.

[0015] FIG. 12 is a block diagram illustrating a device to cloud connectivity landscape, according to some embodiments.

[0016] FIG. 13 is a block diagram illustrating a complex event processing mapping, according to some embodiments.

[0017] FIG. 14 is block diagram of a data platform, according to some embodiments.

[0018] FIG. 15 is an entity graph illustrating relationships between an organization, a space, a system, a point, a time series, and a data source, according to some embodiments.

[0019] FIG. 16 is a flow chart illustrating a device registration process, according to some embodiments.

[0020] FIG. 17 is a flow chart illustrating a data flow associated with a device registration process, according to some embodiments.

[0021] FIG. 18 is a block diagram illustrating a distributed BMS device, according to some embodiments.

SUMMARY

[0022] One implementation of the present disclosure is a method for registering an HVAC device in a distributed building management system (BMS). The method includes requesting a token. The token is configured to authorize a registration of the HVAC device. The method further includes receiving the token at a registration service, and receiving a unique ID associated with the HVAC device at the registration service. The method also includes registering the device into a document database of the registration service and generating a device shadow associated with the HVAC device. The method also includes storing the device shadow in a memory of the distributed BMS.

[0023] Another implementation of the present disclosure is a distributed building management system. The system includes an HVAC device and a distributed BMS device. The distributed BMS device includes a processor. The processor is configured to request a token, the token is configured to authorize a registration of the HVAC device. The processor is further configured to receive the token at a registration service and receive a unique ID associated with the HVAC device. The processor is also configured to register the device into a document database of the registration service, and to generate a device shadow associated with the HVAC device within a data platform of the distributed BMS.

[0024] Another implementation of the present disclosure is method for registering an Internet of Things (IoT) HVAC device in a distributed building management system. The method includes requesting a token, the token configured to authorize a registration of the IoT HVAC device. The method further includes receiving the token at a registration service

and receiving a unique ID associated with the IoT HVAC device. The method further includes registering the device into a document database of the registration service and generating a device shadow associated with the IoT HVAC device within a data platform of the distributed BMS. The method further includes claiming the IoT HVAC device. Claiming the IoT HVAC device provides secure communications between the IoT HVAC device and the distributed building management system.

DETAILED DESCRIPTION

Overview

[0025] Advancements in several technology spaces such as Big Data processing, machine learning, and network communication, and rapid convergence of many technologies have contributed to the new possibilities around “Internet of Things” (IoT). IPv6 communication protocol has exponentially magnified the number of IP addresses available for devices to be connected to the internet, and it has also enabled new capabilities around cybersecurity, network assignment and routing, transmission to multiple destinations, simplified processing by routers, amongst others. Advancements in wireless communication and protocols may allow devices to be connected inexpensively and easily. New protocols like MQTT and ZeroMQ provide lightweight data transport between devices and networks. Big data capabilities around parallel storage and processing of data allow for meaningful ways to deal with the massive data deluge caused by this unprecedented device and data connectivity. IoT may provide opportunities to create new economic benefits and business models. An IoT framework may be useful for use in building management systems (BMS) to allow for easier integration and control of smart devices to keep up with the demand for smart buildings and associated systems.

Building With HVAC Equipment

[0026] Referring now to FIG. 1, a perspective view of a building 10 is shown. Building 10 includes a HVAC system 100. HVAC system 100 may include a plurality of HVAC devices (e.g., heaters, chillers, air handling units, pumps, fans, thermal energy storage, etc.) configured to provide heating, cooling, ventilation, or other services for building 10. For example, HVAC system 100 is shown to include a waterside system 120 and an airside system 130. Waterside system 120 may provide a heated or chilled fluid to an air handling

unit of airside system 130. Airside system 130 may use the heated or chilled fluid to heat or cool an airflow provided to building 10. An exemplary waterside system and airside system which may be used in HVAC system 100 are described in greater detail with reference to FIGS. 2-3.

[0027] HVAC system 100 is shown to include a chiller 102, a boiler 104, and a rooftop air handling unit (AHU) 106. Waterside system 120 may use boiler 104 and chiller 102 to heat or cool a working fluid (e.g., water, glycol, etc.) and may circulate the working fluid to AHU 106. In various embodiments, the HVAC devices of waterside system 120 may be located in or around building 10 (as shown in FIG. 1) or at an offsite location such as a central plant (e.g., a chiller plant, a steam plant, a heat plant, etc.). The working fluid may be heated in boiler 104 or cooled in chiller 102, depending on whether heating or cooling is required in building 10. Boiler 104 may add heat to the circulated fluid, for example, by burning a combustible material (e.g., natural gas) or using an electric heating element. Chiller 102 may place the circulated fluid in a heat exchange relationship with another fluid (e.g., a refrigerant) in a heat exchanger (e.g., an evaporator) to absorb heat from the circulated fluid. The working fluid from chiller 102 and/or boiler 104 may be transported to AHU 106 via piping 108.

[0028] AHU 106 may place the working fluid in a heat exchange relationship with an airflow passing through AHU 106 (e.g., via one or more stages of cooling coils and/or heating coils). The airflow may be, for example, outside air, return air from within building 10, or a combination of both. AHU 106 may transfer heat between the airflow and the working fluid to provide heating or cooling for the airflow. For example, AHU 106 may include one or more fans or blowers configured to pass the airflow over or through a heat exchanger containing the working fluid. The working fluid may then return to chiller 102 or boiler 104 via piping 110.

[0029] Airside system 130 may deliver the airflow supplied by AHU 106 (i.e., the supply airflow) to building 10 via air supply ducts 112 and may provide return air from building 10 to AHU 106 via air return ducts 114. In some embodiments, airside system 130 includes multiple variable air volume (VAV) units 116. For example, airside system 130 is shown to include a separate VAV unit 116 on each floor or zone of building 10. VAV units 116 may

include dampers or other flow control elements that can be operated to control an amount of the supply airflow provided to individual zones of building 10. In other embodiments, airside system 130 delivers the supply airflow into one or more zones of building 10 (e.g., via supply ducts 112) without using intermediate VAV units 116 or other flow control elements. AHU 106 may include various sensors (e.g., temperature sensors, pressure sensors, etc.) configured to measure attributes of the supply airflow. AHU 106 may receive input from sensors located within AHU 106 and/or within the building zone and may adjust the flow rate, temperature, or other attributes of the supply airflow through AHU 106 to achieve setpoint conditions for the building zone.

[0030] Referring now to FIG. 2, a block diagram of a waterside system 200 is shown, according to an exemplary embodiment. In various embodiments, waterside system 200 may supplement or replace waterside system 120 in HVAC system 100 or may be implemented separate from HVAC system 100. When implemented in HVAC system 100, waterside system 200 may include a subset of the HVAC devices in HVAC system 100 (e.g., boiler 104, chiller 102, pumps, valves, etc.) and may operate to supply a heated or chilled fluid to AHU 106. The HVAC devices of waterside system 200 may be located within building 10 (e.g., as components of waterside system 120) or at an offsite location such as a central plant.

[0031] In FIG. 2, waterside system 200 is shown as a central plant having a plurality of subplants 202-212. Subplants 202-212 are shown to include a heater subplant 202, a heat recovery chiller subplant 204, a chiller subplant 206, a cooling tower subplant 208, a hot thermal energy storage (TES) subplant 210, and a cold thermal energy storage (TES) subplant 212. Subplants 202-212 consume resources (e.g., water, natural gas, electricity, etc.) from utilities to serve the thermal energy loads (e.g., hot water, cold water, heating, cooling, etc.) of a building or campus. For example, heater subplant 202 may be configured to heat water in a hot water loop 214 that circulates the hot water between heater subplant 202 and building 10. Chiller subplant 206 may be configured to chill water in a cold water loop 216 that circulates the cold water between chiller subplant 206 and building 10. Heat recovery chiller subplant 204 may be configured to transfer heat from cold water loop 216 to hot water loop 214 to provide additional heating for the hot water and additional cooling for the cold water. Condenser water loop 218 may absorb heat from the cold water in chiller subplant 206 and reject the absorbed heat in cooling tower subplant 208 or transfer the absorbed heat to hot

water loop 214. Hot TES subplant 210 and cold TES subplant 212 may store hot and cold thermal energy, respectively, for subsequent use.

[0032] Hot water loop 214 and cold water loop 216 may deliver the heated and/or chilled water to air handlers located on the rooftop of building 10 (e.g., AHU 106) or to individual floors or zones of building 10 (e.g., VAV units 116). The air handlers push air past heat exchangers (e.g., heating coils or cooling coils) through which the water flows to provide heating or cooling for the air. The heated or cooled air may be delivered to individual zones of building 10 to serve the thermal energy loads of building 10. The water then returns to subplants 202-212 to receive further heating or cooling.

[0033] Although subplants 202-212 are shown and described as heating and cooling water for circulation to a building, it is understood that any other type of working fluid (e.g., glycol, CO₂, etc.) may be used in place of or in addition to water to serve the thermal energy loads. In other embodiments, subplants 202-212 may provide heating and/or cooling directly to the building or campus without requiring an intermediate heat transfer fluid. These and other variations to waterside system 200 are within the teachings of the present invention.

[0034] Each of subplants 202-212 may include a variety of equipment configured to facilitate the functions of the subplant. For example, heater subplant 202 is shown to include a plurality of heating elements 220 (e.g., boilers, electric heaters, etc.) configured to add heat to the hot water in hot water loop 214. Heater subplant 202 is also shown to include several pumps 222 and 224 configured to circulate the hot water in hot water loop 214 and to control the flow rate of the hot water through individual heating elements 220. Chiller subplant 206 is shown to include a plurality of chillers 232 configured to remove heat from the cold water in cold water loop 216. Chiller subplant 206 is also shown to include several pumps 234 and 236 configured to circulate the cold water in cold water loop 216 and to control the flow rate of the cold water through individual chillers 232.

[0035] Heat recovery chiller subplant 204 is shown to include a plurality of heat recovery heat exchangers 226 (e.g., refrigeration circuits) configured to transfer heat from cold water loop 216 to hot water loop 214. Heat recovery chiller subplant 204 is also shown to include several pumps 228 and 230 configured to circulate the hot water and/or cold water through heat recovery heat exchangers 226 and to control the flow rate of the water through

individual heat recovery heat exchangers 226. Cooling tower subplant 208 is shown to include a plurality of cooling towers 238 configured to remove heat from the condenser water in condenser water loop 218. Cooling tower subplant 208 is also shown to include several pumps 240 configured to circulate the condenser water in condenser water loop 218 and to control the flow rate of the condenser water through individual cooling towers 238.

[0036] Hot TES subplant 210 is shown to include a hot TES tank 242 configured to store the hot water for later use. Hot TES subplant 210 may also include one or more pumps or valves configured to control the flow rate of the hot water into or out of hot TES tank 242. Cold TES subplant 212 is shown to include cold TES tanks 244 configured to store the cold water for later use. Cold TES subplant 212 may also include one or more pumps or valves configured to control the flow rate of the cold water into or out of cold TES tanks 244.

[0037] In some embodiments, one or more of the pumps in waterside system 200 (e.g., pumps 222, 224, 228, 230, 234, 236, and/or 240) or pipelines in waterside system 200 include an isolation valve associated therewith. Isolation valves may be integrated with the pumps or positioned upstream or downstream of the pumps to control the fluid flows in waterside system 200. In various embodiments, waterside system 200 may include more, fewer, or different types of devices and/or subplants based on the particular configuration of waterside system 200 and the types of loads served by waterside system 200.

[0038] Referring now to FIG. 3, a block diagram of an airside system 300 is shown, according to an exemplary embodiment. In various embodiments, airside system 300 may supplement or replace airside system 130 in HVAC system 100 or may be implemented separate from HVAC system 100. When implemented in HVAC system 100, airside system 300 may include a subset of the HVAC devices in HVAC system 100 (e.g., AHU 106, VAV units 116, ducts 112-114, fans, dampers, etc.) and may be located in or around building 10. Airside system 300 may operate to heat or cool an airflow provided to building 10 using a heated or chilled fluid provided by waterside system 200.

[0039] In FIG. 3, airside system 300 is shown to include an economizer-type air handling unit (AHU) 302. Economizer-type AHUs vary the amount of outside air and return air used by the air handling unit for heating or cooling. For example, AHU 302 may receive return air 304 from building zone 306 via return air duct 308 and may deliver supply air 310 to building

zone 306 via supply air duct 312. In some embodiments, AHU 302 is a rooftop unit located on the roof of building 10 (e.g., AHU 106 as shown in FIG. 1) or otherwise positioned to receive both return air 304 and outside air 314. AHU 302 may be configured to operate exhaust air damper 316, mixing damper 318, and outside air damper 320 to control an amount of outside air 314 and return air 304 that combine to form supply air 310. Any return air 304 that does not pass through mixing damper 318 may be exhausted from AHU 302 through exhaust damper 316 as exhaust air 322.

[0040] Each of dampers 316-320 may be operated by an actuator. For example, exhaust air damper 316 may be operated by actuator 324, mixing damper 318 may be operated by actuator 326, and outside air damper 320 may be operated by actuator 328. Actuators 324-328 may communicate with an AHU controller 330 via a communications link 332.

Actuators 324-328 may receive control signals from AHU controller 330 and may provide feedback signals to AHU controller 330. Feedback signals may include, for example, an indication of a current actuator or damper position, an amount of torque or force exerted by the actuator, diagnostic information (e.g., results of diagnostic tests performed by actuators 324-328), status information, commissioning information, configuration settings, calibration data, and/or other types of information or data that may be collected, stored, or used by actuators 324-328. AHU controller 330 may be an economizer controller configured to use one or more control algorithms (e.g., state-based algorithms, extremum seeking control (ESC) algorithms, proportional-integral (PI) control algorithms, proportional-integral-derivative (PID) control algorithms, model predictive control (MPC) algorithms, feedback control algorithms, etc.) to control actuators 324-328.

[0041] Still referring to FIG. 3, AHU 302 is shown to include a cooling coil 334, a heating coil 336, and a fan 338 positioned within supply air duct 312. Fan 338 may be configured to force supply air 310 through cooling coil 334 and/or heating coil 336 and provide supply air 310 to building zone 306. AHU controller 330 may communicate with fan 338 via communications link 340 to control a flow rate of supply air 310. In some embodiments, AHU controller 330 controls an amount of heating or cooling applied to supply air 310 by modulating a speed of fan 338.

[0042] Cooling coil 334 may receive a chilled fluid from waterside system 200 (e.g., from cold water loop 216) via piping 342 and may return the chilled fluid to waterside system 200 via piping 344. Valve 346 may be positioned along piping 342 or piping 344 to control a flow rate of the chilled fluid through cooling coil 334. In some embodiments, cooling coil 334 includes multiple stages of cooling coils that can be independently activated and deactivated (e.g., by AHU controller 330) to modulate an amount of cooling applied to supply air 310.

[0043] Heating coil 336 may receive a heated fluid from waterside system 200 (e.g., from hot water loop 214) via piping 348 and may return the heated fluid to waterside system 200 via piping 350. Valve 352 may be positioned along piping 348 or piping 350 to control a flow rate of the heated fluid through heating coil 336. In some embodiments, heating coil 336 includes multiple stages of heating coils that can be independently activated and deactivated (e.g., by AHU controller 330) to modulate an amount of heating applied to supply air 310.

[0044] Each of valves 346 and 352 may be controlled by an actuator. For example, valve 346 may be controlled by actuator 354 and valve 352 may be controlled by actuator 356. Actuators 354-356 may communicate with AHU controller 330 via communications links 358-360. Actuators 354-356 may receive control signals from AHU controller 330 and may provide feedback signals to controller 330. In some embodiments, AHU controller 330 receives a measurement of the supply air temperature from a temperature sensor 362 positioned in supply air duct 312 (e.g., downstream of cooling coil 334 and/or heating coil 336). AHU controller 330 may also receive a measurement of the temperature of building zone 306 from a temperature sensor 364 located in building zone 306.

[0045] In some embodiments, AHU controller 330 operates valves 346 and 352 via actuators 354-356 to modulate an amount of heating or cooling provided to supply air 310 (e.g., to achieve a setpoint temperature for supply air 310 or to maintain the temperature of supply air 310 within a setpoint temperature range). The positions of valves 346 and 352 affect the amount of heating or cooling provided to supply air 310 by cooling coil 334 or heating coil 336 and may correlate with the amount of energy consumed to achieve a desired supply air temperature. AHU controller 330 may control the temperature of supply air 310

and/or building zone 306 by activating or deactivating coils 334-336, adjusting a speed of fan 338, or a combination of both.

Smart Connected HVAC Equipment

[0046] Referring now to FIG. 4, a system 400 is shown including a monitoring and service provider recommendation (MSPR) platform 402, a network 404, a gateway 406, and a number of smart connected HVAC equipment 408 is shown, according to an exemplary embodiment. Smart connected HVAC equipment 408 may include an actuator 410, a damper 412, a chiller 414, a heater 416, a rooftop unit (RTU) 418, an air handling unit (AHU) 420, and/or any other type of equipment or device that can be installed within building 10 (e.g., fans, pumps, valves, etc.). Although the present invention is described primarily with reference to HVAC equipment, it should be understood that the systems and methods described herein may be applicable to a wide variety of building equipment and other types of connected devices (e.g., HVAC equipment, LED lights, mobile phones, elevators, fire safety systems, smart street lamps, cars, televisions, etc.) with embedded intelligence and communication capabilities.

[0047] Smart connected HVAC equipment 408 may be configured to communicate with each other and with remote services (e.g., remote monitoring and analytics services, cloud-based control services, etc.). In some embodiments, smart connected HVAC equipment 408 have ubiquitous connectivity (i.e., are always connected) and have their own processing and analytics capabilities. Smart connected HVAC equipment 408 may be managed in the cloud through various software applications and the analytics models built to control them. As such, a field/supervisory controller or building automation system may not be required. For example, a smart actuator that has built in position feedback, computing power, and a communication network can provide a cost-effective solution that can perform local decision making. A series of smart actuators and dampers that work together can provide completely autonomous manipulation of a building and/or BMS.

[0048] Smart connected HVAC equipment 408 may communicate with each other using any of a variety of communications protocols. In some embodiments, smart connected HVAC equipment 408 communicate with each other wirelessly using a wireless communications protocol (e.g. Wi-Fi, Bluetooth, 3G/4G, 802.15.4, ZigBee, etc.). The

particular communications protocol used by smart connected HVAC equipment 408 may be dependent upon the power requirements, bandwidth requirements, and/or the existing infrastructure within the building in which smart connected HVAC equipment 408 are installed. In some embodiments, smart connected HVAC equipment 408 communicate with each other using a proprietary building equipment protocol (e.g., BACNet, ZigBee, Modbus, etc.) to move data between various devices of smart connected HVAC equipment 408. In order to build applications on top of those protocols, these protocols may be converted into the Internet Protocol (IP). In some embodiments, a communications gateway 406 is used for such a conversion.

[0049] In some embodiments, only a few of the smart connected HVAC equipment 408 communicate with the outside network 404 (e.g., a cellular network, a WAN, the Internet, etc.). However, in other embodiments most (e.g. more than 75%) of the smart connected HVAC equipment 408 may communicate with the outside network 404. Data may be exchanged between smart connected HVAC equipment 408 and then transmitted to the outside network 404 by a subset of smart connected HVAC equipment 408. The types of data transmitted by smart connected HVAC equipment 408 may include, for example, measurements recorded by sensors integrated with smart connected HVAC equipment 408, device status information, diagnostic information, configuration information, device identity information, a software version, a hardware version, or any other information related to smart connected HVAC equipment 408 or the operation thereof. In order for the data to be consumed by the various software applications, a contextual protocol (e.g., RESTful API, CoAP, HTTP, AMQP, MQTT) may be used to provide contextual information on the data. An API may be used to share data with the external world using a clean abstraction.

[0050] Still referring to FIG. 4, system 400 is shown to include a communications gateway 406 and a network 404. Gateway 406 may be used to connect legacy and new equipment (e.g., temperature sensors, actuators, cooling or heating devices, industrial robots, personal health monitoring devices, etc.), to get the data from them, and in return to control them based on the instructions or analytical results from the remote services. Gateway 406 may provide network security, access control, and unique address of legacy devices' endpoints for remote access and protocol mediation services. In some embodiments, gateway 406 is a general-purpose gateway solution made by any of a variety of hardware manufacturers (e.g.,

Intel, FreeScale, Dell, Texas Instruments, etc.). In other embodiments, gateway 406 is a network control engine (NCE) mobile access portal (MAP) gateway used specifically to connect building automation systems and smart equipment. Gateway 406 may use various Internet-based protocols (e.g., CoAP, XMPP, AMQP, MQTT, etc.) and web-based common data exchange (e.g., HTTP RESTful APIs) to translate communications from a building automation system protocol to an Internet protocol.

[0051] Network 404 may include the Internet and/or other types of data networks, such as a local area network (LAN), a wide area network (WAN), a cellular network, a satellite network, a radio network, or any other type of data network or combination thereof. Network 404 may include any number of computing devices (e.g., computers, servers, routers, network switches, etc.) configured to transmit, receive, or relay data. Network 404 may further include any number of hardwired and/or wireless connections. For example, smart connected HVAC equipment 408 may communicate wirelessly (e.g., using a Wi-Fi³³ or cellular radio, etc.) with a transceiver that is hardwired (e.g., via a fiber optic cable, a CAT5 cable, etc.) to a computing device of network 404.

[0052] Network 404 may include services that facilitate managing the fixed or wireless communication with smart connected HVAC equipment 408. Network vendors may include, for example, cellular telecommunications providers (e.g., Verizon, T-Mobile, AT&T, etc.) as well as internet service providers. Communications via network 404 may leverage enterprise contracts and partnerships to optimize the cost of data transmission. Many network carriers provide a secure connection option as a part of premium services. However, a similar degree of network securities can be achieved via employing trust platform chip in smart connected HVAC equipment 408 and using encrypted messaging such as AMQP via an Internet-based secure transport.

[0053] Still referring to FIG. 4, system 400 is shown to include a monitoring and service provider recommendation (MSPR) platform 402. MSPR platform 402 may operate as a remote system that receives and processes data provided by smart connected HVAC equipment 408 from many different buildings. MSPR platform 402 may leverage the data provided by smart connected HVAC equipment 408 to provide a variety of services. Services provided by MSPR platform 402 may include, for example, device management,

data routing and real-time analytics, data management services, and batch analytics. Additionally, MSPR platform 402 may include monitoring and reporting applications, connected chiller applications, fault detection and diagnostics (FDD) applications, data analytics, and automated service provider recommendations. For example, a connected chiller (i.e., a type of smart connected HVAC equipment 408) may communicate with MSPR platform 402. The connected chiller application may integrate industry-leading remote monitoring and analysis tools with planned service agreements and warranties. This allows MSPR platform 402 to provide enhanced responsiveness and expertise to one of the most critical pieces of equipment in the facility.

[0054] Referring now to FIG. 5, MSPR platform 402 is shown as a central system that connects smart connected devices 504 (e.g., HVAC equipment and/or any other devices, smart connected HVAC equipment 408), buildings 506, people 502, and businesses 508. For example, smart connected devices 504 may provide their current status, analytics results, fault detections, measurements, identity information, equipment models that represent smart connected devices 504, and/or other information associated with smart connected devices 504 to MSPR platform 402. MSPR platform 402 may perform analytics on the data provided by smart connected devices 504. Analytics may be used to facilitate the various services provided by MSPR platform 402. For example, MSPR platform 402 may build statistical models that use data from smart connected devices 504 to infer patterns, perform comparisons, perform trend analyses and predictions, or even teach smart connected devices 504 to correct themselves (e.g., by providing adjusted operating parameters to smart connected devices 504).

[0055] MSPR platform 402 may use the data from smart connected devices 504 to determine how smart connected devices 504 are being used, to broaden the value proposition beyond the physical equipment, to include valuable data and value-added services, and to form closer relationships with customers. MSPR platform 402 may create usage reports for sales, marketing and product development to improve quality and create better pricing and product positioning. MSPR platform 402 may provide the usage reports to various people 502 (e.g., a building owner, a facility manager, etc.) to provide insight into how smart connected devices 504 are being used. In some embodiments, MSPR platform 402 augments

data from smart connected devices 504 with external data (e.g., weather data, utility data, meter data, building occupancy, etc.) to provide extra information for better decision making.

[0056] The benefits provided by MSPR platform 402 include increased uptime for smart connected HVAC equipment 408, reduced future repair costs, extended asset life, using service experts with operational and trend data to assist in troubleshooting, and higher service renewal. MSPR platform 402 may be configured to implement a condition-based maintenance program to shorten the time to repair via remote diagnostics and optimized logistics in parts ordering and tool rentals. Potential outcomes of the services provided by MSPR platform 402 include a decreased number of unplanned repairs, optimized routine maintenance intervals, and reduced routine maintenance.

[0057] Referring now to FIG. 6, a smart connected device 602 may be connected to a building infrastructure 606, an owner 608, MSPR platform 402, a manufacturer 610, a facility manager 612, a contractor 614, and/or other smart connected devices and controllers 604. Smart connected device 602 may transmit its current status, analytics results, fault detections, measurements, its identity, an equipment model that represents smart connected device 602, and/or other information to the various entities with which smart connected device 602 is connected. For example, a smart connected rooftop may interact with an owner 608, an occupant, an OEM, and a contractor directly. A rooftop failure or failure symptom may be sent to MSPR platform 402 to orchestrate replacement or initiate a maintenance project. MSPR platform 402 may send alerts and a list of local service providers to the building owner 608. Thereby, certified contractors 614 who subscribe to MSPR platform 402 may have a higher chance to win the service contract. The service provider recommendation features of MSPR platform 402 are described in greater detail below.

Automated Monitoring and Diagnostics to Improve Products and Services

[0058] MSPR platform 402 may use the data provided by smart connected HVAC equipment 408 to develop improved products and/or services. Developing improved products and services may include improving existing products and services as well as developing new products and services. For example, MSPR platform 402 may determine how to improve the operation of smart connected HVAC equipment 408 (e.g., optimizing energy consumption in a building, maintaining uptime of the equipment, etc.). MSPR

platform 402 may use the remote diagnostics and repair to reduce downtime and unscheduled maintenance. In some embodiments, MSPR platform 402 creates a continuous feedback loop of how the customer uses smart connected HVAC equipment 408 to inform design, engineering and manufacturing decisions, to make the equipment better. MSPR platform 402 may also send automatic software updates to smart connected HVAC equipment 408 to add features and improve the performance of the equipment without any physical intervention.

[0059] In some embodiments, MSPR platform 402 uses the data provided by smart connected HVAC equipment 408 to help customers operate the equipment better and to enable service technicians to service the equipment better. The connectivity provided by smart connected HVAC equipment 408 allows MSPR platform 402 to monitor the equipment for critical alarms and notify service technicians if any issues arise. As the amount of collected data increases, the analytics model used by MSPR platform 402 continues to learn and improve over time. The analytics model may use the information from smart connected HVAC equipment 408 to identify opportunities for creating new physical products or even new information products. For example, MSPR platform 402 may identify opportunities to combine the functionality of two or more existing products (e.g., a video camera within a LED light bulb) to develop a new and improved product. The new and improved products may include, for example, a sensor or controller that can perform diagnostics and self-troubleshooting and/or other types of functionality that may eliminate the need for other products.

[0060] Advantageously, the connectivity provided by smart connected HVAC equipment 408 may facilitate a ubiquitous connection of various types of equipment within a building. Machine learning provided by MSPR platform 402 may use information provided by smart connected HVAC equipment 408 to develop a comprehensive view of controls in the building environment. In some embodiments, MSPR platform 402 provides building operators with a visually clean and intuitive view of the building operations and the ability to resolve issues in real-time. As more information is gathered regarding the patterns of how the building works, and under what circumstances and parameters, this information can be used by people outside of the manufacturing and building industry to improve products and services that affect the building.

[0061] MSPR platform 402 may allow vendors of HVAC equipment 408 and related services to sell more of their products and services. For example, MSPR platform 402 may generate usage information that can be used to develop a better understanding of the lifecycle and usage of the HVAC equipment 408. This information may also enable service providers to sell more services proactively. For example, MSPR platform 402 may use the lifecycle information for a particular type of HVAC equipment 408 to determine when that HVAC equipment 408 is expected to require maintenance or replacement. MSPR platform 402 may then recommend preventative maintenance and/or replacement before a failure occurs. Such information may also allow an equipment vendor to optimize sales channels to sell more equipment and parts.

[0062] MSPR platform 402 may reduce service operational costs and increase efficiency. For example, advanced diagnostics and remote monitoring capabilities provided by MSPR platform 402 may reduce the time required for a service technician to troubleshoot an issue. This may reduce the time spent performing service calls and may improve productivity.

[0063] MSPR platform 402 may enhance the value of installed equipment. For example, MSPR platform 402 can analyze the usage information from smart connected HVAC equipment 408 to provide insights to customers and optimize the performance of the HVAC equipment 408. A building owner or operator can interact with MSPR platform 402 (e.g., via a monitoring and control interface) to obtain current status information, control parameters, diagnostic information, and other types of information related to the installed equipment (e.g., equipment manuals, warranty information, etc.). The control functionality provided by MSPR platform 402 may make controls seamless and transparent to building owners and operators.

[0064] MSPR platform 402 may create more value for customers with minimal physical contact with smart connected HVAC equipment 408. For example, MSPR platform 402 may automatically send updates to smart connected HVAC equipment 408 to enhance features and fix bugs. Analytics provided by MSPR platform 402 may provide customers with information (e.g., via an interface of a mobile device) to act upon on potential failures in their equipment or building.

[0065] MSPR platform 402 may allow an equipment/service vendor to increase its customer base with better differentiated products and services. For example, MSPR platform 402 can recommend specific types of equipment and/or services that would provide value to a customer based on the usage information gathered from the customer's equipment. Additionally, MSPR platform 402 as a whole can be provided as a service to new and existing customers.

[0066] MSPR platform 402 may create new business models and opportunities. For example, MSPR platform 402 may allow a contractor to increase the number of service contracts and margins. The usage information from smart connected HVAC equipment 408 can also be provided to an insurance provider. The insurance provider may use the usage information to determine an appropriate risk level for a building, which allows the insurance provider to set more accurate insurance premiums. The proactive repair and replacement suggestions provided by MSPR platform 402 may decrease the number of failures (e.g., by repairing or replacing equipment before failures occur), which reduces insurance claims and improves the margins of an insurance contract.

[0067] Referring now to FIG. 7, a process 700 for implementing MSPR platform 402 is shown, according to an exemplary embodiment. Process 700 is shown to include three stages: connected equipment 702, connected buildings 704, and connected business 706. Each of these stages can be implemented by making changes to sensors, data collection, and a business model. Changes to sensors may include changes made to physical devices and equipment. Each device or manufactured part becomes a sensor of the environment that they are actuating. Changes to data collection may include changes in the systematic collection, management, and analysis of the data that collected from the sensors (i.e., smart connected HVAC equipment 408). Changes to the business model may include changes that can be made to monetize the features provided by MSPR platform 402.

[0068] In connected equipment stage 702, ubiquitous connectivity of smart connected HVAC equipment 408 in a building may be provided. MSPR platform 402 may use data analytics to analyze information provided by smart connected HVAC equipment 408. Such data analytics may include, for example, modeling, graphing, and scaling out the information

provided by smart connected HVAC equipment 408. Data analytics may further include real-time data analytics and machine learning.

[0069] Changes to the business model may include improving existing businesses (e.g., making them more efficient) and improving existing products. MSPR platform 402 may offer data analytics products as a service (e.g., with monthly billing) to allow building operators to get a clean and holistic view of the data associated with their buildings from mobile devices. Service technicians may also access the clean and holistic view of the data associated with a building to easily diagnose and repair problems more efficiently. Existing products can be offered as a service rather than product ownership. For example, a building owner or operator may subscribe to MSPR platform 402 (e.g., paying a monthly subscription fee), which provides access to the information provided by MSPR platform 402 including alerts when service and/or repair is recommended. Usage data from smart connected HVAC equipment 408 may be used to improve manufacturing reactively by detecting and fixing problems with equipment parts.

[0070] In connected buildings stage 704, information from smart connected HVAC equipment 408 can be aggregated across buildings to improve the capabilities and efficiency of smart connected HVAC equipment 408 (e.g., improving the autonomous control decisions made by the HVAC equipment 408). MSPR platform 402 may develop richer and more flexible models to integrate data from different buildings (e.g., richer schema). MSPR platform 402 may also develop richer analytical models (e.g., graph and probabilistic models) to deal with data heterogeneity and the added complexity of modeling across buildings (e.g., using other data to add context such as local/national laws and environmental/weather related operational considerations).

[0071] Changes to the business model may include expanding the services from connected equipment stage 702. Predictive analytics may be used to forecast a future electricity bill for the building based on historical data for other buildings in the region). A manufacturer, distributor, or service provider can use the information provided by MSPR platform 402 to guarantee equipment uptime (e.g., 95% uptime) or indoor temperature. MSPR platform 402 may monetize such information by charging monthly/annual service fees or by taking percentage of the cost savings.

[0072] Changes to the business model may further include changing the customer relationships and the value chain. For example, customer relationships may change from one-off purchases and services to more of a continuous consultative sales relationship, thereby increasing the lifetime value of a customer. MSPR platform 402 may establish direct relationships with customers (e.g., building owners) by providing customers with access to the monitoring information and service provider recommendations generated by MSPR platform 402.

[0073] In connected business stage 706, smart connected HVAC equipment 408 may be augmented with its own computing power and control capabilities. New features may be added to the data analytics, monitoring, reporting, and service provider recommendations generated by MSPR platform 402.

[0074] Changes to the business model may use data as a form of currency. For example, the data gathered from smart connected HVAC equipment 408 can be monetized in HVAC-related products, services, and markets (e.g., by selling more equipment, repair services, etc.), as well as in other industries. MSPR platform 402 may aggregate relevant data and models for the components, equipment and people across multiple different buildings. The data can be segmented by different regions, building types, age, size, and other factors. In some embodiments, MSPR platform 402 provides the data to insurance companies, which may use the data to refine their actuarial model and create pricing that's based on true usage and occupants behaviors. MSPR platform 402 may also provide insurance companies with data from water leakage detection sensors integrated with some types of smart connected HVAC equipment 408 (e.g., connected rooftop units) to provide an early warning of potential water damage.

[0075] In some embodiments, MSPR platform 402 provides the data to utilities, which may use the data to understand the energy usage profiles of the buildings and help them better manage the grid and the infrastructure that they need to build. In some embodiments, MSPR platform 402 provides the data to governmental agencies (e.g., city, state, national, etc.), which may use the data for better planning and allocation of resources. In some embodiments, MSPR platform 402 provides the data to energy storage companies, which may use the data to estimate the amount of energy generated by the buildings. MSPR

platform 402 may help building owners to optimize equipment performance and connect them with the contractors to fix problems.

Manufacturer-Centric Customer Relationships

[0076] Referring now to FIG. 8, a block diagram 800 illustrating a traditional customer relationship in the HVAC industry is shown. In the traditional customer relationship, an equipment manufacturer 802 provides HVAC equipment to a distributor 804. Distributor 804 receives purchase orders from a contractor 806 (e.g., a reseller or service provider) and provides the HVAC equipment to contractor 806. Contractor 806 then installs the HVAC equipment in the building of an owner or end user 808. Manufacturer 802 interacts only with distributor 804 and has no contact with building owner or end user 808 of the HVAC equipment. Once the HVAC equipment is installed, owner or end user 808 interacts only with contractor 806 if the HVAC equipment requires service or replacement.

[0077] Referring now to FIG. 9, a block diagram 900 illustrating a manufacturer-centric customer relationship made possible by MSPR platform 402 is shown. In the manufacturer-centric customer relationship, manufacturer 802 uses MSPR platform 402 to interact directly with distributor 804, contractor 806, and building owner or end user 808. Smart connected HVAC equipment 408 within the building of owner or end user 808 communicates with MSPR platform 402, which may be owned or operated by manufacturer 802. For example, smart connected HVAC equipment 408 may transmit its current status, analytics results, fault detections, measurements, its identity, an equipment model that represents smart connected HVAC equipment 408, a software version, a hardware version, and/or other information to MSPR platform 402. MSPR platform 402 may use the data from smart connected HVAC equipment 408 to automatically detect and diagnose faults and to determine appropriate replacement or repair actions for smart connected HVAC equipment 408. MSPR platform 402 may send alerts and a list of local contractors 806 (e.g., service providers) to the building owner 808. The building owner 808 may then select one of contractors 806 to service the HVAC equipment.

[0078] The manufacturer-centric customer relationship represents a fundamental shift in managing customer relationships in the HVAC industry. This relationship change may result in weaker dependency on distributors 804 and contractors 806. Manufacturer 802 now has

the opportunity to capture more profits from the overall value chain. Furthermore, manufacturer 802 can use the data received from smart connected HVAC equipment 408 to learn how its products and features are being accessed and utilized.

[0079] A detected fault represents repair or replacement opportunity for smart connected HVAC equipment 408, which becomes revenue for contractor 806 and a part sale opportunity for distributor 804. MSPR platform 402 may present these opportunities to both contractor 806 and distributor 804 to capture business in almost real-time. Given an informed fault (e.g., a fault accompanied by diagnostic information), contractor 806 may prepare a service cost estimate based on service part availability and diagnostic results. Contractor 806 may submit a bid to MSPR platform 402, which provides the bid, along with bids from other contractors, to building owner 808. Building owner 808 can select a contractor 806 based on the bid information and service proposals. Once a contractor 806 is selected, MSPR platform 402 may inform the selected contractor 806 that it has won the service contract.

Access to Smart Connected HVAC Devices

[0080] Referring now to FIG. 10, a block diagram 1000 illustrating the types of information provided between a smart connected device 1002, a building owner 1006, MSPR platform 402, and a contractor 1004 is shown, according to an exemplary embodiment. When smart connected device 1002 is installed, building owner 1006 may register smart connected device 1002 with MSPR platform 402. In some embodiments, smart connected device 1002 is provisioned in such a way that only building owner 1006 (and possibly MSPR platform 402) has access to smart connected device 1002. Smart connected device 1002 sends device information (e.g., status, identity, diagnostic results, measurements, etc.) to MSPR platform 402.

[0081] When a repair or replacement opportunity is identified by MSPR platform 402, MSPR platform 402 may provide temporary access credentials to contractor 1004. Contractor 1004 may use the temporary access credentials to access smart connected device 1002 and obtain detailed status and diagnostic information from smart connected device 1002. The temporary access credentials may expire after a defined time period or upon completion of a defined action (e.g., completing service on the smart connected device 1002).

which prevents contractor 1004 from accessing smart connected device 1002 once the service contract is complete.

Internet of Things Framework

[0082] Referring now to FIG. 11, a block diagram illustrating the components of an ecosystem 1100 in which MSPR platform 402 may be implemented is shown, according to an exemplary embodiment. Ecosystem 1100 is shown to include an Internet of Things (IoT) platform 1140, which may be the same or similar to MSPR platform 402 previously described. Ecosystem 1100 may allow IoT platform 1140 to facilitate self-conscious buildings that include smart connected equipment and/or devices (e.g., smart connected HVAC equipment 408, etc.). Many different types of partnerships may be used to facilitate self-conscious buildings. Examples of such partnerships include regional partnerships, global partnerships, channel partnerships, industry organization, and technology partners. In FIG. 11, each vertical column 1102-1118 represents technology components that could be installed in the self-conscious building, provided by IoT platform 1140, or purchased from or co-developed with a vendor or partner.

[0083] IoT platform 1140 of ecosystem 1100 may include a network of physical objects or “things” embedded with electronics, software, sensors, and/or network connectivity that enable such objects to collect and exchange data. The IoT platform 1140 may facilitate linking the physical and digital world by allowing remote sensing and control of devices across new and/or previously existing communication infrastructure. The IoT platform 1140 represents components and technologies that may enable delivering an end-to-end solution for IoT enabled products and services. The IoT platform 1140 also can include various processes and applications, which may further be utilized in creating and maintaining an IoT ecosystem 1100.

[0084] The IoT platform 1140 is shown to include vertical columns (e.g. technology concepts) such as smart connected devices 1102, a smart gateway 1104, network services 1106, device management 1108, data routing and real-time data analytics, data service platform 1112, analytics 1114, delivery 1116 and business/operation support 1118. Each of these technology components will be described in more detail below.

[0085] The smart connected devices 1102 can include one or more devices within a BMS, and particularly “smart devices” such as the smart HVAC equipment 408, described above. As shown in FIG. 11, the smart devices can include sensors 1120, actuators 1122, smart equipment 1124, smart buildings 1126, and the like. According to one embodiment, a smart connected device 1102 includes any device which has communication capabilities, computing power, and that is capable of making decisions at a local level (e.g., in a limited context, etc.). Communication with the smart connected devices 1102 may be through any wireless or wired communication protocol. The computing power may be enabled by a microprocessor with an embedded operating system (e.g., Linux, Android, iOS, RTOS, Windows 10, etc.). The computing power may be used locally to store data from the device (e.g., temporarily, etc.) and/or execute pre-determined operations (e.g., decision trees, etc.). The pre-determined operations may include isolated fault detection, device diagnostics, and/or other operations. The smart devices may additionally have fault response capabilities to allow the smart devices to be adaptive and responsive to changing environmental and/or operational conditions (e.g., weather, loading, etc.). In some embodiments, the ecosystem 1100 includes devices that are not smart connected devices 1102, but may be connected to the IoT platform 1140 via device or field gateways used as a proxy to facilitate communication between the non-smart devices and the IoT platform 1140 over public and/or private networks (e.g., using fully secure defensible server platforms with high capability hardware, etc.). Such connection is described more fully herein.

[0086] Smart connected devices 1102 may further include actuators, dampers, chillers, heaters, rooftop units (RTU), air handling units (AHU), and/or any other type of equipment or device that can be installed within a building (e.g., fans, pumps, valves, etc.). Although the present invention is described primarily with reference to HVAC equipment, it should be understood that the systems and methods described herein may be applicable to a wide variety of building equipment and other types of connected devices (e.g., HVAC equipment, LED lights, mobile phones, tablets, computers, elevators, fire safety systems, smart street lamps, cars, televisions, security systems, refrigerators, music systems, printers, washing machines, dish washers, coffee makers, etc.) with embedded intelligence and communication capabilities.

[0087] Ecosystem 1100 is shown to include smart gateway 1104 technical component. The smart gateway technical component may include smart gateway 1128. The gateway 1128 may be used to connect legacy and new equipment (e.g., temperature sensors, actuators, cooling or heating devices, industrial robots, personal health monitoring devices, etc.) to get the data from them, and in return to control them based on the instructions or analytical results from the remote services. The gateway 1128 may provide network security, access control, and unique addresses of legacy devices' endpoints for remote access and protocol mediation services. In some embodiments, the gateway 1128 is a general-purpose gateway solution made by any of a variety of hardware manufacturers (e.g., Intel, FreeScale, Dell, Texas Instruments, etc.). In other embodiments, gateway 1128 is a NCE or MAP gateway used specifically to connect building automation systems and smart equipment. The gateway 1128 may use various Internet-based protocols (e.g., CoAP, XMPP, AMQP, MQTT, etc.) and web based common data exchange (e.g., HTTP RESTful APIs) to translate communications from a building automation system protocol to an Internet protocol. For example, the gateway 1128 may provide protocol conversions that make legacy non-IP enabled devices able to be accessed through modern web/IP protocols (e.g., converting BACnet Serial to CoAP, MQTT, or AMQP).

[0088] The gateway 1128 may include a soft component and/or a physical device with embedded components that performs various functions. For example, the gateway 1128 may optimize the cost of communication between a connected device (e.g., smart device, smart connected devices 1102, non-smart connected things, etc.) and the rest of the digital world. In another example, the gateway 1128 may identify resources contained in the connected devices. In yet another example, the gateway 1128 may perform semantic mediation of data being received from the connected devices (e.g., naming translation of data obtained from devices for global consumption in a standardized manner, etc.).

[0089] In one embodiment, the gateway 1128 allows one or more smart connected devices 1102 to make outbound connections to a public or private cloud-based server, which is used for further storage and processing by components of ecosystem 1100. Inbound connections may not be typically allowed for cybersecurity considerations; however, in some instances, secured and controlled inbound messaging is used to drive actions at the device level that may be facilitated by the IoT platform 1140. In one example, the gateway 1128 may leverage

an organization's internal technology infrastructure and/or a public telemetry infrastructure to provide a secure and controlled inbound messaging scheme. In a further embodiment, the gateway 1128 is configured to provide protocol conversion services, network address translation services, containers for messages, applications to understand different protocols such as Bluetooth, ZigBee, Z-wave, BACNet, etc., and/or any other user installed application.

[0090] In one embodiment, the gateway 1128 includes a number of field gateway aspects that primarily interface with devices and cloud-based servers. The field gateway aspects can enable the gateway 1128 to perform high scale telemetry ingestion, device identification, device management, and cloud-to-device commanding (e.g., when allowed). For example, in a home, several smart devices like a security system, a television, a refrigerator, a music system, a printer, a computer, a washing machine, a dish-washer, a coffee maker, a garage door, etc. may have elements of field gateways built into them and you could use a singular home automation device to act as the cloud gateway. In another example, in a manufacturing or process plant, individual production line machines may have field gateways built into them and connect via some common cloud gateway organized by production lines, processes, and/or zones. In still another example, in an office building having an HVAC system (e.g., smart connected HVAC equipment 408, etc.), there may be dozens of devices and hundreds of sensors with smart field gateway capabilities connected through a common cloud gateway.

[0091] The network service 1106 may include the Internet and/or other types of data networks, such as a local area network (LAN), a wide area network (WAN), an Internet area network (IAN), a home area network (HAN), a body area network (BAN), a cellular network, a satellite network, a radio network, or any other type of data network or combination thereof. Network service 1106 is shown to include a firewall/proxy 1130, one or more transport protocols 1132 (e.g., WLAN/LAN, ZigBee, Wired/Wireless, PAN/BAN/Power Line, BTLE, HAN), one or more protocol handlers 1134, a message handler 1136, and a message cache 1138. The protocol handlers 1134 may facilitate the translation of data received over the multiple communication protocols into a uniform, understandable, and/or useable format. The message handlers 1136 may facilitate the transportation of messages (e.g., between the smart connected devices 1102 and a cloud, etc.). The message cache 1138 may enable increased speed in the retrieval of data. The firewall/proxy 1130 may be configured to drive security and privacy policies.

[0092] The network service 1106 may include any number of computing devices (e.g., computers, servers, routers, network switches, etc.) configured to transmit, receive, or relay data (e.g., from smart connected devices 1102 to a public or private cloud-based server, etc.). Network service 1106 may further include any number of hardwired and/or wireless connections. For example, smart connected HVAC equipment 408 and/or smart connected devices 1102 may communicate wirelessly (e.g., using a Wi-Fi, Bluetooth, EnOcean, near field communication (NFC), LoRA, ZigBee, cellular radio, etc.) with a transceiver that is hardwired (e.g., via a fiber optic cable, a CAT5 cable, etc.) to a computing device of network service 1106. Network service 1106 may include services that facilitate managing the wired and/or wireless communication with smart connected HVAC equipment 408 and/or smart connected devices 1102. Network vendors may include, for example, cellular telecommunications providers (e.g., Verizon, T-Mobile, AT&T, etc.), as well as internet service providers. Communications via network service 1106 may leverage enterprise contracts and partnerships to optimize the cost of data transmission. Many network carriers provide a secure connection option as a part of premium services. However, a similar degree of network securities can be achieved via employing trust platform chip in smart connected HVAC equipment 408 and/or smart connected devices 1102 and using encrypted messaging such as AMQP via an Internet-based secure transport.

[0093] Referring to FIG. 12, a device (e.g., smart connected devices 1102, smart connected HVAC equipment 408, etc.) to cloud connectivity landscape 1200 is shown according to one embodiment. According to some embodiments, the device to cloud connectivity landscape 1200 leverages devices, gateways, and network services to connect the devices to a cloud. As shown in FIG. 12, the device to cloud connectivity landscape 1200 includes a plurality of special purpose devices, shown as special purpose devices 1202. The special purpose devices 1202 may include sensors, valves, servos, switches, etc. The special purpose devices 1202 may be communicably coupled to one or more smart devices, shown as smart devices 1204. The smart devices 1204 may include a processor with an embedded operating system (e.g., Linux, Android, iOS, RTOS, Windows 10, etc.). The special purpose devices 1202 may communicate with the smart devices 1204 via wired and/or wireless communications protocols (e.g., Wi-Fi, Bluetooth, NFC, ZigBee, etc.). In some embodiments, the smart devices 1204 are included within the special purpose devices 1202.

[0094] The smart devices 1204 may be communicably coupled to a network device (e.g., NAT, firewall, router, etc.), shown as network device 1206. The network device 1206 may communicate with the smart devices 1204 via wired and/or wireless communications protocols (e.g., Wi-Fi, Bluetooth, NFC, ZigBee, cellular, etc.). According to one embodiment, the special purpose devices 1202, the smart devices 1204, and the network device 1206 form an internal network. In some embodiments, the connections between the smart devices 1204 and the network device 1206 are initiated and transmitted by the smart devices 1204. In some embodiments, the network device 1206 is capable of initiating a connection with the smart devices 1204 to provide a command and/or update (e.g., from a remote server, a cloud, etc.). The network device 1206 may be communicably coupled to gateway, shown as field gateway 1208. In one embodiment, the field gateway 1208 may have a public IP address, but be a fully secured and well defensible server platform. In other embodiments, the field gateway 1208 may have a private IP address. The field gateway 1208 may be communicably coupled to a cloud-based server, such as cloud-based server 1210. The cloud-based server 1210 may monitor the special purpose devices 1202 and/or the smart devices 1204. In some embodiments, the cloud-based server 1210 is used to send updates and/or commands to the special purpose devices 1202 and/or smart devices 1204.

[0095] Referring back to FIG. 11, the device management technology concept 1108 is shown to include a device identity and access management module 1142, and a device management module 1144. According to one exemplary embodiment, managing the smart connected devices 1102 through the device management technology concept 1108 of the IoT platform 1140 includes four aspects from an identity and access management view point including (i) device provisioning, (ii) device registration, (iii) telemetry ingestion, and (iv) command and control. Device provisioning may include setting up a device to establish a secure, trusted relationship with the digital world. The device management technology concept 1108 may generate a secure key to be assigned to a respective device such that the device is able to interact with the rest of the IoT platform 1140. Regarding device registration, the device management technology concept 1108 may register each device and maintain a list of provisioned devices and associated metadata. Device registration is described in more detail below. Regarding telemetry ingestion, the device management technology concept 1108 may provide a simple, secure path for receiving data from the

connected devices. Regarding command and control, the device management technology concept 1108 may provide functionality for securely sending data to a device (e.g., using existing outbound connections, etc.).

[0096] Device management technology concept 1108 may also facilitate complete lifecycle management of a device. In some embodiments, the device management technology concept 1108 facilitates tracking a device from manufacture to install. In some embodiments, the device management technology concept 1108 facilitates distributing and licensing device contained software including remote updates for new features, security, and other maintenance type activities. In some embodiments, the device management technology concept 1108 facilitates monitoring the recovery and decommissioning of non-usable devices post useful life. In some embodiments, the device management technology concept 1108 facilitates monitoring the health of a device. In some embodiments, the device management technology concept 1108 facilitates monitoring customer usage patterns, release levels, and maintenance protocols to extract additional business value. The device management technology concept 1108 may provide secure end-to-end connectivity, easy integration into embedded products, simple registration workflow, easy diagnosis and remediation of connectivity problems, remote user access for operation (with the ability to override at LAN), fast and reliable software updates, time series data push, remote write-backs to device via automation, device location tracking, device time sync (with consideration to time zone and automated changes to time zone in events like day light savings), licensing of device and features within the device, rules engine/scheduling of device actions from the cloud, and application program interfaces (APIs) for extension of capabilities in devices and in the cloud.

[0097] Data routing and real-time data analytics technology concept 1110 may act as the backend distribution infrastructure of the IoT platform 1140. In one embodiment, the data routing and real-time data analytics technology concept 1110 may be a third party system, such as Kafka, Storm, Event Hub, etc. By way of example, distributed message routing module 1148 of data routing and real-time data analytics technology concept 1110 may be configured to send messages and data elements generated from devices to the correct data platform storage locations. The storage locations (or applications) may use listener applications to receive and process the messages. Distributed message routing 1148 may also

act as the front door for event ingestion, and sometimes as a bi-directional control action conduit to the devices or system from which the message events are received.

[0098] The complex event processing (CEP) module 1146 (e.g., hot path analytics, etc.) may be configured to identify meaningful events and facilitate responding to such events quickly. Anomalies or other patterns may trigger an event in the system such that the CEP module 1146 begins additional processing or implements additional control logic in response thereto. Referring now to FIG. 13, there are multiple steps involved in CEP, as shown by CEP mapping 1300. As shown by CEP mapping 1300, CEP includes multiple steps including event production 1302 (e.g., via applications, devices, sensors, web and social, etc.), collection of data 1304 (e.g., via cloud gateways, field gateways, etc.), queuing of events 1306 (e.g., via event hubs, Kafkam RabbitMQ, ActiveMQ, etc.), transformation of events 1308 (e.g., via stream processing, storage adapters, etc.), preparation for and actual long-term storage 1310, and multi-format presentation of the analyzed events 1312 (e.g., via dashboards, search and query, spreadsheet data analytics, on smart devices, etc.) for reporting and/or other further actions.

[0099] In traditional data management and enterprise systems, message routing and event processing types of activities are sequential and spaced by more elaborate classification, cleansing, storage, and analytical steps. Referring back to FIG. 11, the IoT platform 1140 of the present disclosure facilitates receiving simultaneous events or near simultaneous events, taking advantage of early insights from time series data to take immediate remedial actions. The distributed message routing module 1148 may be capable of processing millions of events per second in real-time and in different computing environments to meet the needs of real-time analysis. Distributed message routing 1148 may also involve ingestion, processing, and placing back millions of messages in a message distributor for multiple listener applications to pick up. In some embodiments, the distributed message routing module 1148 performs data transformation and validation.

[0100] The data service platform technology concept 1112 may be configured to manage a large quantity of structured, unstructured, and streaming data. A big data processing module 1150 may include a Hadoop distributed files system (HDFS) configured to execute distributed parallel storage using (i) name nodes to track the placement of physical data

across various Hadoop instances and (ii) data nodes that physically store the data. The HDFS may allow multiple computing devices (e.g., simple consumer grade computing devices, etc.) to be organized virtually to store large amounts of data. The big data processing module 1150 may also include a Map Reduce function for processing large volumes and transactions of data (e.g., structured, unstructured, and streaming). The Map Reduce function may use parallel distributed algorithms for orchestration of the clustering required for storage and processing of data.

[0101] The massive amounts of data may contain different values for different analytics and insights (e.g., data can have different meanings, etc.). This may require the abstraction of data into multiple meanings through a collection of keys and value pairs of the data, which may be achieved through associative arrays. The big data processing module 1150 may include a key-value store for managing such associative arrays through dictionaries and hash. Dictionaries may include a collection of objects and/or records, which have a plurality of different fields within them, each containing data. Such objects and/or records may be stored and retrieved using a key that uniquely identifies the object and/or record such that the key may be used to quickly locate the data within the database.

[0102] The big data processing module 1150 may additionally or alternatively include graph databases or graph stores that use graph structures for semantic queries with nodes (e.g., entities, etc.), properties (e.g., information about the entities, etc.), and edges (e.g., a connection between the nodes and properties, etc.) to store the data. The big data processing module 1150 may additionally or alternatively include Spark. According to some embodiments, Spark is an open source cluster computing framework built using multi-stage in-memory primitives. Spark may accelerate processing performance by order of magnitude and may be complementary to machine learning of the IoT platform 1140.

[0103] The data service platform technology concept 1112 may further include a relational database management system (RDBMS) 1152 may be useful for storing data associated with applications that have low latency data retrieval needs, as the RDBMS 1152 has a natural low latency. For example, consumer-end or front-end applications traditionally have low latency data retrieval needs. Thus, the data associated with such applications may be stored in the RDBMS 1152, rather than by big data processing module 1150. The data stored in the

RDBMS 1152 may be parsed, transformed, and/or enriched prior to storages in RDBMS 1152.

[0104] A data integration module 1154 facilitates connecting and collecting data (e.g., structured data, unstructured data, streaming data, etc.) from almost any type of device (e.g., smart connected devices 1102, smart connected HVAC equipment 408, etc.). The format of the collected data may vary greatly from device to device. The data integration module 1154 is configured to process the collected data such that the data is stored in a native state or substantially the native state of the data as collected (e.g., as the native state may be used and analyzed differently later, etc.). The data integration module 1154 may use asynchronous communication to collect the data (e.g., making the integration of the data simpler, etc.). Layers of abstraction may be used during any processing or further storage. The data integration module 1154 may additionally provide an ease of semantic mediation of the collected data (e.g., such that the IoT platform 1140 may use the data in a meaningful way, etc.). According to one embodiment, the data integration module 1154 includes a plurality of microservices that form the integration fabric. In some embodiments, the data integration module 1154 is independent of the other components of data service platform 1112.

[0105] Analytics technology concept 1114 may include a massively parallel data analytics module 1158. The massively parallel data analytics module 1158 may include multiple processors configured to run analytical processing. The massively parallel data analytics module 1158 may divide large data sets into smaller segments that are analyzed (e.g., operated on, etc.) by specifically assigned processors (e.g., with their own operating system and memory, etc.). Messaging interfaces may aggregate the results following the analysis by each processor. Such a system may allow for improvements in processing and flexible scalability.

[0106] The IoT platform 1140 increases the capabilities to collect real-time operational and/or performance data from devices and/or machines (e.g., a very frequent intervals, continuously, etc.). A time series analysis module 1164 within the analytics technology concept 1114 may be configured to receive large quantities of streaming time series data for analysis. The time series analysis module 1164 may analyze time series data over a time domain and/or a frequency domain. The time series analysis module 1164 may use such

analysis to forecast future events and/or identify trends. The time series analysis module 1164 may combine multiple parameters from the time series data and environmental and/or influence data for fault detection and diagnostics (FDD). The IoT platform 1140 may facilitate the use of automated FDD due to the vast availability of data capable of being received by, stored, and processed by the various components of the IoT platform 1140. FDD analysis may include rule based FDD analysis, model based FDD analysis, and/or case based FDD analysis, among other possibilities. Rules based FDD analysis may use boundary conditions of observed data to detect and isolate faults (e.g., using simple or complex if/then/else/hence logic blocks or structures, etc.). Model based FDD analysis may use different types of statistical models in a more applied analysis. Case based FDD analysis may use past situation-solution examples to adapt to new and/or similar situations such that new behaviors are learnt over time (e.g. adaptive learning, etc.) by modifying analytical parameters.

[0107] The analytics technology concept 1114 may further include a machine learning module 1166. The machine learning module 1166 may be configured to use data mining techniques and/or other learning algorithms to build models to interpret various data received from the various devices or components (e.g., smart devices, smart connected devices 1102, smart connected HVAC equipment 408, etc.) to detect, classify, and/or predict future outcomes. Such learning algorithms may be associated with rule learning, artificial neural networks, inductive logic programming, and/or clustering and Bayesian networks. The machine learning module 1166 may solve complex problems, predict scenarios not previously modeled, and/or develop new insights through the use of statistical methods to self-identify algorithms for analysis and association. The machine learning module 1166 may be executed either through custom programming and/or usage of standard or open source tools (e.g., such as SicKit, Spark's machine learning, etc.).

[0108] The analytics technology concept 1114 may further include an advanced data mining module 1162. The advanced data mining module 1162 may use statistical data analysis, as well as other algorithmic methods, to find patterns within data. The statistical data analysis may include statistical approaches involving regression analysis, neural networks, and/or decision trees. The advanced data mining module 1162 may apply certain techniques including association rules for initial data exploration, fuzzy data mining

approaches, rough set models, support vector machines, and genetic algorithms to solve special problems. The advanced data mining module 1162 may be used in a wide array of industries to solve number of complex issues and/or generate insights, which involves the interplay of multiple different types/classes of data that may not have obvious associations. The advanced data mining module 1162 may apply methodologies including Cross-Industry Standard Process for Data Mining (CRISP-DM) and/or Sample-Explore-Modify-Model-Assess (SEMMA). Such methodologies may be applied in an iterative cycle by advanced data mining 1162 to provide a better analysis.

[0109] The analytics technology concept 1114 may further include a business intelligence module 1160. The business intelligence module 1160 may be configured to enable the easy creation and access to dashboards and analytics across multiple data sources and types. Business intelligence module 1160 may be further configured to facilitate creating packages of content (e.g., data, analytics, etc.) for distribution to other users (e.g., in the same organization, in the same industry, visualization for the masses, etc.). Such distribution may allow others to conduct independent analytics on the content and/or create independent dashboards and/or reports. The content may be delivered through multiple channels including desktop, mobile, and/or web.

[0110] Referring still to FIG. 11, the ecosystem 1100 is shown to include a delivery technology concept 1116. The delivery technology concept 1116 is related to channel and distribution strategy and is shown to include a delivery applications module 1168, a data visualization module 1170, a product distribution module 1172, an application service API module 1174 and an integration to enterprise applications module 1176. The product distribution module 1172 may include off-line distribution of IoT related products, services, and on-line distribution of solutions for a certain customer and/or a market (e.g., delivery applications module 1168). The application service API module 1174 may be provided to app developers to deliver information products. The data visualization module 1170 and exploration tools may be used for rapid delivery. The delivery technology concept 1116 may include integration to one or more enterprise applications module 1176.

[0111] Ecosystem 1100 is shown to further include the business/operation support technology concept 1118. The business/operation support technology concept 1118 may

facilitate the integration and optimization of devices to unite interrelated applications. The business/operation support technology concept 1118 may provide capabilities for customer management, managing partners who are contributors to IoT platform 1140, managing commercial transactions, business reporting, and financial reporting. For example, if the IoT platform 1140 includes financial transaction services, then CRM, ERP and/or financial payment service integration may be used. The business/operation support technology concept 1118 may further include business applications such as a customer management applications module 1178 (e.g., CRM, etc.), a partner management applications module 1180, a billing module 1182, a reporting applications module 1184, and an ERP module 1186. The reporting application module 1184 may be configured to facilitate providing the data from IoT platform 1140 to outside businesses (e.g., insurance companies, utility providers, governmental agencies, etc.) that may have an interest in such data. The business/operation support technology concept 1118 may allow a manufacturer to leverage IoT enabled product related data such as install base information, operational performance data, maintenance history, etc. to attract new service providers (e.g., who may be intermediate customers, etc.).

[0112] The Ecosystem 1100 is further shown to include security, privacy, access control, and compliance management technology concept 1190. Multi-layered and multi-dimensional intrusion detection and prevention mechanisms may provide security at the device level, the data level, the network level, and/or the application level. The same intelligence that enables devices to perform their tasks may also enable them to recognize and counteract threats. This does not require an evolutionary approach, but rather an evolution of measures that have proven successful in IT networks, adapted to the challenges of IoT and to the constraints of connected devices. At any given point in time, IoT platform 1140 may support multiple users and stake holders including building owners, building operators, tenants, service technicians, manufacturers, and the like. Remote accessibility of connected products may involve complex identity management through a unified login and product management experience. For example, a single login may allow a customer to sign on to all connected products and services associated with IoT platform 1140.

[0113] The security, privacy, access control, and compliance management technology concept 1190 may provide encryption for data and connections at some or all stages. Each device and/or every data transaction associated with the IoT platform 1140 may have a

unique identity which may provide easy traceability and enable authentication. The security, privacy, access control, and compliance management technology concept 1190 may provide perimeter protection, intrusion detection, and/or response and audit trails (e.g., at real-time speed, etc.). The security, privacy, access control, and compliance management technology concept 1190 may be able to isolate any non-secure device and/or connection, and/or have a mechanism to accept such non-secure device and/or connection with calculated risks. The security, privacy, access control, and compliance management technology concept 1190 may have mechanisms to detect pattern anomalies in device connectivity, network traffic, and/or data communication (e.g., instant indicators of a possible intrusion, etc.). The security, privacy, access control, and compliance management technology concept 1190 may comply with various standards including, but not limited to, ISO/IEC 27001, NIST 800-82 v2, RFC2196, and/or ISA/IEC-62443.

[0114] There may be many different actors or personas involved with IoT platform 1140 with different data access needs including the devices and sensors themselves, manufacturers of such devices and sensors, installers, owners, users, maintainers, application service providers, technology platform providers, cloud hosting providers, etc. Security, privacy, access control, and compliance management technology concept 1190 may provide each of these actors with different action rights to the data (e.g., who has access to what data, what actions may one take with the data generated, etc.).

[0115] Referring now to FIG. 14, a data platform 1400 (e.g., for the IoT platform 1140, etc.) is shown according to one embodiment. As shown in FIG. 14, the data platform 1400 includes a device 1402 (e.g. an on-premises device, a smart connected device 1102, an HVAC equipment 408, etc.) communicably coupled to a device reverse proxy 1404 and a mobile/web reverse proxy 1408. The device reverse proxy 1404 and the mobile/web reverse proxy 1408 may further be communicably coupled to a mobile/web device 1406 (e.g., an off-premises device, etc.). Additionally, the device reverse proxy 1404 and the mobile/web reverse proxy 1408 also may be communicatively coupled, respectively, to one or more components and/or application program interfaces (APIs) of the data platform 1400. As shown in FIG. 14, the one or more components and/or APIs of the data platform 1400 include an identity management (IDM) component 1410, an IoT hub 1420, one or more message processors 1430 (e.g., status processor 1432, feedback processor 1434, device information

processor 1436, telemetry processor 1438), a security API 1440, an identity API 1450 and an application API 1460, a weather API 1470, a time series API 1474, an entity API 1478, a notification API 1484, and an email API 1488.

[0116] As an overview, data platform 1400 may be a collection of services which collect and serve up building objects and time series data. Points in the entity API 1478 may contain time series objects which include an ID and sample Url. The ID and sample Url in the time series object may be used to query time series API 1474. Parts of time series API 1474 may allow a user to query by space or system. In this case, the time series API 1474 may look up the corresponding time series objects in the entity API 1478. To use the time series API 1474 and/or the entity API 1478, an action token may need to be acquired (e.g., from the IDM component 1410) for authentication and authorization. Various HTTP verbs may be used with data platform 1400 to perform various actions including GET, POST, PUT, PATCH, and DELETE. GET may be used to read from an API. POST may be used to create an item or to execute an action. PUT may be used to update an item, or create an item if it does not exist. PATCH may be used to update specific properties of an item. DELETE may be used to delete a single item (or a cascading delete when deleting points, as associate time series may also be deleted).

[0117] As show in FIG. 14, the IDM component 1410 includes an identity management system (IMS) 1411, a client management system (CMS) 1412, a user management system (UMS) 1413, a token support module 1414 (e.g., for OpenID connect, etc.), an external user support module 1415 (e.g., Microsoft, Facebook, etc.), and a local user support module 1416 (e.g., registration, forgotten password, etc.). According to an exemplary embodiment, IMS 1411 is configured to implement an OpenID Connect protocol which is an identity layer on top of OAuth 2.0 protocol. The OpenID connect protocol allows clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and rest-like manner. The OpenID Connect protocol allows clients of all types, including Web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users. The specification suite is extensible, allowing participants to use optional features such as encryption of identity data, discovery of OpenID providers, and session management. OAuth 2.0 protocol focuses on client developer simplicity while providing specific

authorization flows for web applications, desktop applications, mobile phones, and living room devices. IMS 1411 may use IdentityServer3 (e.g., a .NET/Katana-based framework and hostable component) for implementing the protocol.

[0118] IMS 1411 may be configured to restrict web services to unauthorized users and applications. Such restriction may be based on a user's tokens. Tokens may represent a set of claims that may be used to restrict a client's permissions when using an IMS-secured endpoint (e.g., such as an HTTP API, etc.). Tokens may be requested from IMS 1411 by clients. Clients may send the tokens to any IMS-secured endpoint (e.g., using Bearer authorization in an HTTP Authorization header for HTTP-based APIs, etc.). The tokens may be good for a preset time duration (e.g., one hour, thirty minutes, two hours, etc.).

[0119] As show in FIG. 14, the security API 1440 includes user/role storage 1441, permission storage 1442, group storage 1443, client/scope storage 1444, token storage 1445, and device storage 1446. Security API 1440 may also communicate with the identity API 1450. The identity API 1450 can include a claim device module 1452, a get claimed devices module 1454, a command device 1456, and a get device information module 1458. The application API 1460 may include a check for updates module 1462 and a device registry backdoor module 1464. According to one embodiment, the security API 1440 is configured to manage users, roles, groups, devices, and/or relationships therebetween. In some embodiments, a PostgreSQL database is used for storing such data (e.g., in an on-premises scenario). In some embodiments, a variety of technologies are used including, but not limited to, Azure Active Directory, Azure IoT Hub, Azure DocumentDB, and/or Azure Tables (e.g., in a cloud scenario).

[0120] The user/role storage module 1441 may be configured to store data and/or information relating to users and/or roles. A user may effectively represent an individual identity usable in the data platform 1400. An example of information stored in the user/role storage module 1441 relating to a user is shown in Table 1. A role may effectively represent a collection of permissions for a user or a group. Each API in the data platform 1400 may have different interpretations for roles. An example of information stored in user/role storage 1441 relating to a role is shown in Table 2. Group storage 1443 may be configured to store data and/or information relating to a group. A group may effectively represent a collection of

users and/or devices in the data platform 1400. An example of information stored in the group storage 1443 relating to a group is shown in Table 3. Device storage 1446 may be configured to store data and/or information relating to a device. A device may facilitate interaction with the IoT Hub 1420 such that metadata and commands may be defined for a device. An example of information stored in the device storage 1446 relating to a device is shown in Table 4.

Table 1: Users

Property	Type	Description
Id	String	Friendly identifier. Identifies the username for locally authenticated users and a crafted representation of a username for externally authenticated users.
Subject	String	A consistent identifier that is usually a GUID. Useful when deleting and recreating an identical representation to distinguish between the previous one and the new one.
Username	String	A secondary Id property. Needed when updating Id.
Credentials	JSON Object	Contains properties related to the user's credentials such as an encrypted password and a cryptography algorithm.
Identity	JSON Object	Contains properties related to the user's identity such as name, phone, email, and extra information retrieved from external identity providers.
Meta	JSON Object	Contains properties related to the user's metadata such as verification status, failed attempts, and various dates.
Privilege	JSON Object	Contains properties related to the user's privilege such as roles and permissions.

Table 2: Roles

Property	Type	Description
Id	String	Friendly identifier. Identifies the name of the role.
Subject	String	A consistent identifier that is usually a GUID. Useful when deleting and recreating an identical representation to distinguish between the previous one and the new one.
Name	String	A secondary Id property. Needed when updating Id.
Description	String	Describes the purpose of the role.

Table 3: Groups

Property	Type	Description
Id	String	Friendly identifier. Identifies the name of the group.
Subject	String	A consistent identifier that is usually a GUID. This is useful when deleting and recreating an identical representation to distinguish between the previous one and the new one.
Name	String	A secondary Id property. Needed when updating Id.

Description	String	Describes the purpose of the group.
Members	JSON Object	Contains properties related to the group's members such as users and devices.
Privilege	JSON Object	Contains properties related to the group's privilege such as roles and permissions.

Table 4: Devices

Property	Type	Description
Id	String	Friendly identifier. Identifies the device name in IoT Hub.
PrimaryKey	Base64 String	Used to securely communicate to IoT Hub. If omitted on creation, the API will generate one.
SecondaryKey	Base64 String	Used when changing the PrimaryKey, but is not needed for general communication. If omitted, the API will generate one.
Properties	JSON Object	Used to store any metadata for the device.
Commands	JSON Array	Used to define supported commands for the device.
Telemetries	JSON Array	Used to show mapped telemetries for the device.
Status	JSON Object	Used to show the status for the device.

[0121] The weather API 1470 is configured to communicate with one or more external weather providers 1472 (e.g., Aeris Weather, etc.). Such communication may facilitate integrating weather information (e.g., current weather data, weather forecasts, historical data, based on location such as country, state, and/or zip code, etc.) into web and/or mobile applications. Weather API 1470 may automatically append the correct security credentials using the IMS token claims.

[0122] The entity API 1478 (e.g., having hierarchical navigation 1480) includes entities including organizations, spaces, systems, points, time series, and data sources. According to an exemplary embodiment, the entities are open types such that each supports dynamic properties. The entities have the properties shown in Table 5.

Table 5: Entities

property	type	description
id	string	Unique identifier. Limited to alphanumeric characters, "_", "-", "~", and ".". We recommend using GUIDs.
name	string	
description	string	
image	string	A base64 encoded image. This is validated by converting the base64 string to bytes and attempting to create a System.Drawing.Image. Supported formats: BMP, GIF, JPEG, PNG, TIFF.
entityTemplate	EntityTemplate	Optional. The entityTemplate describes an entity type. When

		omitted, the entity is “generic”. The entityTemplate describes the expected dynamic properties and related entities. Entity templates replace the deprecated systemType, spaceType, and pointRole properties.
entityTemplateId		This property is provided for convenience so you do not need to expand the entityTemplate to find the id.
<i>DynamicProperties</i>		Everything derived from Entity is an open type, meaning it supports dynamic properties.
createdDateUtc	DateTime	The date and time this entity was created.
modifiedDateUtc	DateTime	The date and time this entity was modified.

[0123] An entity can have an associated entity template. The entity template indicates the “type” of the entity and may have additional metadata as well. Entity templates may have all of the properties of the entities (see Table 5), as well as the properties shown in Tables 6–8.

Table 6: Entity Templates

property	type	description
baseEntity	string	Point, System, Space, or Organization
properties	Collection(Jci.Be.Data.PropertyMetadata)	See Table 7
relationships	Collection(Jci.Be.Data.RelationshipMetadata)	See Table 8

Table 7: Property Metadata

property	type	description
name	string	The name of the dynamic property.
description	string	An optional description.
odatatype	string	The OData type of the property value. The default odatatype is String. The primitive types are: Byte, Short (Int16), Integer (Int32), Long (Int64), Double, Decimal, Boolean, Date, Char, String. For properties that represent a collection of values, the odatatype is the element type enclosed in parentheses and prefixed with "Collection". For example: “Collection(String)”
required	boolean	If true, the application should require this property to be populated.

Table 8: Relationship Metadata

property	type	description
navigationProperty	string	The name of the navigation property this metadata applies to.
expectedTemplates	Collection (Jci.Be.Data.EntityTemplate)	The templates in this list are the expected templates for entities referenced by the navigation property.
allowOtherTypes	boolean	If false, entities references by this navigation

		property should only use one of the expectedTemplates and should not be generic entities without a define entityTemplate.
--	--	---

[0124] Organizations may include a company, tenant, and/or another group of people that occupy and/or own a space. Organizations may have all of the properties of the entities (see Table 5), as well as the properties shown in Table 9.

Table 9: Organizations

property	type	description
reportingCurrency	string	Applications may use a dynamic property instead. The currency is the units id of a unit with quantity = currency.
reportingDateFormat	string	Applications may use a dynamic property instead. Date formats are up to the application and are not validated by the EntityAPI.
reportingUnitsIds	ReportingUnits[]	Applications may use a dynamic property instead. An array of quantity, commodity, and unitsId. For example: <pre>"reportingUnitsIds": [{"quantity": "power", "commodity": null, "unitsId": "kilowatts"}, {"quantity": "energy", "commodity": "Electricity", "unitsId": "kilowatt-hours"}, {"quantity": "energy", "commodity": "Energy", "unitsId": "British-thermal-units"}, {"quantity": "volume", "commodity": "NaturalGas", "unitsId": "standard-cubic-foot"}, {"quantity": "volume", "commodity": "LiquidPropane", "unitsId": "us-gallons"}, {"quantity": "area", "commodity": null, "unitsId": "square-feet"}, {"quantity": "pressure", "commodity": null, "unitsId": "inches-of-water"}, {"quantity": "currency", "commodity": null, "unitsId": "USD"}]</pre> A given quantity and commodity combination can only appear in the list once.
parent	Organization	A navigation property linking this organization to its parent.
parentId	string	The parent id. Read-only.
contains	Organization[]	A derived (read-only) navigation property. A list of organizations which have this organization as its parent.

owns	Space[]	This may be omitted. A derived (read-only) navigation property. A list of spaces which are owned by this organization.
occupies	Space[]	A derived (read-only) navigation property. A list of spaces which are occupied by this organization.
dataSources	DataSource[]	A derived (read-only) navigation property. A list of data sources which are associated with this organization.
parentAncestors	Organization[]	A derived (read-only) navigation property. A list of all organizations that can be reached by following Organization.parent relationships.
containsDescendents	Organization[]	A derived (read-only) navigation property. A list of organizations that can be reached by following the Organization.contains relationships.
usesSystems	System[]	A derived (read-only) navigation property. A list of systems where the system usedByOrganization property references this organization.

[0125] Spaces may include sites, building, and/or areas of a building. Spaces may have all of the properties of the entities (see Table 5), as well as the properties shown in Table 10.

Table 10: Spaces

property	type	description
spaceType	string	May use entityTemplateId instead. Possible values: Region, Site, Campus, Facility, Building, Wing, Floor, Room, Suite, Zone
use	string	Applications may use a dynamic property instead. Used to categorize spaces, especially buildings.
location	Complex object	
area	double	
areaUnitsId	string	
locatedIn	Space	
locatedInId	string	The space id for the locatedIn space. Read-only.
ownedBy	Organization	This may be omitted.
ownedById	string	This may be omitted. The organization id for the owned by organization. Read-only.
occupiedBy	Organization	
occupiedById	string	The organization id for the occupied by organization. Read-only.
points	Points[]	This may be omitted. These points are directly associated with the space.
servedBySystems	System[]	A derived (read-only) navigation property.

		A list of systems whose list of servesSpaces includes this space.
containsSystems	System[]	May use servedBySystems instead. A derived (read-only) navigation property. A list of systems which are directly located in this space (immediate children).
containsSpaces	Space[]	A derived (read-only) navigation property. A list of spaces which are directly located in this space (immediate children).
ancestorSpaces	Space[]	May use locatedInAncestors instead.
locatedInAncestors	Space[]	A derived (read-only) navigation property. A list of spaces that this space is located in. This is the transitive closure of the spaces reachable from the locatedIn relationships.
descendentSpaces	Space[]	May use containsSpacesDescendents instead.
containsSpacesDescendents	Space[]	A derived (read-only) navigation property. A list of spaces contained by this space. This is the transitive closure of the spaces reachable from the containsSpaces relationships.
descendentSystems	System[]	May use servedBySystemsDescendents instead.
servedBySystemsDescendents	System[]	A derived (read-only) navigation property. A list of systems serving this space and contained spaces and their subsystems. This is the transitive closure of systems reachable from the containsSpaces, servedBySystems and subsystems relationships.
ownedByAncestors	Organization[]	A derived (read-only) navigation property. A list of Organizations that can be reached by following the Space.ownedBy and Organization.parent relationships.
occupiedByAncestors	Organization[]	A derived (read-only) navigation property. A list of Organizations that can be reached by following the Space.locatedIn, Space.occupiedBy and Organization.parent relationships.

[0126] Systems may include energy, HVAC, and/or other control systems. Systems can be nested. For example, a main meter could have a subsystem which are sub-meters. Systems may have all of the properties of the entities (see Table 5), as well as the properties shown in Table 11.

Table 11: Systems

property	type	description
systemType	string	May use entityType instead. Possible values: GenericEquipment, Meter, AirHandlingUnit, VavBox,

		RooftopUnit, CRAC, Chiller, ChilledBeam, Boiler, HeatExchanger, Humidifier, Plant, Pump, VariableSpeedDrive, Fan, VariableFrequencyDrive, UnitVentilator, HeatPump, FumeHood, FanCoilUnit, WeatherStation, NetworkDevice, FieldBus
locatedIn	Space	May use servesSpaces instead. The space that this system is physically located in.
partOf	System	The system that this system is part of.
partOfId	string	The system id of the partOf system. Read-only.
dataSource	DataSource	The data source that defined this system.
dataSourceId	string	The data source id. Read-only.
points	Points[]	A list of points used by this system.
servesSpaces	Space[]	A list of spaces that this system directly serves.
subSystems	System[]	A derived (read-only) navigation property. This is the list of systems which are part of this system.
ancestorSpaces	Space[]	May use servesSpacesAncestors instead.
servesSpacesAncestors	Space[]	A derived (read-only) navigation property. A list of spaces that this system serves. This is the transitive closure of the spaces reachable from the System.partOf, System.servesSpaces and Space.locatedIn relationships.
descendentSystems	System[]	May use subSystemDescendents instead.
subSystemDescendents	System[]	A derived (read-only) navigation property. A list of subsystems. This is the transitive closure of systems reachable from the subsystems relationships.
partOfAncestors	System[]	A derived (read-only) navigation property. A list of Systems that can be reached by following the System.partOf relationships.
usedByOrganization	Organization	The organization that directly uses this system. This is to allow virtual systems (with calculated points) to be associated with organizations.

[0127] Points may identify a single value in a building automation system (BAS) that is being monitored. The points may have a native reference which is a BAS identifier. A point's source is defined as online, offline, or virtual. An online point may receive its data from the BAS. An offline point may get its data through a user interface (UI). A virtual point may be calculated dynamically. Online and offline points may have a time series with a raw transformation type. Virtual points may have a time series with a custom expression transformation type. A point may have one time series for each transformation type. Points may have all of the properties of the entities (see Table 5), as well as the properties shown in Table 12.

Table 12: Points

property	type	description
source	string	Possible values: online – gets its values from the BAS offline – gets its values imported by the user virtual – calculated values baseline – baseline data
nativeReference	string	
pointRole	string	May use entityTemplateId instead. Must be one of the PointRole enumeration values.
classId	int	The Metasys or BACnet classid.
dataSource	DataSource	
dataSourceId	string	The dataSource id. Read-only.
commodityName	string	May use a dynamic property instead. Possible values: Undefined, Electricity, NaturalGas, ChilledWater, HotWater, Steam, Water, Sewage, LiquidPropane, FuelOilHomeHeating, FuelOilCommercialHeating, FuelOilResidual, Diesel, Coal, Energy
minValue	double	The minimum value allowed for this point. Values below the minimum may be discarded.
maxValue	double	The maximum value allowed for this point. Values above the maximum may be discarded.
resetValue	double	The value at which a meter consumption value resets to zero.
nativeEnumId	string	The native identifier for the enumeration from the underlying system. Null if this point is not an enumeration value.
unitsId	string	The unit of measure for the raw values for this point.
customTransformExpression	string	The CustomTransformExpression provides the formula used to compute the values for this point.
usedBySystems	System[]	A derived (read-only) navigation property. A list of systems which use this point.
usedBySpaces	Space[]	A derived (read-only) navigation property. A list of spaces which use this point.
time series	Time series[]	A derived (read-only) navigation property. A list of time series for this point.

[0128] Time series may have all of the properties of the entities (see Table 5), as well as the properties shown in Table 13.

Table 13: Time Series

property	type	description
sourceTime seriesId	string	The time series that this time series was derived from.

seriesType	string	Possible Values: Cumulative, Interval, Instantaneous
intervalMinutes	int	Obsolete
dataType	string	All samples in the time series may be stored as double. The DataType field describes the native data type.
transformationType	string	A point may have either a Raw or CustomExpression time series. The other transformation types are derived from this base time series. Possible Values: Raw, BoundsLimited, AverageQuarterHour, AverageHourly, AverageDaily, AverageMonthly, AverageYearly, TotalQuarterHour, TotalHourly, TotalDaily, TotalMonthly, TotalYearly, DeltaQuarterHour, DeltaHourly, DeltaDaily, DeltaMonthly, DeltaYearly, CustomExpression
rollupInterval	string	A read-only value derived from the transformationType which describes the periodicity of the samples in this time series.
customTransformExpression	string	When the transformationType is set to "CustomExpression", the CustomTransformExpression field provides the formula used to compute the values for this time series.
unitsId	string	The units of measure for the values in this time series.
samplesUrl	string	A read-only value the give you a base URL to query the time series API with.
point	Point	Required. The point this time series belongs to.
pointId	string	The point id. Read-only.

[0129] When a transformation type property is set to "CustomExpression" on a time series entity, a custom transform expression property may hold an expression that is evaluated every time a new source sample is added to time series API 1474. For example, the custom expression 'point("ID1") + point("ID2")' may add the value of the samples for point ID1 and point ID2 when a new sample is added to Time Series API 1474 for either point. The result of this calculation is then stored with the time series id of the time series that holds the custom expression.

[0130] A data source is the BAS or other source for the entity configuration. The drivers in the data collector may be the data sources for Metasys by Johnson Control, Inc., FX, and BACnet. Data sources may have all of the properties of the entities (see Table 5), as well as the properties shown in Table 14.

Table 14: Data Sources

property	Type	description
configurationDiscoveryFilter	string	
configurationDiscoveryStatus	string	Possible Values: Requested, Started, Finished
connectionStatus	string	Possible Values: Unknown, ConnectionTestRequested, ConnectionTestStarted, ConnectionTestFailed, ConnectionTestSucceeded
connectionTestDate	DateTimeOffset	The date and time the connection test started or finished.
host	string	Host name or IP address
port	int	Port number
deviceNbr	int	Device Number
username	string	
password	string	
dataSourceType	string	
organization	Organization	
points	Point[]	A derived (read-only) navigation property. A list of points associated with this data source.
systems	System[]	A derived (read-only) navigation property. A list of systems associated with this data source.

[0131] A units endpoint may list units of measure. Units may have all of the properties of the entities (see Table 5), as well as the properties shown in Table 15.

Table 15: Units

property	type	description
symbol	string	
alias	string	An alternate symbol
quantity	string	A way of categorizing units to identify units which can be converted to one another. Possible values: unknown, acceleration, area, currency, capacitance, current, electric_conductance, electric_resistance, energy, entropy, force, frequency, illuminance, inductance, information, length, luminous_flux, luminous_intensity, magnetic_flux, magnetic_flux_density, mass, mass_flow, other, plane_angle, power, pressure, specific_energy, temperature, time, velocity, voltage, volume, volumetric_flow
measureType	string	The Metasys categories for units which are not as detailed as quantity.
unitSystem	string	Primary unit system the units belong to.

		SI, US, metric, Imperial, and other values
metasysUnitsCode	string	Equivalent Metasys units code
metasysUnitsId	int	Equivalent Metasys units id

[0132] Referring now to FIG. 15, an entity graph 1500 is shown, according to some embodiments. In some embodiments, entity graph 1000 is generated or used by the entity API 1478, as described with reference to FIG. 14. The entity graph 1500 describes how a building is organized and how the different systems and spaces within the building relate to each other. For example, entity graph 1500 is shown to include an organization 1502, a space 1504, a system 1506, a point 1508, a time series 1510, and a data source 1512. The arrows interconnecting organization 1502, space 1504, system 1506, point 1508, time series 1510, and data source 1512 identify the relationships between such entities. In some embodiments, the relationships are stored as attributes of the entity described by the attribute.

[0133] Organization 1502 is shown to include a contains descendants attribute 1514, a parent ancestors attribute 1516, a contains attribute 1518, a parent attribute 1520, an occupies attribute 1524, an owns attribute 1530, a uses system attribute 1548, and a data source attribute 1580. The contains descendants attribute 1514 identifies any descendant entities contained within organization 1502. The parent ancestors attribute 1516 identifies any parent entities to organization 1502. The contains attribute 1518 identifies any other organizations contained within organization 1502. The asterisk alongside the contains attribute 1518 indicates that organization 1502 can contain any number of other organizations. The parent attribute 1520 identifies a parent organization within which organization 1502 associated with. The number 1 alongside the parent attribute 1520 indicates that organization 1502 can be associated with exactly one other parent organization. The occupies attribute 1526 identifies any spaces occupied by organization 1502. The asterisk alongside the occupies attribute 1526 indicates that organization 1502 can occupy any number of spaces. The owns attribute 1530 identifies any spaces owned by organization 1502. The asterisk alongside the owned attribute 1530 indicates that organization 1502 can own any number of spaces. The uses system attribute 1548 identifies systems used by organization 1502. The data source attribute 1580 identifies any data sources that are associated with organization 1502. The asterisk alongside the data source attribute 1580 indicates that any number of data sources can be associated with organization 1502.

[0134] Space 1504 is shown to include an occupied by ancestors attribute 1522, an occupied by attribute 1524, an owned by ancestors attribute 1526, an owned by attribute 1528, a contains space descendants attribute 1532, a located in ancestors attribute 1534, a contains spaces attribute 1536, a located in attribute 1538, a served by system descendants attribute 1540, a served by systems attribute 1546, and a points attribute 1560. The occupied by ancestors attribute 1522 identifies one or more ancestors to organization 1502 that are occupied by space 1504. The asterisk alongside the occupied by ancestors attribute 1522 indicates that space 1504 can be occupied by any number of ancestors. The occupied by attribute 1524 identifies an organization occupied by space 1504. The number 1 alongside the occupied by attribute 1524 indicates that space 1504 can be occupied by exactly one organization. The owned by ancestors attribute 1526 identifies one or more ancestors to organization 1502 that own space 1504. The asterisk alongside the owned by ancestors attribute 1526 indicates that space 1504 can be owned by any number of ancestors. The owned by attribute 1528 identifies an organization that owns space 1504. The number 1 alongside the owned by attribute 1528 indicates that space 1504 can be owned by exactly one organization.

[0135] The contains space descendants attribute 1532 identifies any descendants to space 1504 that are contained within space 1504. The located in ancestors attribute 1534 identifies any ancestors to space 1504 within which space 1504 is located. The contains spaces attribute 1536 identifies any other spaces contained within space 1504. The asterisk alongside the contains spaces attribute 1536 indicates that space 1504 can contain any number of other spaces. The located in attribute 1538 identifies another space within which space 1504 is located. The number 1 alongside the located in attribute 1538 indicates that space 1504 can be located in exactly one other space. The served by system descendants attribute 1540 identifies any descendent systems that serve space 1504. The asterisk alongside the served by descendant systems attribute 1540 indicates that space 1504 can be served by any number of descendant systems. The served by systems attribute 1546 identifies any systems that serve space 1504. The asterisk alongside the served by systems attribute 1546 indicates that space 1504 can be served by any number of systems. The points attribute 1560 identifies any data points that are associated with space 1504. The asterisk

alongside the points attribute 1560 indicates that any number of data points can be associated with space 1504.

[0136] System 1006 is shown to include a serves space ancestors attribute 1542, a serves spaces attribute 1544, a subsystem descendants attribute 1550, a part of ancestors attribute 1552, a subsystems attribute 1554, a part of attribute 1556, a used by organization attribute 1582, a points attribute 1564, and a data source attribute 1572. The serves space ancestors attribute 1542 identifies any ancestors to space 1504 that are served by system 1506. The asterisk alongside the serves ancestor spaces attribute 1542 indicates that system 1506 can serve any number of ancestor spaces. The serves spaces attribute 1544 identifies any spaces that are served by system 1506. The asterisk alongside the serves spaces attribute 1544 indicates that system 1506 can serve any number of spaces. The used by organization attribute 1582 identifies systems used by the organization 1502. The asterisk alongside the used by organization attribute 1582 indicates system 1506 can be used by any number of organizations.

[0137] The subsystem descendants attribute 1550 identifies any subsystem descendants of other systems contained within system 1506. The part of ancestors attribute 1552 identifies any ancestors to system 1506 that system 1506 is part of. The subsystems attribute 1554 identifies any subsystems contained within system 1506. The asterisk alongside the subsystems attribute 1554 indicates that system 1506 can contain any number of subsystems. The part of attribute 1556 identifies any other systems that system 1506 is part of. The number 1 alongside the part of attribute 1556 indicates that system 1506 can be part of exactly one other system. The points attribute 1564 identifies any data points that are associated with system 1506. The asterisk alongside the points attribute 1564 indicates that any number of data points can be associated with system 1506. The data source attribute 1572 identifies any data sources that are associated with system 1506. The asterisk alongside the data source attribute 1572 indicates that any number of data sources can be associated with system 1506.

[0138] Time series 1510 is shown to include a point attribute 1568. The point attribute 1568 identifies a point that is associated with the time series 1510. The number 1 alongside the point attribute 1568 indicates exactly one point is associated with the time series 1510.

[0139] Point 1508 is shown to include a used by spaces attribute 1558, a used by systems attribute 1562, a time series attribute 1566, and a data source attribute 1576. The used by spaces attribute 1558 identifies data points used by space 1504. The asterisk alongside the used by spaces attribute 1558 indicates that point 1008 can be used by any number of spaces. The used by systems attribute 1562 identifies data points used by system 1506. The asterisk alongside the used by systems attribute 1562 indicates that point 1008 can be used by any number of systems. The time series attribute 1566 identifies a data point associated with time series 1510. The asterisk alongside the time series attribute 1566 indicates that point 1008 can be associated with any number of time series. The data source attribute 1576 identifies data points associated with data source 1512. The asterisk alongside the data source attribute 1576 indicates that point 1008 can be associated with any number of data sources.

[0140] Data source 1512 is shown to include a systems attribute 1570, a points attribute 1574, and an organizations attribute 1578. The systems attribute 1570 identifies systems associated with data source 1512. The asterisk next to systems attribute 1570 indicates that any number of systems can be associated with data source 1512. The points attribute 1574 identifies any data points that are associated with data source 1512. The asterisk alongside the points attribute 1574 indicates that any number of data points can be associated with data source 1512. The data source attribute 1580 identifies an organization associated with data source 1512. The number 1 next to organization attribute 1578 indicates that one organization can be associated with data source 1512.

[0141] Referring back to FIG. 14, time series API 1474 (e.g., having queryable streams 1476) is configured to display documentation for points, time series, samples, messages, and/or job endpoints. Time series API 1474 may facilitate displaying a sample for a single point and/or multiple points. A point may have a raw time series which has original samples. Other time series on the point may be rollups calculated based on the raw time series. The sum, average, and delta parameters (e.g., quarter hour, hourly, daily, monthly, yearly, etc.) may be used to select a time series. The uniform resource identifier (URI) parameters for one or more points is shown in Table 15.

Table 15: URI Parameters – Points

Name	Description	Type
------	-------------	------

startTime	Optional. ISO8601 date format. If not specified all samples before the endTime are returned.	date
endTime	Optional. ISO8601 date format. If not specified all samples after startTime are returned. If neither startTime or endTime are specified, all samples are returned.	date
sum	Optional. Specifies the period to sum by. Possible values: quarterly (i.e. quarter hour), hourly, daily, monthly, yearly	string
average	Optional. Specifies the period to average by. Possible values: quarterly, hourly, daily, monthly, yearly	string
delta	Optional. Specifies the period to compute deltas by. Possible values: quarterly, hourly, daily, monthly, yearly	string
points	Required (if multiple). A comma separated list of point ids.	string

[0142] Time series API 1474 may facilitate displaying, deleting, and/or receiving statistics of samples of one or more time series. The URI parameters for one or more time series is shown in Table 16.

Table 16: URI Parameters – Time series

Name	Description	Type
time seriesId	time series id to get	string
ids	optional list of additional time series ids to get	Collection of string
startTime	Start Time (localtime + offset), default is UTC now minus 1 day	date
endTime	End Time (localtime + offset), default is UTC now	date
orderby	Supports ordering by timestamp. An optional ASC or DESC keyword sets the sort direction.	string
top	Limits the number of samples returned per time series.	integer
skip	Excludes the first n samples per time series.	Integer
convertedUnitsId	UnitsId of the units you want the sample values converted to.	string

[0143] Time series API 1474 may also facilitate determining which samples have been cleansed. For example, when a point is created, an time series (e.g., with a transformation type of “is cleansed”) is created for the point. The “is cleansed” time series stores samples at the timestamp when a sample triggered a cleanser to modify its data. The “is cleansed” time series is queried like any other time series object, and returns different values based on which cleanser was run on that sample. The cleanser may include a bounds limiting cleanser, an instantaneous consumption cleanser, an interpolate gap filler, and/or a data spike cleanser.

[0144] Job endpoints of the time series API 1474 may be used to interact with a job manager. According to an exemplary embodiment, the job manager is a background process

in the time series API 1474 used to schedule jobs (e.g., repeatable jobs, etc.). A job may be an activity that interacts with time series data, such as collecting weather data, detecting faults, etc. When a job is run, the time series API 1474 is configured to create one or more tasks to perform the work. A job may include the parameters shown in Table 17. A user may use the time series API 1474 to return a list of registered job types, create a new job, get scheduled jobs, delete a scheduled job, get job history (e.g., scheduled jobs, running jobs, completed tasks, etc.), and get and set job manager settings (see Table 18).

Table 17: Job Parameters

Name	Description	Type
id	Job id	string
type	Registered job type	string
next	UTC date time the job should run next	date time (ISO 8601)
interval	Time interval the job should repeat if null, the job doesn't repeat	timespan (ISO 8601 duration)
settings	Dictionary of key/value pairs used to customize the job	dictionary

Table 18: Job Manager Settings

Name	Description	Type
taskWorkerCount	The number of threads processing tasks If set to zero the job manager will not run tasks	integer number
taskQueuePollingInterval	The interval the job manager waits before checking for new tasks	timespan
taskQueueCount	The number of tasks waiting to be run This value cannot be set	integer number
jobQueuePollingInterval	The interval the job manager waits before checking for new jobs	integer number
jobQueueCount	The number of jobs waiting to be run This value cannot be set	integer number

[0145] By way of example, the time series API 1474 may run a job to collect weather related data from a service provider (e.g., accessed through the weather API 1470, etc.). The time series API 1474 may store the weather related data so that it may be queried. To activate this process, a weather station system may be added to a space through Entity API 1478. Prior to the weather station system being created, weather related points and a space to associate the weather station with may be identified and created. For example, a process may include (i) creating a space that the weather station may use, (ii) creating a weather point to

store data against, and (iii) creating a weather station and connecting the weather point to the space.

[0146] After a weather station system is created, a weather collector job may be added to the job manager to initiate the data collection process. The first time the weather collector job runs it may try to determine a weather id for the weather station by using the latitude and longitude of the associated space to lookup up the closest weather id. Every time the weather job runs it may try to collect data missing since the last time it ran (e.g., based off of a timestamp of an outdoor air temperature point, etc.). In some embodiments, if no data is able to be found for a predetermined time frame (e.g., the last three years, etc.), the job will create a task for each month for the predetermined time frame to fill in the missing data. A weather report may then be generated on a desired, repeating basis (e.g., hourly, daily, etc.) and the weather related data is able to be queried like any other point (e.g., an operator can receive information relating to the current temperature at a desired location, etc.).

[0147] Referring still to FIG. 14, IoT hub 1420 may facilitate bi-directional communication between the cloud and devices in a secure, reliable, and uniform manner. As shown in FIG. 14, IoT hub 1420 includes a device registry module 1422, a metadata API 1424 (e.g., including device status, command feedbacks, etc.), an egress API 1426, and an ingress API 1428. The device registry module 1422 is configured to maintain a collection of credentials of devices (e.g., devices 1402, web/mobile devices 1406, etc.) that may be used to communicate with IoT Hub 1420. Each device may have two usable keys (e.g., a security key, a license key, etc.) that can be rotated as necessary. In some embodiments, the credentials (e.g., keys, etc.) are created and shared with the device at the time of manufacturing. In some embodiments, a device registry backdoor 1464 of Security API 1440 allows for the registration (e.g., assignment of credential/keys, etc.) post-manufacturing.

[0148] The egress API 1426 is configured to facilitate sending a message (e.g., a command message, etc.) from IoT hub 1420. The message may be used to issue a command to a device (e.g., device 1402, web/mobile device 1406, etc.) to take some action. Following receiving and processing the command, the device may respond with a message indicating whether the action is complete, rejected, or abandoned.

[0149] The ingress API 1428 is configured to facilitate receiving messages from a device (e.g., device 1402, web/mobile device 1406, etc.). The messages received from a device may include a device info message, a telemetry message, or still another message. The device info message may be used to define and/or update properties and/or supported commands for a device. The telemetry message may be used to record telemetry data for later retrieval and use. The telemetry data may be stored in time series API 1474.

[0150] Referring still to FIG. 14, notification API 1484 may be configured to communicate with external notification services 1486 (e.g., Azure notification hubs, etc.). Such communication may facilitate providing notifications to a device (e.g., device 1402, web/mobile devices 1406, etc.). Email API 1488 may be configured communicate with external email services 1490 (e.g., SendGrid, etc.). Such communication may facilitate providing emails to a device (e.g., device 1402, web/mobile devices 1406, etc.).

Device Registration

[0151] When a new device is introduced into an IoT environment, such as IoT environment 1100, described above, the device needs to be registered within IoT environment to ensure proper security and operation of the device within the IoT environment. As described above, devices incorporated into an IoT environment may include HVAC equipment 408, smart connected devices 1102, and the like. Turning now to FIG. 16, a process 1600 for registering a device within an IoT environment is shown, according to some embodiments. In one embodiment, the process 1600 may be associated with the device management technology concept 1108, described above. At process block 1602, a firmware token is obtained for the device to be registered. The firmware token may be used to authorize a request to register the device. The firmware tokens may further represent an identity of the device to be registered. For example, the firmware token may establish what permissions the device will have in the system. The firmware token may further establish one or more access levels of the device. In one embodiment, the firmware tokens may be stored in the token storage 1445 of the security API 1440.

[0152] In one embodiment, the firmware tokens represent a set of claims that can be used to restrict a client's (e.g. HVAC equipment 408, smart connected devices 1102, and the like) permissions when using secured systems. For example, the firmware tokens may restrict a

client's permissions when using an IMS-secured endpoint, such as an HTTP API. Using the firmware tokens for a security model, as described above, can also be called a claims-based security model. Various claims are required to be included with the firmware tokens, but the firmware tokens can generally include any string of data as a claim. For example, a subject claim may be a consistent user ID. This claim may be available for all firmware tokens that are not user-less tokens. In some embodiments, the firmware tokens may be requires from an IMS by clients, which may then send the firmware tokens to an IMS-secured endpoint. In one embodiment, the firmware tokens may be sent to an IMS-secured endpoint using Bearer authorization in an HTTP Authorization header for HTTP-based APIs. In some embodiments, the firmware tokens may be time limited. For example, a firmware token may be good for one hour, although some firmware tokens may be available for more than one hour or less than one hour. In some embodiments, the firmware tokens are JSON Web Tokens (JWT). JWT use an open standard for encoding claims as a JSON object. The firmware tokens may provide an abstraction by replacing different authorization constructs (e.g. username and passwords, assertions, etc.) for a single token understood by a resource. This abstraction can enable issuing firmware tokens that are valid for a short time period.

[0153] At process block 1604, the new device may be registered with the IoT environment. In one embodiment, an API is used to register the device. For example, the application API 1460 may register the device. The application API 1460 may require the firmware token obtained at process block 1602. The application API 1460 may further require a unique device ID to be provided, that is associated with the new device to be registered. In one embodiment, the unique device ID is provided by the device manufacturer. For example, the unique device ID may be located on the device itself for reference. In one embodiment, the unique device ID is a media access control (MAC) address. In other embodiments, the unique device ID may be a device serial number, a device ID code, or other unique identifier. Once the proper authentication has been provided (e.g. the firmware token and the unique device ID), the device will be registered within a document database of the IoT environment associated with the security API 1440, such as via device storage 1446. The document database may contain a list of all devices registered within the IoT environment. In one embodiment, the document database is in an Azure[®] database from Microsoft[®]. Further, the

Security API may generate a primary key and a secondary key upon the device being registered. The primary key may be used to claim the device, as described below.

[0154] Once the device is registered, a device shadow is generated at process block 1606. The device shadow may be a virtual representation of the physical device being registered. In one embodiment, the device shadow is a JSON blob that represents the physical device. The device shadow may allow for other devices within the IoT environment, either real or virtual, to read one or more data points associated with the device shadow. For example, the physical device may pass data point values to the device shadow to allow the data point values to be read by other devices in the IoT environment. In some embodiments, the other devices within the IoT environment may be able to write values to the device shadow. These values can then be passed to the physical device from the device shadow to allow for parameters to be changed within the physical device. In one embodiment, the device shadow is created based on a template associated with the particular device. For example, where the device is a sensor, the virtual device may be generated to have data points associated with a sensor, such as temperature data points where the sensor is a temperature sensor. In some embodiments, the templates may be standard templates stored within the IoT environment. In other embodiments, the templates may be provided by a manufacturer associated with the physical device. For example, once the unique device ID is known, the IoT environment may query a database associated with the manufacturer of the physical device to obtain a template associated with the physical device for use in generating the shadow device.

[0155] At process block 1608, the device shadow is updated. Updating the device shadow may include including additional data points that may not have been included in the template used to generate the device shadow. For example, where the IoT environment generates the device shadow using a pre-existing template, some attributes and data points may not be included in the template depending on how specific the template is. As a more specific example, if the physical device being registered is a temperature sensor, the IoT environment may select a template associated with a standard temperature sensors. However, if the temperature sensors includes additional functionality, such as the ability to provide humidity data, this can be conveyed to the IoT environment, and the device shadow can be updated to reflect the additional data points. Thus, the pre-existing template may be compared to the attributes and data points of the physical device. In some embodiments, the attributes and

data points associated with the physical device may be provided by a user. However, in some examples the physical device may broadcast specific attributes and data points to the data platform 1400, such as to the application API 1460.

[0156] Finally, at process block 1610, the physical device is claimed. Claiming the physical device allows for data collected by the physical device to be provided to a user view. Claiming the physical device may further allow for secure communications from a cloud-based server to the physical device. Claiming the device can further provide a user with the ability to link other services, such as an If This Then That (IFTTT) service to communicate with the physical device on behalf of the user. In one embodiment, the unique ID and the primary key generated at process block 1604 are used by the Security API 1440 to claim the device. In some embodiments, the Security API 1440 may require the unique ID, the primary key, and the firmware token used to register the device. In some embodiments the device is claimed via the claim device module 1452 within the identity API 1450.

[0157] Turning now to FIG. 17, a flow diagram illustrating the data flow 1700 during the physical device registration process 1600 is shown in detail. In some embodiments, the data flow 1700 is performed by the security, privacy, access control and compliance management technology concept 1190, or via data platform 1400 as described above. At process block 1702, a create device command is provided. The create device command can generate an add device instruction 1704 within a security logic API 1706. In some embodiments, the security logic API 1706 may be part of the security API 1440 described above. The security logic API 1706 may then issue a register device command at process block 1708. The register device command can cause an initialize device command to be generated by the security logic API 1706 at process block 1710. The initialize device command can provide a signal to the physical device to instruct the device to perform a necessary initialization processes. The initialization process may configure the physical device to fully communicate on one or more communication networks. Initializing the physical device may also include instructing the physical device to provide certain information to the IoT environment 1100 and/or the security logic API 1706. Once the device has been initialized, random keys can be created for the device at process block 1712, as described above. In one embodiment, a primary key and a secondary key may be generated at process block 1712. In other embodiments, the register device command may initiate an overwrite process at process block 1714 where the

physical device being registered has previously been registered within the IoT environment 1100 and/or the data platform 1400. The overwrite process may replace the data current associated with a previously registered physical device with the newly registered physical device. In some embodiments, a user may be asked whether they want to override the previously registered physical device.

[0158] The register device command can further generate an add device command that is provided to a device repository 1716 (e.g. device storage 1446 of the data platform 1400) at process block 1718. Further at process block 1718, the device repository 1716 can determine if the new physical device currently exists in the repository. If the device currently exists, the associated shadow device can be read at process block 1720. In one embodiment, data points associated with the shadow device are read at process block 1722. Further, if the device is determined to currently exist at process block 1718, the document repository 1730 may read the shadow device at process block 1721. In a further embodiment, data points associated with the shadow device are read at process block 1721, by the document repository 1730. If the device is determined not to exist at process block 1718, an add device command is provided to the device repository 1716 at process block 1722. At process block 1724, a set authentication command can be issued to establish one or more authentication parameters associated with the physical device being registered. At process block 1726 a manager-client registry can be read. The manager-client registry may include relationships associated with one or more devices within IoT environment 1100. Thus, the device repository 1716 may determine what, if any, relationships are associated with the new physical device. Once the manager-client registry has been read, the device repository 1716 can provide an Add Device Async command to the device registry module 1422 within the IoT Hub 1420, at process block 1728. The Add Device Async command may register the device within the IoT Hub 1420, and thereby within the IoT environment 1100. At process block 1727, the device may be claimed.

[0159] The document repository 1730 may also receive an add device command at process block 1732. In some examples, the document repository received the add device command when it is determined that the device currently exists at process block 1718. In one embodiment, the document repository 1730 may be associated with the security API 1440. At process block 1738 a read client command is generated. The client command may read

clients within the IoT environment which may be associated with the new physical device. A document associated with the new physical device may be created in a document database 1740 at process block 1742. The document database 1740 may contain a list of all devices registered within the IoT environment. In one embodiment, the document database 1740 is in an Azure[®] database from Microsoft[®].

[0160] At process block 1744, an update device command may be received by the data platform 1400. The update device command may update a registered physical device in the IoT environment 1100 with one or more device properties 1746. The one or more device properties can include a device ID 1748, a device state 1750, a build quality 1752, a product version 1754, or other properties associated with the physical device. The properties of the registered physical device can then be updated at process block 1756 within the security logic API 1706. Finally, the registered physical device may then be updated within the device registry module 1422 at process block 1758.

[0161] Turning now to FIG. 18, a block diagram illustrating a distributed BMS device 1800 is shown, according to some embodiments. The distributed BMS device 1800 can be a smart connected device 1102 or an HVAC equipment 408 as described above. The distributed BMS device 1800 may further be a gateway 1128. In some embodiments, the distributed BMS device 1800 may be a virtual device on a cloud-based server (e.g. cloud-based server 1210). In other embodiments, the distributed BMS device 1800 may be a service provided by a cloud-based server. The distributed BMS device 1800 may include a processing circuit 1802 and a network interface 1804.

[0162] The network interface 1804 can allow the distributed BMS device 1800 to communicate with an IP network 1806. In some embodiments, the network interface 1804 can communicate with the IP network 1806 and one or more other non-IP networks (e.g. BACnet). The network interface 1804 may be or include wired or wireless communications interfaces (e.g., jacks, antennas, transmitters, receivers, transceivers, wire terminals, etc.) for conducting data communications with the IP network 1806. In various embodiments, communications via the network interface 1804 can be direct (e.g., local wired or wireless communications) or via a communications network (e.g., a WAN, the Internet, a cellular network, etc.). For example, the network interface 1804 can include an Ethernet card and

port for sending and receiving data via an Ethernet-based communications link or network. In another example, the network interface 1804 can include a Wi-Fi transceiver for communicating via a wireless communications network. In another example, the network interface 1804 can include cellular or mobile phone communications transceivers. In one embodiment, the network interface 1804 is a power line communications interface. In other embodiments, the network interface 1804 is an Ethernet interface. The network interface 1804 may allow the distributed BMS device 1800 to communicate with a device 1402, as described above.

[0163] The processing circuit 1802 is shown to include a processor 1808 and a memory 1810. The processor 1808 may be a general purpose or specific purpose processor, an application specific integrated circuit (ASIC), one or more field programmable gate arrays (FPGAs), a group of processing components, or other suitable processing components. The processor 1808 may be configured to execute computer code or instructions stored in memory 1810 or received from other computer readable media (e.g., CDROM, network storage, a remote server, etc.).

[0164] Memory 1810 may include one or more devices (e.g., memory units, memory devices, storage devices, etc.) for storing data and/or computer code for completing and/or facilitating the various processes described in the present disclosure. Memory 1810 may include random access memory (RAM), read-only memory (ROM), hard drive storage, temporary storage, non-volatile memory, flash memory, optical memory, or any other suitable memory for storing software objects and/or computer instructions. Memory 1810 may include database components, object code components, script components, or any other type of information structure for supporting the various activities and information structures described in the present disclosure. Memory 1810 may be communicably connected to the processor 1808 via processing circuit 1802 and may include computer code for executing (e.g., by processor 1808) one or more processes described herein. For example, the memory 1810 may be contain executable code for the device registration process 1600 described above.

[0165] The memory 1810 may include an IoT hub, such as IoT hub 1420. The IoT hub 1420 may include device registry module 1422. The device registration module 1422 can

perform the device registration process 1600 described above. As described above, the device registry module 1422 may serve as a device registration service for registering devices in a distributed BMS system. In one embodiment, the device registry module 1422 may be in communication with the security API 1440 to access one or more modules associated with the security API 1440, such as the device storage 1446 and the token storage 1445 for purposes of performing the device registration process 1600. The memory 1810 may further include a device shadows module 1812. The device shadows module 1812 may store one or more device shadows associated with HVAC devices in a distributed BMS, such as the device 1402. While not shown, it is contemplated that the memory 1810 may include some or all of the elements of the data platform 1400, described above. In some embodiments, there may be multiple distributed BMS devices in a distributed BMS, and the elements of data platform 1400 may be distributed among several BMS devices in a distributed BMS, such as system 408. For purposes of this disclosure, the terms distributed BMS and IoT environment should be understood to be interchangeable.

Configuration of Exemplary Embodiments

[0166] The construction and arrangement of the systems and methods as shown in the various exemplary embodiments are illustrative only. Although only a few embodiments have been described in detail in this disclosure, many modifications are possible (e.g., variations in sizes, dimensions, structures, shapes and proportions of the various elements, values of parameters, mounting arrangements, use of materials, colors, orientations, etc.). For example, the position of elements may be reversed or otherwise varied and the nature or number of discrete elements or positions may be altered or varied. Accordingly, all such modifications are intended to be included within the scope of the present disclosure. The order or sequence of any process or method steps may be varied or re-sequenced according to alternative embodiments. Other substitutions, modifications, changes, and omissions may be made in the design, operating conditions and arrangement of the exemplary embodiments without departing from the scope of the present disclosure.

[0167] The present disclosure contemplates methods, systems and program products on any machine-readable media for accomplishing various operations. The embodiments of the present disclosure may be implemented using existing computer processors, or by a special

purpose computer processor for an appropriate system, incorporated for this or another purpose, or by a hardwired system. Embodiments within the scope of the present disclosure include program products comprising machine-readable media for carrying or having machine-executable instructions or data structures stored thereon. Such machine-readable media can be any available media that can be accessed by a general purpose or special purpose computer or other machine with a processor. By way of example, such machine-readable media can comprise RAM, ROM, EPROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code in the form of machine-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer or other machine with a processor. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a machine, the machine properly views the connection as a machine-readable medium. Thus, any such connection is properly termed a machine-readable medium. Combinations of the above are also included within the scope of machine-readable media. Machine-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing machines to perform a certain function or group of functions.

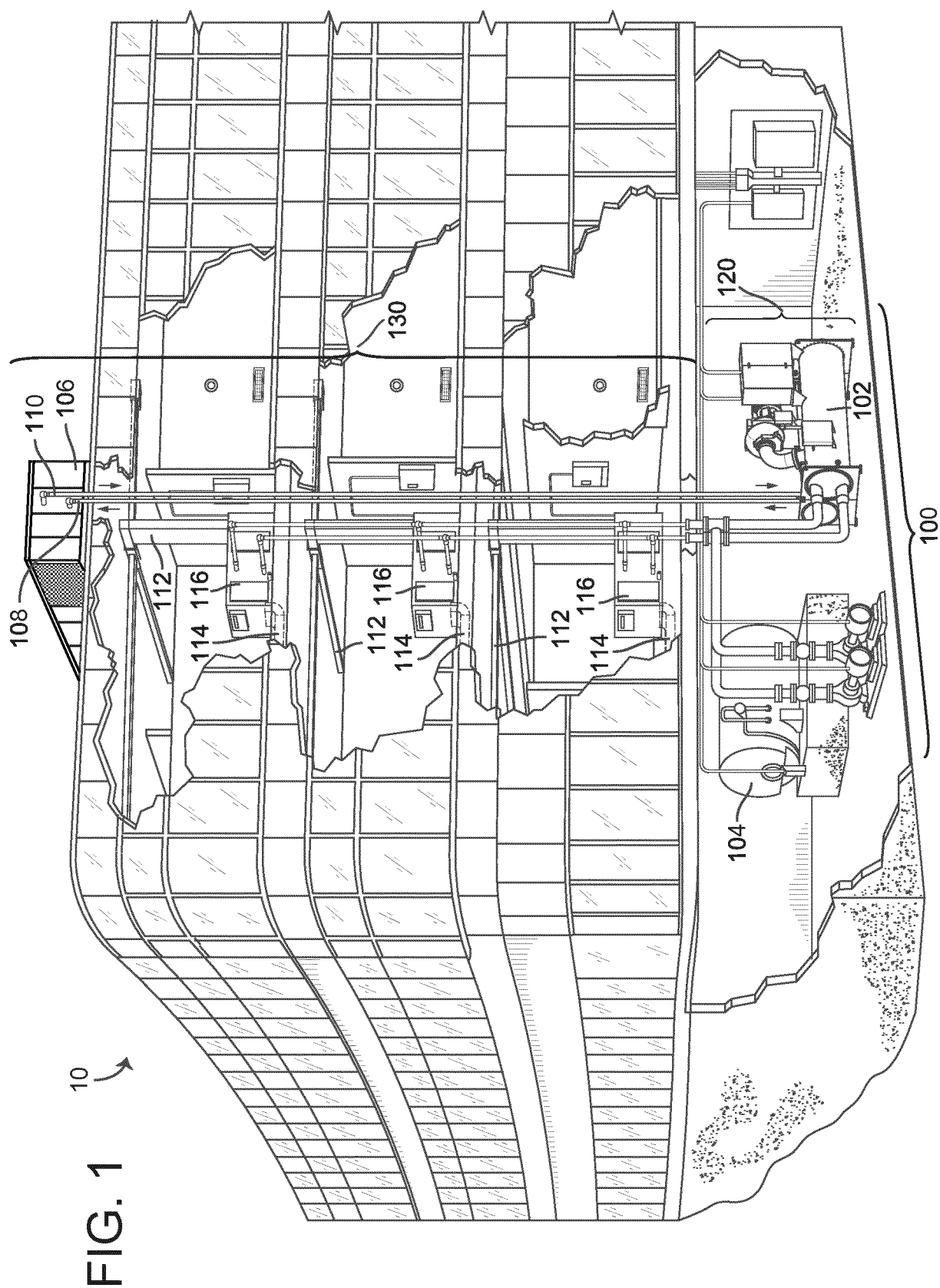
[0168] Although the figures show a specific order of method steps, the order of the steps may differ from what is depicted. Also two or more steps may be performed concurrently or with partial concurrence. Such variation will depend on the software and hardware systems chosen and on designer choice. All such variations are within the scope of the disclosure. Likewise, software implementations could be accomplished with standard programming techniques with rule based logic and other logic to accomplish the various connection steps, processing steps, comparison steps and decision steps.

WHAT IS CLAIMED IS:

1. A method for registering an HVAC device in a distributed building management system (BMS), comprising:
 - requesting a token, the token configured to authorize a registration of the HVAC device;
 - receiving the token at a registration service;
 - receiving a unique ID associated with the HVAC device at the registration service;
 - registering the device into a document database of the registration service;
 - generating a device shadow associated with the HVAC device; and
 - storing the device shadow in a memory of the distributed BMS.
2. The method of claim 1, wherein generating the device shadow comprises creating a generic device shadow based on a device template, wherein the device template comprises one or more data points associated with the HVAC device.
3. The method of claim 2, wherein the device template is based on a device type of the HVAC device.
4. The method of claim 2, further comprising comparing the data points of the device template against one or more data points of the HVAC device.
5. The method of claim 4, further comprising updating the device shadow with the data points of the device that are different from data points of the device template.
6. The method of claim 1, further comprising claiming the HVAC device, wherein claiming the HVAC device provides secure communications between the HVAC device and the distributed building management system.
7. The method of claim 1, wherein the token determines one or more permissions of the HVAC device.

8. The method of claim 1, wherein the unique device ID is one of a media access control address and a serial number of the device.
9. A distributed building management system, the system comprising:
 - an HVAC device; and
 - a distributed BMS device, comprising a processor, wherein the processor is configured to:
 - request a token, the token configured to authorize a registration of the HVAC device;
 - receive the token at a registration service;
 - receive a unique ID associated with the HVAC device;
 - register the device into a document database of the registration service; and
 - generate a device shadow associated with the HVAC device within a data platform of the distributed (BMS).
10. The system of claim 9, wherein generating the device shadow comprises creating a generic device shadow based on a device template, wherein the device template comprises one or more data points associated with the HVAC device.
11. The system of claim 10, wherein the device template is based on a device type of the HVAC device.
12. The system of claim 10, wherein the processor is further configured to compare the data points of the device template against one or more data points of the HVAC device.
13. The system of claim 12, wherein the processor is further configured to update the device shadow, with the data points of the device that are different from data points of the device template.
14. The system of claim 9, wherein the processor is further configured to claim the HVAC device, wherein claiming the HVAC device provides secure communications between the HVAC device and the distributed building management system.

15. The system of claim 9, wherein the token determines one or more permissions of the HVAC device.
16. The system of claim 9, wherein the unique device ID is one of a media access control address and a serial number of the HVAC device.
17. The system of claim 9, wherein the distributed BMS device is one of an HVAC device, a BMS controller, and a cloud-based service.
18. A method for registering an Internet of Things (IoT) HVAC device in a distributed building management system (BMS), comprising:
 - requesting a token, the token configured to authorize a registration of the IoT HVAC device;
 - receiving the token at a registration service;
 - receiving a unique ID associated with the IoT HVAC device;
 - registering the device into a document database of the registration service;
 - generating a device shadow associated with the IoT HVAC device within a data platform of the distributed BMS; and
 - claiming the IoT HVAC device, wherein claiming the IoT HVAC device provides secure communications between the IoT HVAC device and the distributed building management system.
19. The method of claim 18, wherein generating the device shadow comprises creating a generic device shadow based on a device template, wherein the device template comprises one or more data points associated with the IoT HVAC device and is based on a device type of the IoT HVAC device.
20. The method of claim 19, further comprising:
 - comparing the data points of the device template against one or more data points of the HVAC device; and
 - updating the device shadow with the data points of the device that are different from data points of the device template.



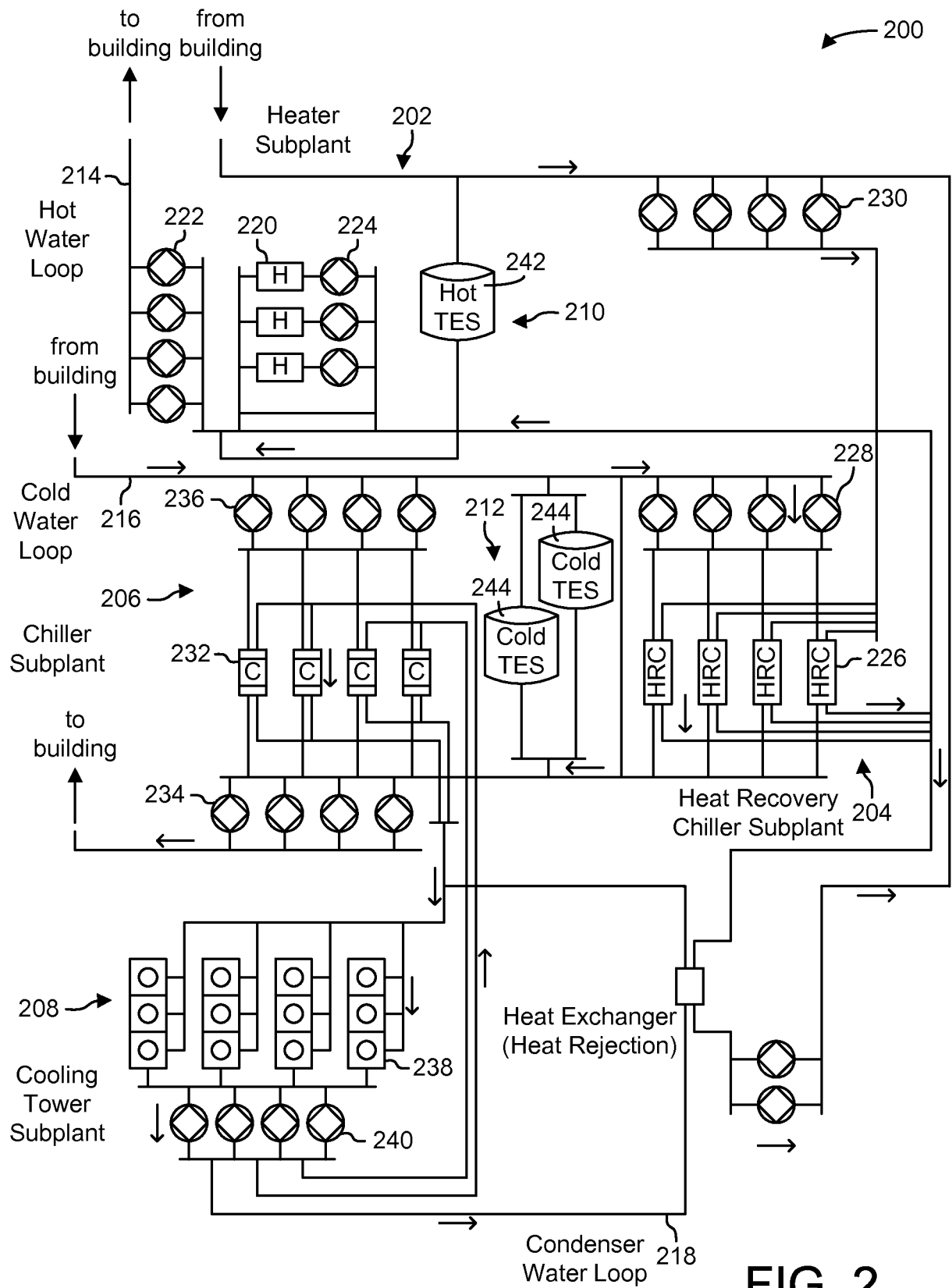


FIG. 2

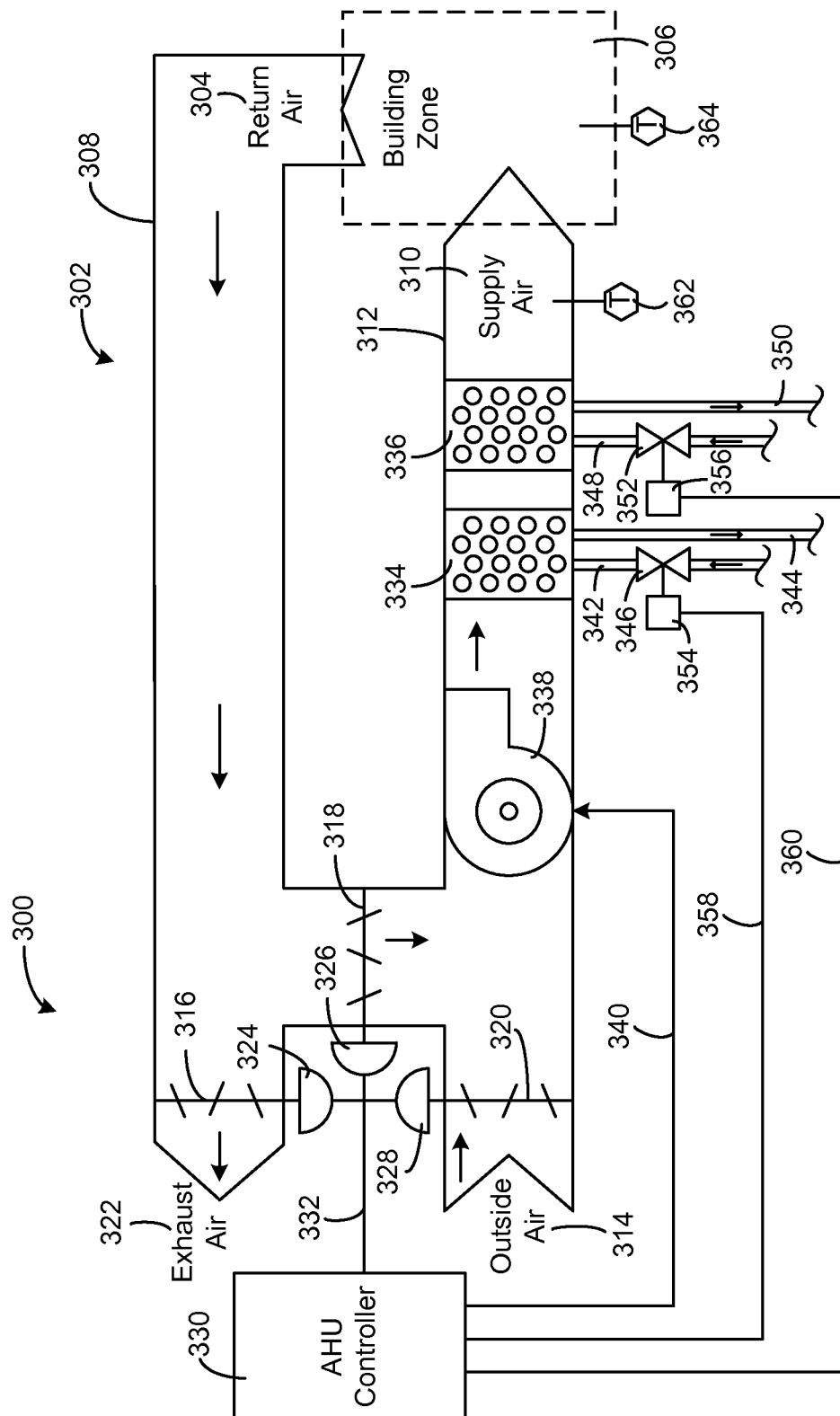


FIG. 3

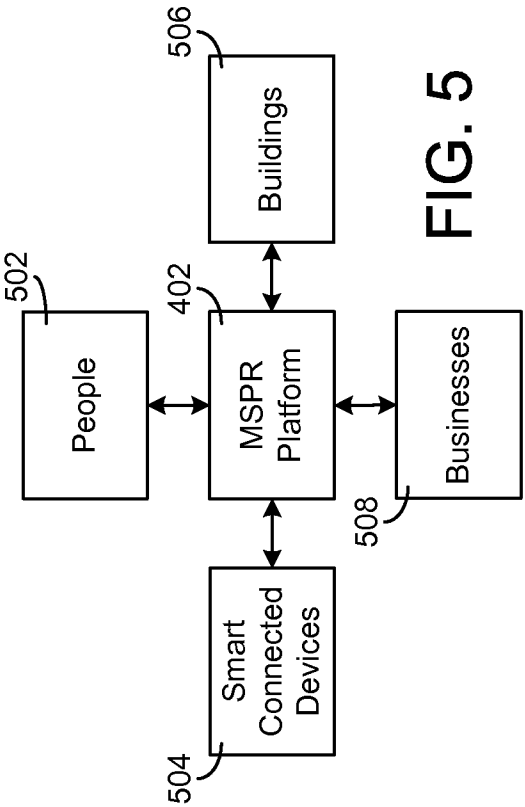


FIG. 5

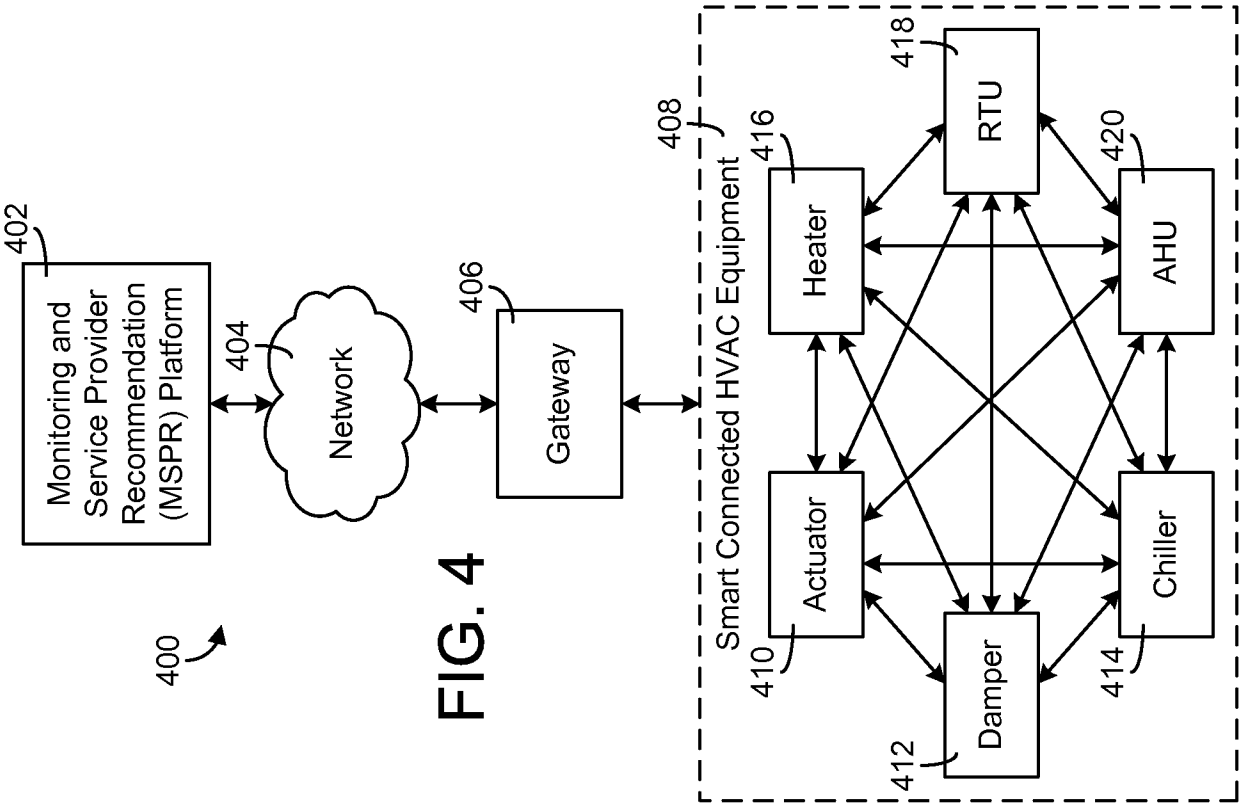


FIG. 4

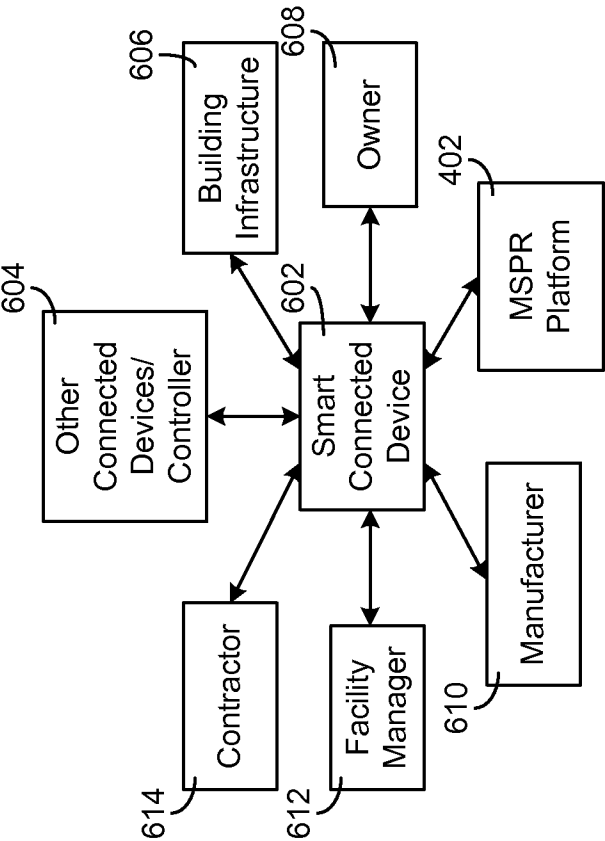


FIG. 6

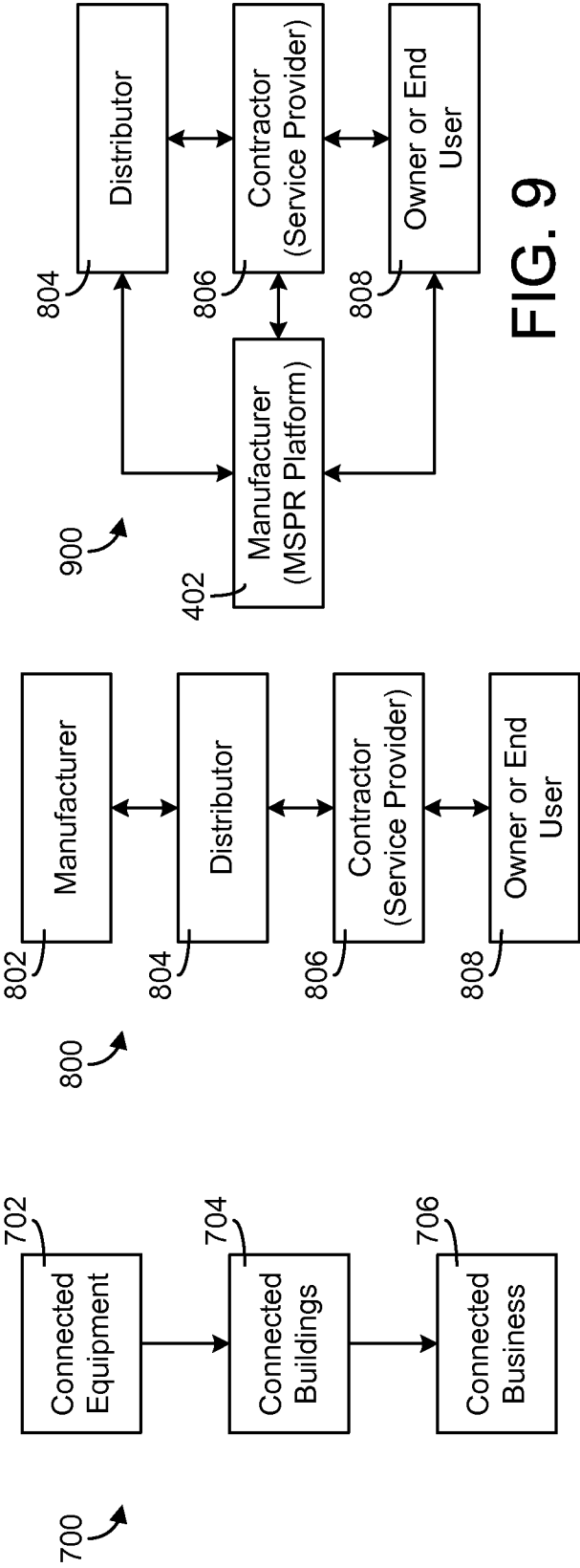


FIG. 9

FIG. 8

FIG. 7

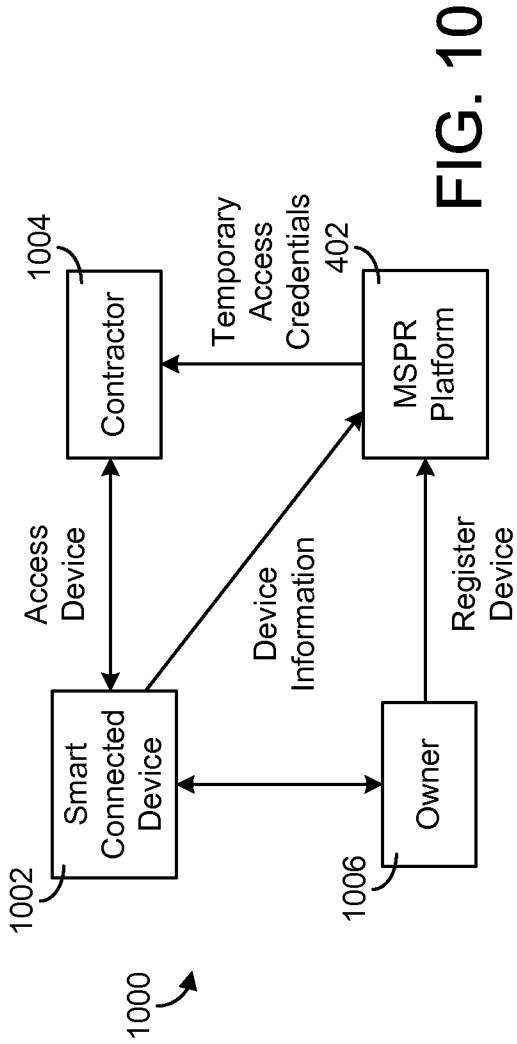
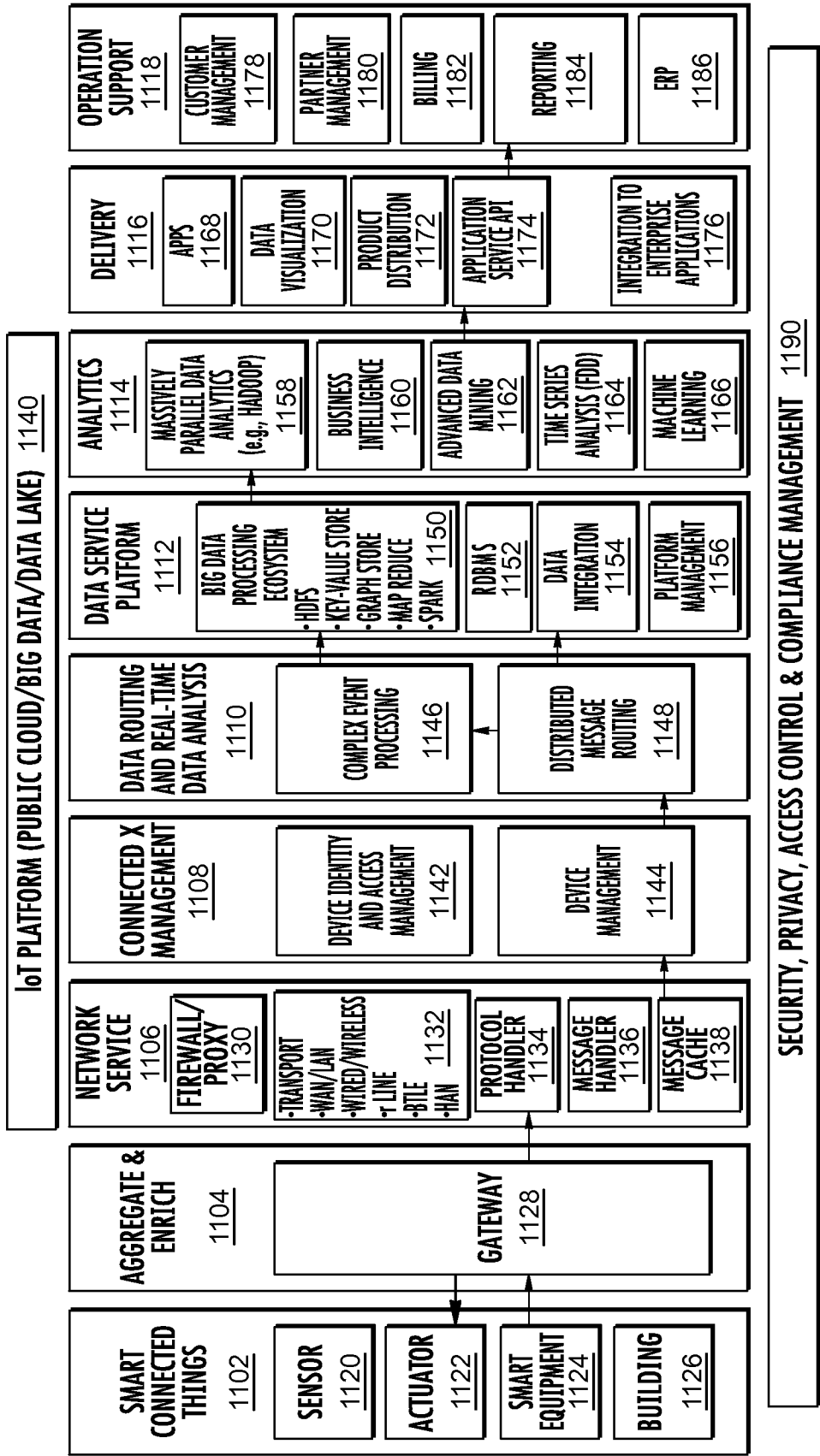


FIG. 10

1100 →



→ :DATA ← :CONTROL

FIG. 11

1200

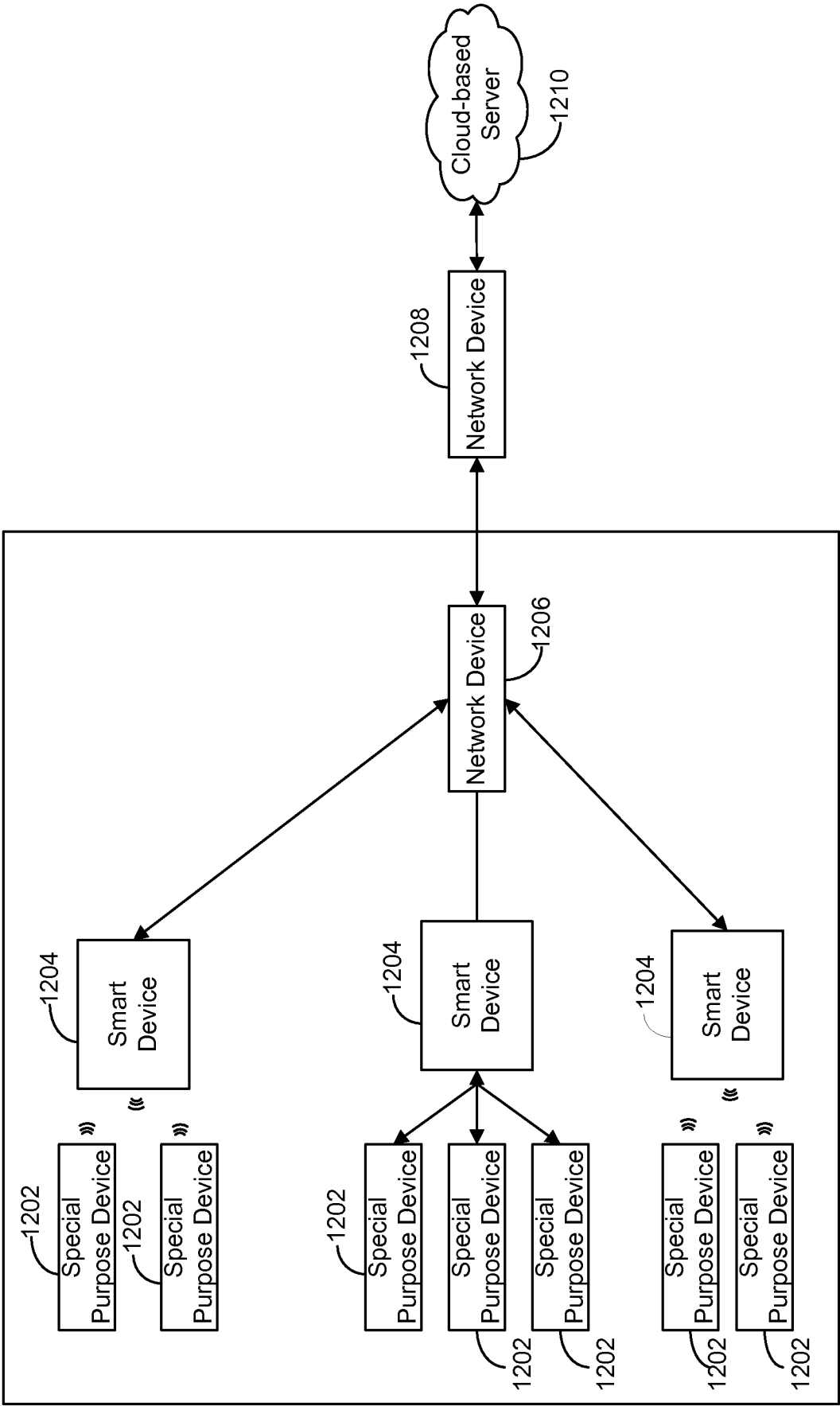


FIG. 12

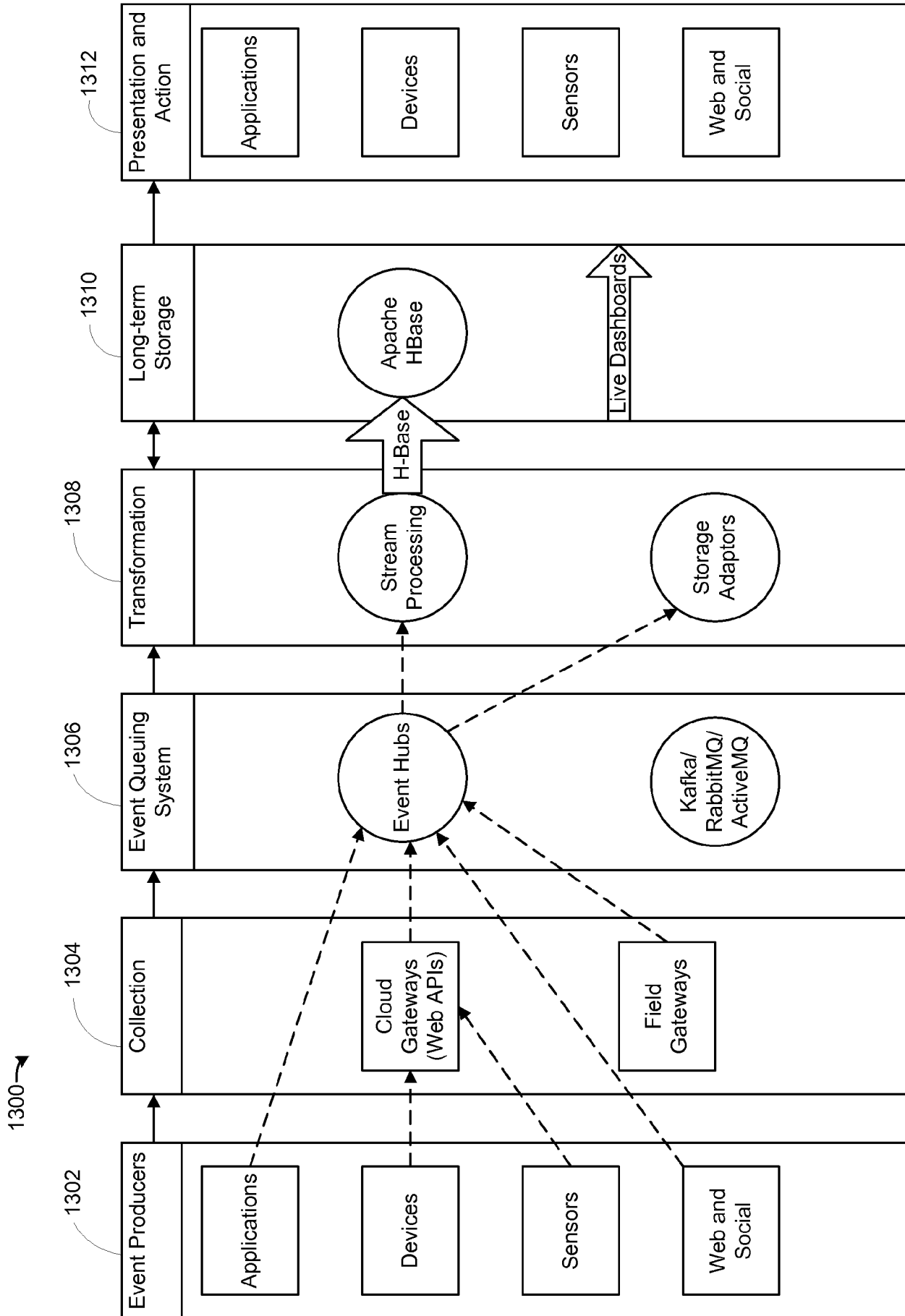
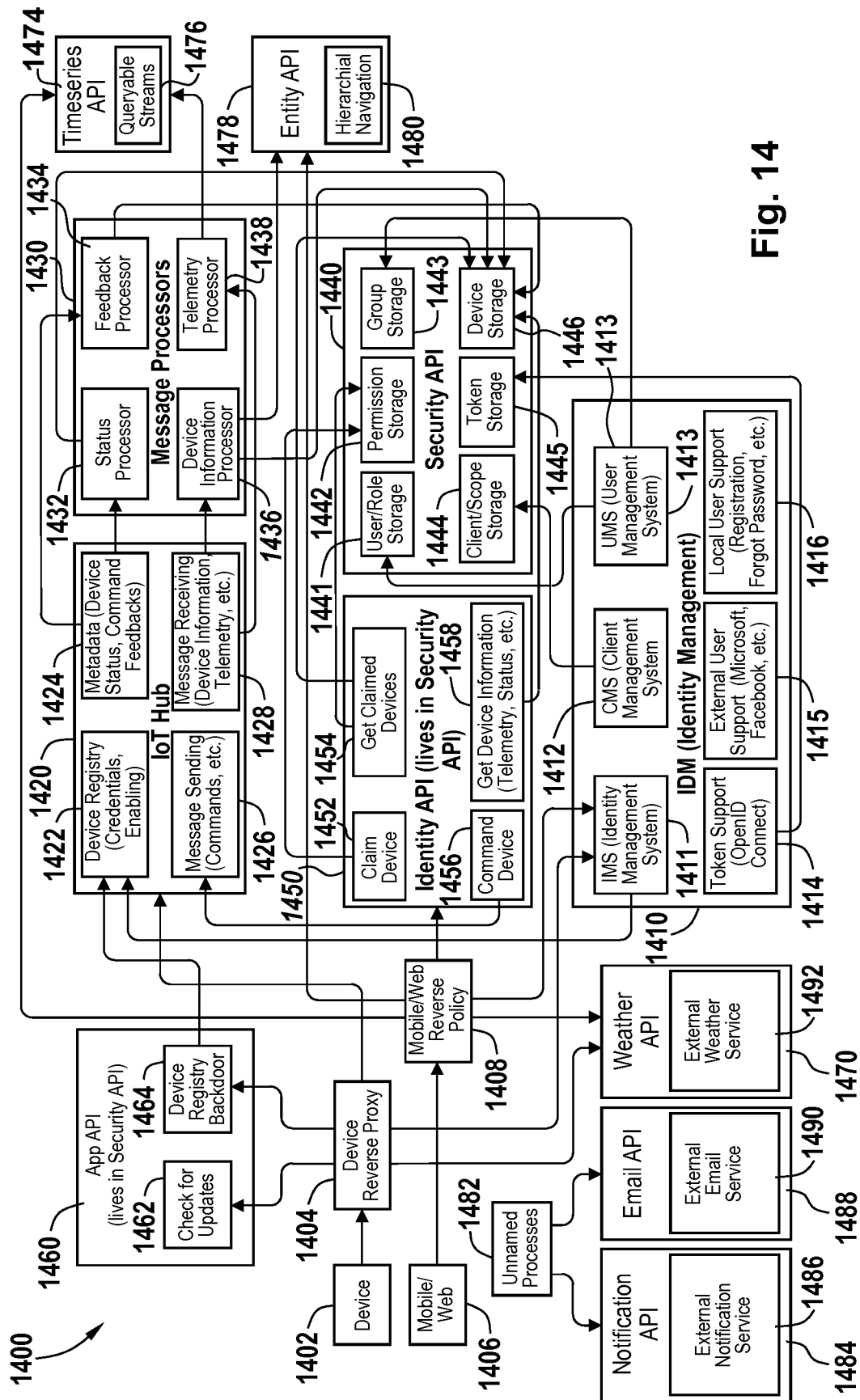
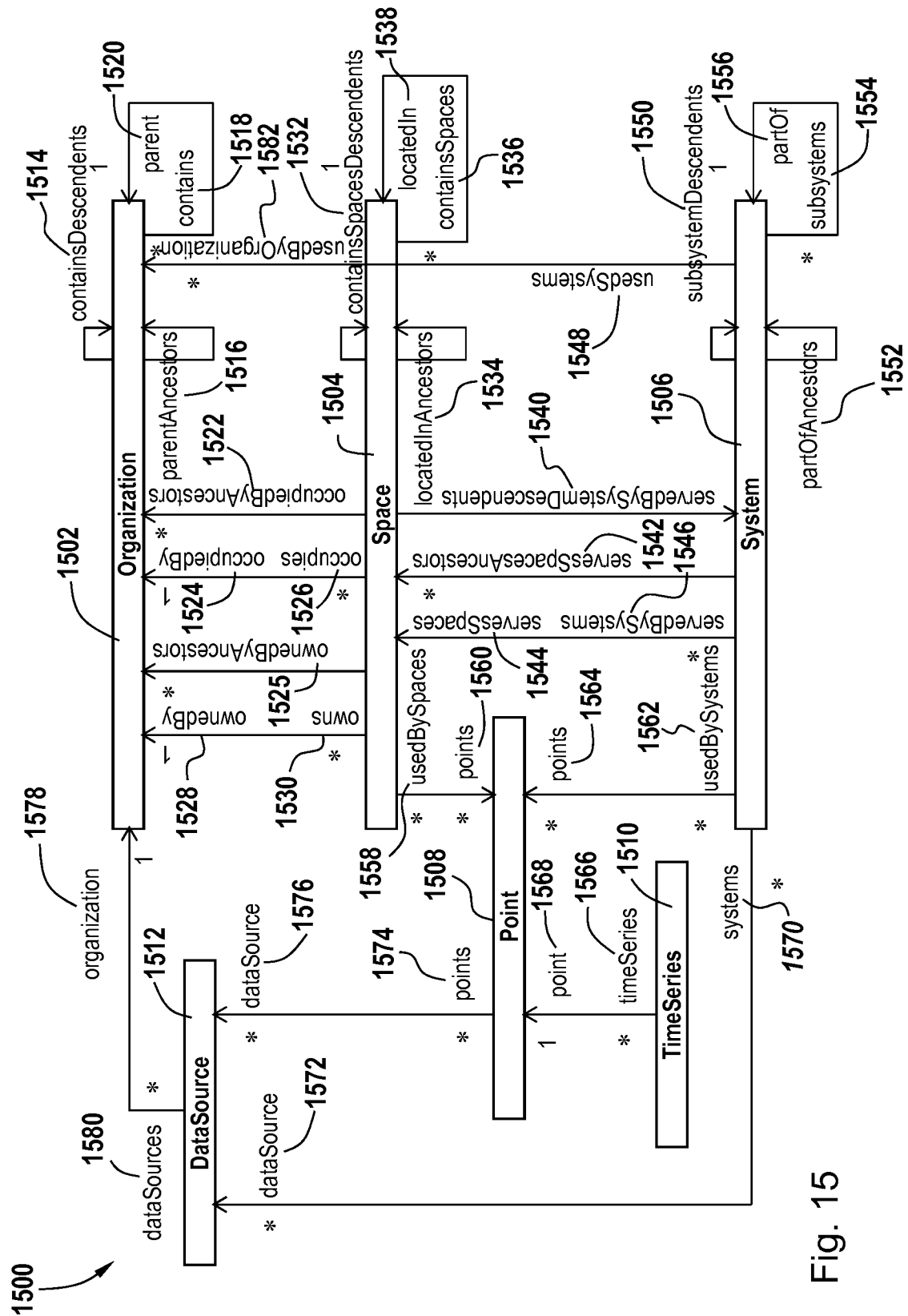


FIG. 13





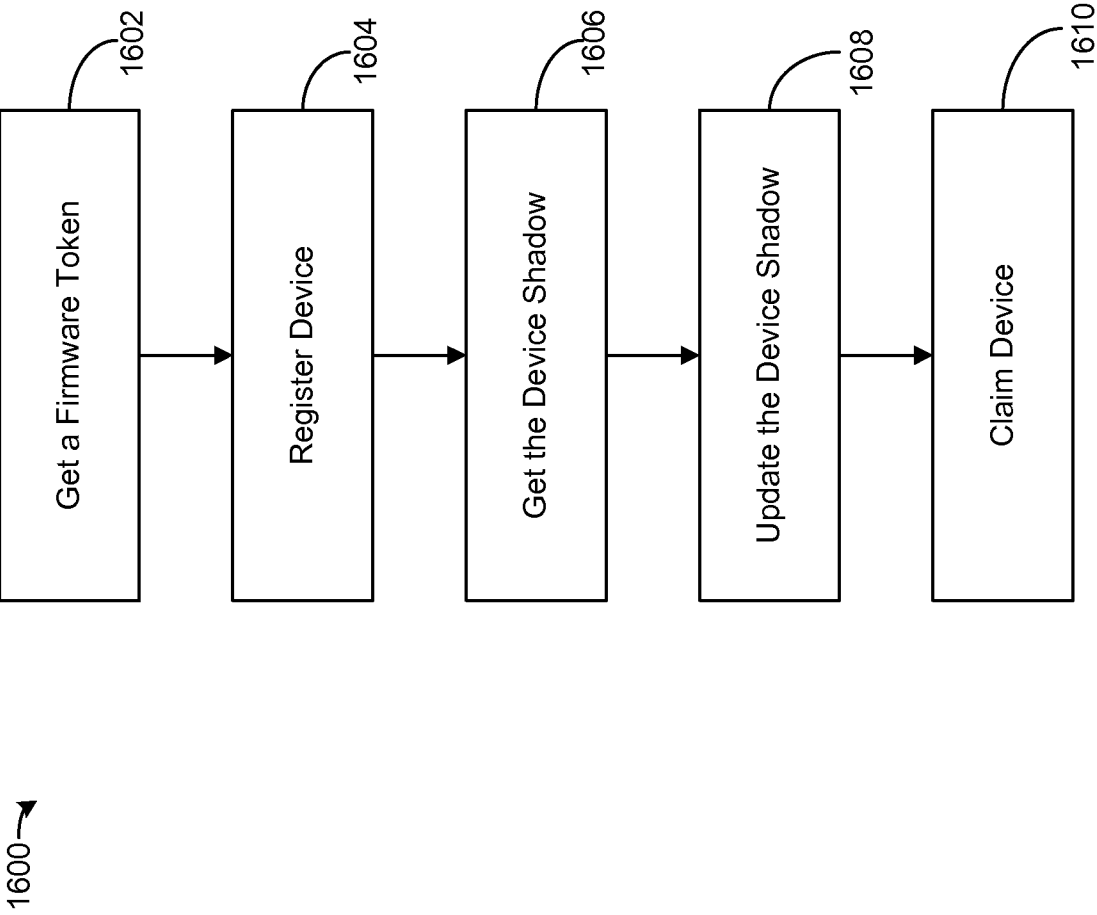


FIG. 16

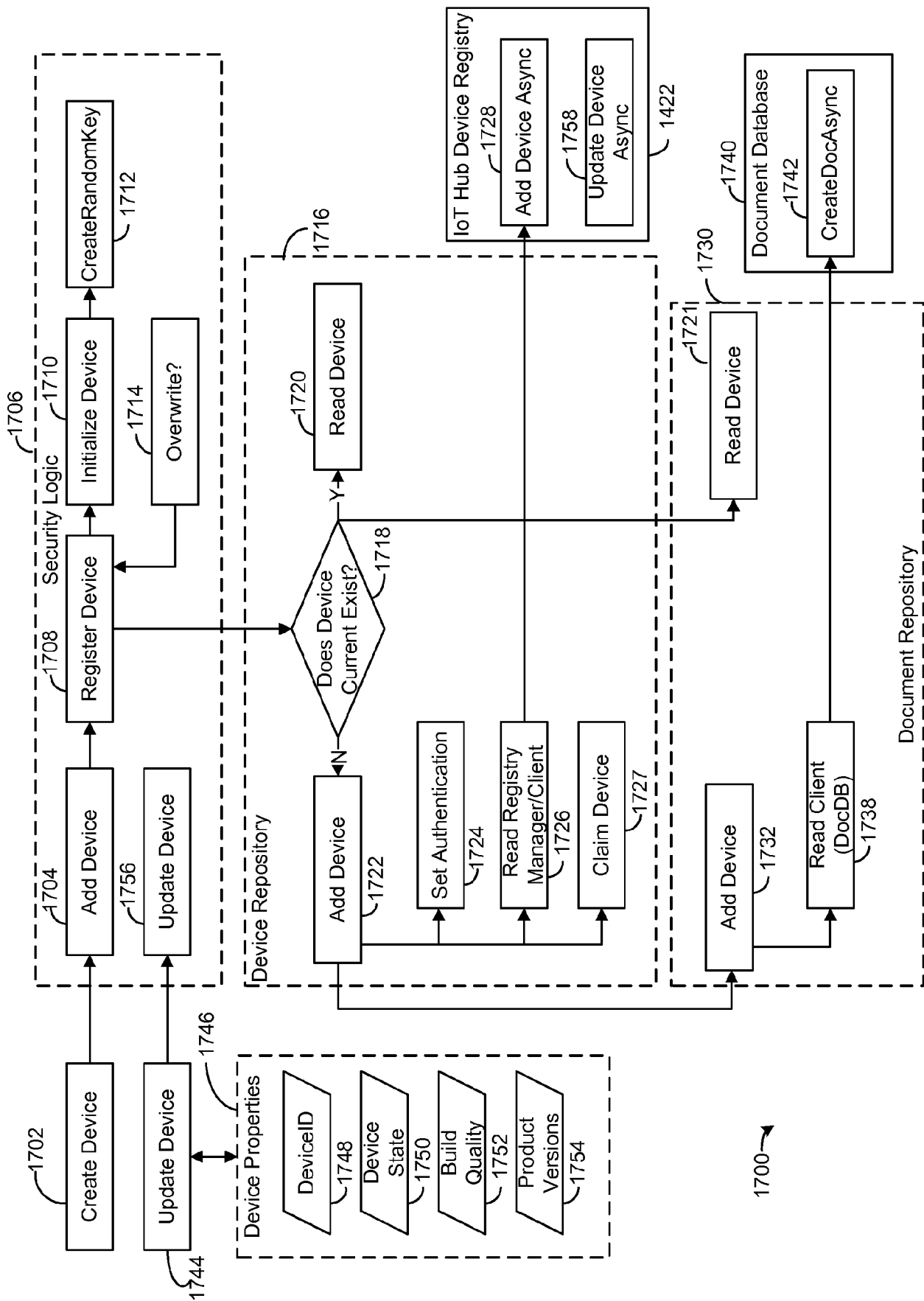


FIG. 17

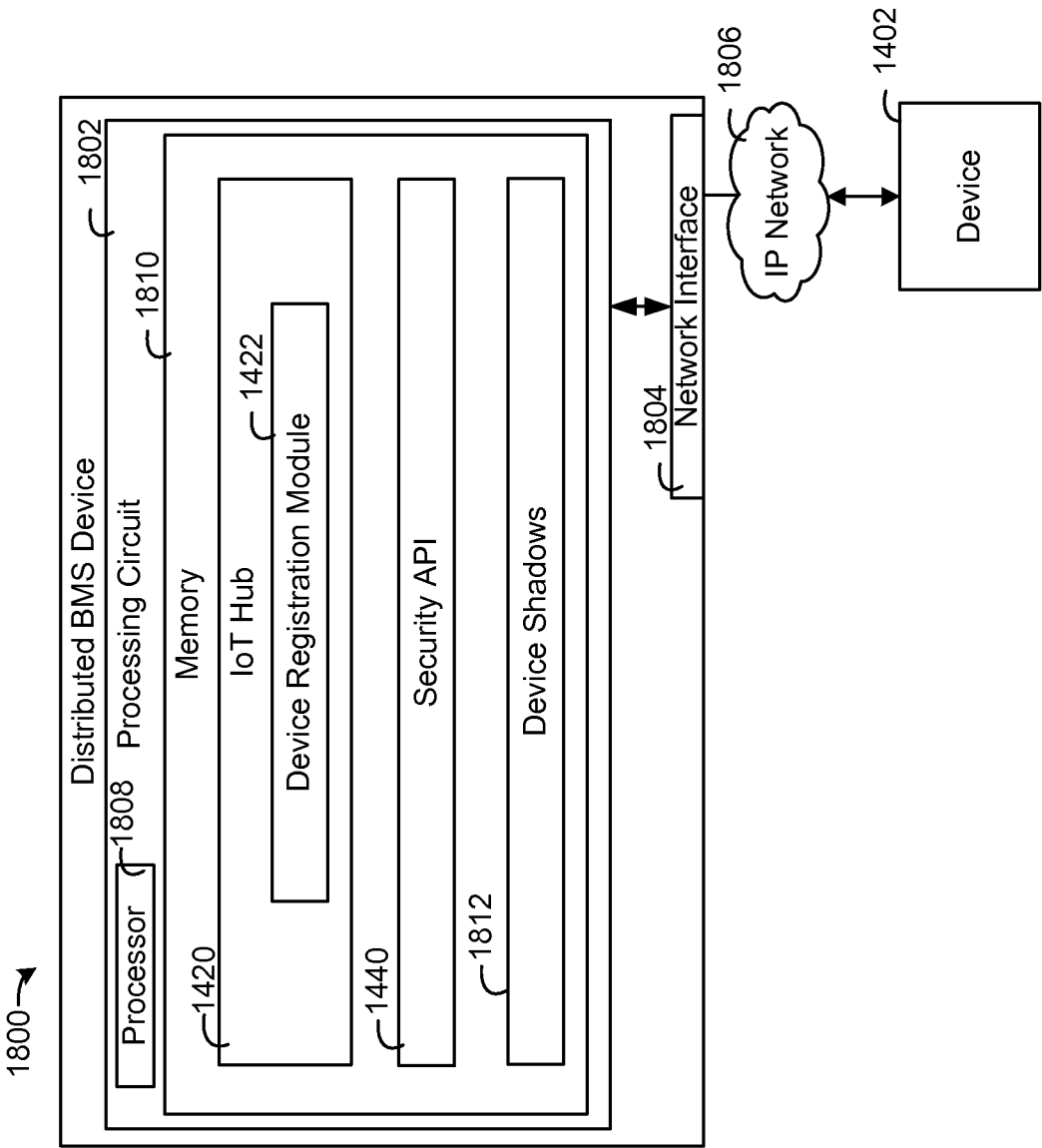


FIG. 18

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2017/025181

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G05B 15/02; F24F 11/00; G05B 1/00; G06K 9/32; G06N 5/04; G06Q 10/06 (2017.01)

CPC - G05B 15/02; G05B 2219/2614; F24F 11/006; G05B 1/00; G05B 2219/23363; G05B 2219/2642; G06F 21/32; G06F 21/34; G06F 21/6218; G06F 2221/2149; G06K 9/3216; G06K 9/3241; G06K 2009/3225; G06K 2009/3291; G06N 5/04; G06Q 10/06313; G06Q 50/08; G07C 9/00166; G08B 7/062; G08B 21/10; G08B 25/005; H04L 12/2803; H04L 63/083; H04L 63/101; H04L 63/20; H04L 67/1068; H04L 67/16; H04W 4/005; H04W 4/008; H04W 4/22; H04W 12/06 (2017.02)

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)

See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

USPC - 340/5.610 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/0237071 A1 (INTERTRUST TECHNOLOGIES CORPORATION) 20 August 2015 (20.08.2015) entire document	1-20
P,X	US 2017/0011318 A1 (JOHNSON CONTROLS TECHNOLOGY COMPANY) 12 January 2017 (12.01.2017) entire document	1-20
A	US 2013/0214902 A1 (PINEAU et al) 22 August 2013 (22.08.2013) entire document	1-20
A	US 2016/0086045 A1 (SCHNEIDER ELECTRIC BUILDINGS, LLC) 24 March 2016 (24.03.2016) entire document	1-20

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"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

20 May 2017

Date of mailing of the international search report

16 JUN 2017

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450
Facsimile No. 571-273-8300

Authorized officer

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774