



(22) **Date de dépôt/Filing Date:** 2014/12/19

(41) **Mise à la disp. pub./Open to Public Insp.:** 2015/04/02

(45) **Date de délivrance/Issue Date:** 2016/08/02

(30) **Priorités/Priorities:** 2014/02/14 (US61/940,003);
2014/07/07 (US62/021,438); 2014/07/30 (US14/446,412);
2014/08/27 (US14/469,931); 2014/10/20 (US14/519,032)

(51) **Cl.Int./Int.Cl.** *H02J 13/00* (2006.01),
G05B 19/00 (2006.01), *H02J 9/00* (2006.01),
H01M 10/42 (2006.01), *H01M 10/48* (2006.01)

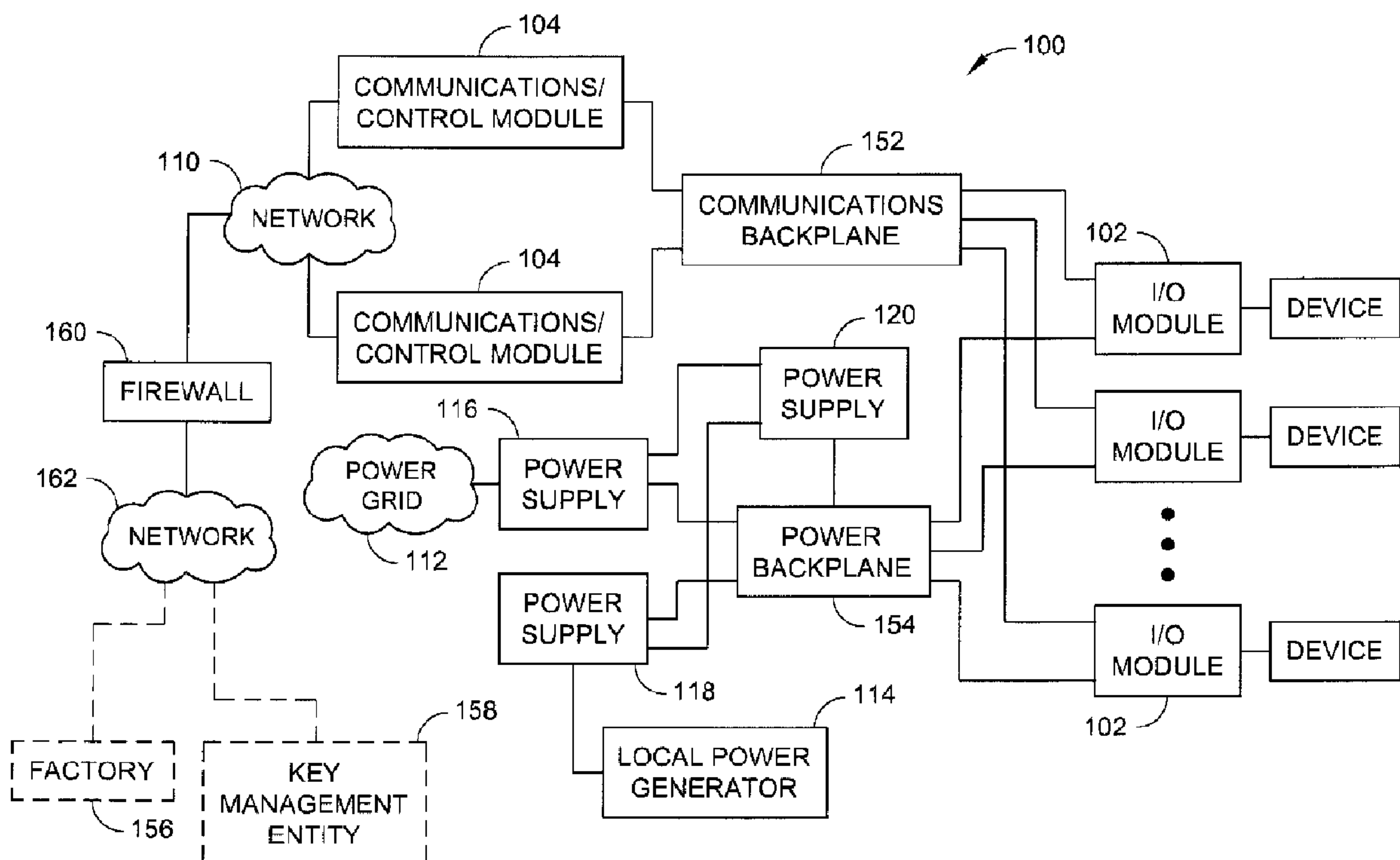
(72) **Inventeurs/Inventors:**
ROOYAKKERS, ALBERT, US;
CALVIN, JAMES G., US;
CRANSHAW, GEORGE, US

(73) **Propriétaire/Owner:**
BEDROCK AUTOMATION PLATFORMS INC., US

(74) **Agent:** BLANEY MCMURTRY LLP

(54) **Titre : SYSTEME D'ALIMENTATION SECURISE POUR UN SYSTEME DE COMMANDE INDUSTRIEL**

(54) **Title: SECURE POWER SUPPLY FOR AN INDUSTRIAL CONTROL SYSTEM**



(57) **Abrégé/Abstract:**

A control system includes an electrical power source and an alternating current (AC) power supply electrically coupled with the electrical power source. An uninterruptable power supply is electrically coupled with the AC power supply for storing and returning electrical energy supplied by the AC power supply. The uninterruptable power supply includes multiple battery modules. Each battery module includes a battery cell and a battery monitor configured to monitor the battery cell. Each battery module also includes a controller operatively coupled with the battery modules. The controller is configured to receive diagnostic information from the battery modules. The uninterruptable power supply can also include one or more authentication modules to participate in an authentication sequence between two or more of a battery module, the controller, a device to be coupled with the uninterruptable power supply, an action originator in the control system, and so forth.



ABSTRACT

A control system includes an electrical power source and an alternating current (AC) power supply electrically coupled with the electrical power source. An uninterruptable power supply is electrically coupled with the AC power supply for storing and returning electrical energy supplied by the AC power supply. The uninterruptable power supply includes multiple battery modules. Each battery module includes a battery cell and a battery monitor configured to monitor the battery cell. Each battery module also includes a controller operatively coupled with the battery modules. The controller is configured to receive diagnostic information from the battery modules. The uninterruptable power supply can also include one or more authentication modules to participate in an authentication sequence between two or more of a battery module, the controller, a device to be coupled with the uninterruptable power supply, an action originator in the control system, and so forth.

SECURE POWER SUPPLY FOR AN INDUSTRIAL CONTROL SYSTEM

BACKGROUND

[0001] Industrial control systems, such as standard industrial control systems (ICS) or programmable automation controllers (PAC), include various types of control equipment used in industrial production, such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLC), and industrial safety systems certified to safety standards such as IEC1508. These systems are used in industries including electrical, water and wastewater, oil and gas production and refining, chemical, food, pharmaceuticals and robotics. Using information collected from various types of sensors to measure process variables, automated and/or operator-driven supervisory commands from the industrial control system can be transmitted to various actuator devices such as control valves, hydraulic actuators, magnetic actuators, electrical switches, motors, solenoids, and the like. These actuator devices collect data from sensors and sensor systems, open and close valves and breakers, regulate valves and motors, monitor the industrial process for alarm conditions, and so forth.

[0002] In other examples, SCADA systems can use open-loop control with process sites that may be widely separated geographically. These systems use Remote Terminal Units (RTUs) to send supervisory data to one or more control centers. SCADA applications that deploy RTU's include fluid pipelines, electrical distribution and large communication systems. DCS systems are generally used for real-time data collection and continuous control with high-bandwidth, low-latency data networks and are used in large campus industrial process plants, such as oil and gas, refining, chemical, pharmaceutical, food and beverage, water and wastewater, pulp and paper, utility power, and mining and metals. PLCs more typically provide Boolean and sequential logic operations, and timers, as well as continuous control and are often used in stand-alone machinery and robotics. Further, ICE and PAC systems can be used in facility processes for buildings, airports, ships, space stations, and the like (e.g., to monitor and control Heating, Ventilation, and Air Conditioning (HVAC) equipment and energy consumption). As industrial control systems evolve, new technologies are combining

aspects of these various types of control systems. For instance, PACs can include aspects of SCADA, DCS, and PLCs.

SUMMARY

[0003] A control system includes an electrical power source and an alternating current (AC) power supply electrically coupled with the electrical power source. An uninterruptable power supply is electrically coupled with the AC power supply for storing and returning electrical energy supplied by the AC power supply. The uninterruptable power supply includes multiple battery modules. Each battery module includes a battery cell and a battery monitor configured to monitor the battery cell. Each battery module also includes a controller operatively coupled with the battery modules. The controller is configured to receive diagnostic information from the battery modules. The control system also includes a control element or subsystem electrically connected to the AC power supply. The uninterruptable power supply is configured to return electrical energy to the AC power supply to power the control element or subsystem when electrical energy supplied by the electrical power source is interrupted. The uninterruptable power supply can also include one or more authentication modules to participate in an authentication sequence between two or more of a battery module, the controller, a device to be coupled with the uninterruptable power supply, an action originator in the control system, and so forth.

[0004] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

DRAWINGS

[0005] The Detailed Description is described with reference to the accompanying figures. The use of the same reference numbers in different instances in the description and the figures may indicate similar or identical items.

[0006] FIG. 1 is a block diagram illustrating a power supply that includes one or more authentication modules in accordance with example embodiments of the present disclosure.

[0007] FIG. 2 is a block diagram illustrating an industrial control system in accordance with example embodiments of the present disclosure.

[0008] FIG. 3 is a block diagram illustrating an industrial control system, such as the industrial control system of FIG. 2, where the industrial control system receives electrical power from multiple sources, such as a power grid and one or more local power generators, and where one or more backup power supplies are configured to store and return electrical energy using multiple battery modules in accordance with example embodiments of the present disclosure.

[0009] FIG. 4 is a block diagram illustrating a backup power supply configured to communicatively couple with a system, such as the industrial control system of FIG. 2, and configured to connect to an electrical power source (e.g., the power grid and/or local power generator of FIG. 2) to store and return electrical energy, where the backup power supply includes a controller and multiple battery modules, and each battery module has a battery monitor communicatively coupled with the controller in accordance with example embodiments of the present disclosure.

[0010] FIG. 5 is a block diagram illustrating a backup power supply, such as the backup power supply illustrated in FIG. 4, where the backup power supply is configured to communicatively couple with a system, such as the industrial control system of FIG. 2, and where the backup power supply includes a controller configured to provide the system with information regarding the status of multiple battery modules included with the backup power supply in accordance with example embodiments of the present disclosure.

[0011] FIG. 6 is a diagrammatic illustration of a secure control system that authenticates devices, such as the power supply illustrated in FIG. 1 and/or other devices, such as powered devices connected to the power supply illustrated in FIG. 1, in accordance with example embodiments of the present disclosure.

[0012] FIG. 7 is a block diagram illustrating an action authentication path for an industrial control system, such as the secure control system of FIG. 6, in accordance with example embodiments of the present disclosure.

[0013] FIG. 8 is a block diagram further illustrating the action authentication path of FIG. 7 in accordance with example embodiments of the present disclosure.

[0014] FIG. 9 is a flow diagram illustrating a method for authenticating an action request in accordance with example embodiments of the present disclosure.

DETAILED DESCRIPTION

Overview

[0015] In industrial control system settings, power is typically supplied to automation equipment such as controllers, input/output (I/O) modules, and so forth from a power grid (e.g., using high voltage power from AC mains), using local power generation (e.g., using on-site turbines and/or diesel power generators), and so on. Often, backup power is also supplied to automation equipment in these settings from batteries. For example, large scale battery storage can be provided in an industrial setting using, for instance, lead-acid batteries. Power from large scale battery storage can be supplied using centralized, alternating current (AC) power transmission techniques. In other examples, smaller, decentralized direct current (DC) battery supplies are used. For instance, backup battery power is supplied by smaller lead-acid batteries at the level of cabinets, controllers, I/O modules, and so forth. However, lead-acid batteries have a comparatively low energy density when compared to newer rechargeable battery technologies, such as lithium-ion batteries. Further, in these configurations, the backup batteries are generally separate from control hardware, requiring separate connections to each battery to monitor battery status. For example, backup batteries in industrial automation settings are typically connected to spare I/O ports of control hardware to monitor the activity (e.g., on/off status) of such batteries.

[0016] Systems and techniques are described herein that facilitate monitoring and/or control of battery supplies in industrial control system settings, such as uninterruptable power supply (UPS) equipment. The techniques and systems described can be

implemented using higher energy density rechargeable battery technologies, such as lithium-ion rechargeable battery technologies. In embodiments of the disclosure, an industrial UPS furnishes communications and/or security features, such as bidirectional system communications, control system integration, cyber security integration, and so on. For example, an industrial UPS provides status information, diagnostic information, reliability information, bidirectional communications, and so forth. In some embodiments, an industrial UPS implements key encryption microcontroller techniques.

[0017] In some embodiments, a power supply includes circuitry (e.g., a printed circuit board (PCB), an integrated circuit (IC) chip, and/or other circuitry) that can perform an authentication of the power supply and/or a device connected to the power supply. This can prevent or minimize the potential for plugging a power supply into a device not intended to be used with that particular power supply or type of power supply (e.g., preventing or minimizing the possibility that a low voltage power supply is plugged into a high voltage device). For example, the power supply performs a “handshake” operation with a coupled module to verify that the power supply is mated with an appropriate and/or desired device. In some embodiments, an indicator, such as a light emitting diode (LED) indicator light, is used to provide notification of this authentication. For instance, a multi-colored LED and/or a single color LED provides diagnostic information to indicate the status of an authentication (e.g., using a solid glow, no glow, blinking, one color for one state and another color for another state, etc.).

[0018] In some embodiments, the power supply can be used to authenticate another device, such as an instrument that receives power from the power supply. For instance, power supply circuitry can be used to authenticate a powered device, a type of powered device, the manufacturer of a powered device, and so on. In this manner, the use of counterfeit equipment in an industrial automation setting can be prevented or minimized. Further, the power supply can be used to authenticate itself to equipment, such as controllers, input/output (I/O) modules, end devices, field devices (e.g., process sensors and/or actuators), and so forth. In some embodiments, the power supply facilitates cryptographic communication between the power supply and a device connected to the

power supply. For example, a power supply can provide bi-directional cryptographic communications between the power supply and end devices, field devices, and so on. Further, in some embodiments, an operator can use a power supply connected to a network to obtain authentication information about a field device, such as a sensor, actuator or any other instrument. In some embodiments, two or more authentication modules (e.g., a first authentication module and a second authentication module) are configured to perform an authentication sequence (e.g., a “handshake”) when a new device is installed, at startup/reset, periodically, at scheduled times, and/or other predefined events. Should the authentication modules fail to authenticate another device and/or one another, at least one of the devices (e.g., the unauthenticated device) can be partially or completely disabled and/or restricted from communicating with other devices.

[0019] In industrial control systems, various industrial elements/subsystems (e.g., input/output modules, power modules, field devices, switches, workstations, and/or physical interconnect devices) are controlled or driven by control elements/subsystems (e.g., one or more communications/control modules). The control elements/subsystems operate according to programming and action requests (e.g., executable software modules, control commands, data requests, and the like) received from an action originator, such as, but not necessarily limited to: an operator interface (e.g., a SCADA or human machine interface (HMI)), an engineering interface, a local application, a remote application, and so on. Where multiple action originators are present, the industrial control system can be vulnerable to unauthorized access to data and/or controls. Further, the industrial control system may be vulnerable to malware, spyware, or other corrupt/malicious software that can be transmitted in the form of an update, application image, control command, or the like. Simply authenticating the operator may not be enough to secure the system from malicious actors or even unintentionally unauthorized requests/commands that can be originated via a valid login or a seemingly valid (e.g., hacked) application or operator/engineering interface.

[0020] The present disclosure is directed to controllers, systems, and techniques for preventing unauthorized action requests from being processed in an industrial control

system. A predefined selection of operations or all operator actions and/or other control actions or requests can be secured via an authentication path from an action originator to an industrial element/controller (e.g., communications/control module, input/output (I/O) module, power module, field device, switch, workstation, physical interconnect device, or the like). In implementations, the industrial control system requires an action authenticator to sign an action request generated by the action originator. Unsigned action requests may automatically result in an error and will not be processed or executed by the industrial element/controller. The industrial element/controller can be configured to receive the signed action request, verify the authenticity of the signed action request, and perform a requested action when the authenticity of the signed action request is verified. In this manner, malicious or otherwise unauthorized action requests are not processed, and thus the system can be protected from malware, spyware, unauthorized changes of control parameters, unauthorized access to data, and so forth.

Example Implementations

[0021] Referring generally to FIGS. 1 through 6, example power supplies 120 are described in accordance with the present disclosure. In some embodiments, a power supply 120 includes one or more authentication modules 134 configured to authenticate the power supply 120 and/or one or more battery modules 122 of the power supply 120 to a device connected to the power supply 120, such as an I/O module 102, a control module 104, and so forth (e.g., as illustrated in FIG. 1). The authentication module 134 can also be used to authenticate one or more devices connected to the power supply 120. In some embodiments, the authentication module 134 stores a unique identifier 136 and/or a security credential 138 associated with the power supply 120 (e.g., as shown in FIG. 5, where an authentication module is implemented using a controller 128 including a processor 140 and a memory 142 that stores one or more unique identifiers 136 and/or security credentials 138). The authentication module 134 can be configured to establish and/or prevent connection to devices connected to the power supply 120 based upon the authentication. The power supply 120 can also include an indicator (e.g., an indicator light 144) to indicate the authentication (e.g., to an operator).

[0022] In some embodiments, the power supply 120 includes an alert module 146. In embodiments of the disclosure, the alert module 146 is configured to provide an alert (e.g., to an operator) when a condition and/or set of conditions is met for the power supply 120 and/or a device connected to the power supply 120. For example, an alert is generated by an authentication module 134 and provided by an alert module 146 when authentication of the power supply 120 and/or a device connected to the power supply is obtained and/or fails. For example, a power supply 120 performs a “handshake” operation with a coupled powered device (e.g., an I/O module 102 and/or a control module 104) to verify that the power supply 120 is mated with an appropriate and/or desired device. If not, the alert module 146 can be used to alert an operator (e.g., via a network). In some embodiments, an alert is provided to an operator in the form of an email. In other embodiments, an alert is provided to an operator in the form of a text message. However, these alerts are provided by way of example and are not meant to limit the present disclosure. In other embodiments, different alerts are provided to an operator. Further, multiple alerts can be provided to an operator when a condition is met for an authentication procedure (e.g., an email and a text message, and so forth). It should also be noted that alerts can be provided by an authentication module 134 and/or an alert module 146 for other conditions, including, but not necessarily limited to: power supply failure, battery module failure, connected device failure, various error conditions for a power supply and/or a powered device, and so forth.

[0023] The authentication module 134 can also be configured to encrypt communication between the power supply 120 and one or more devices connected to the power supply 120. As shown in FIG. 1, a power supply 120 can include an encryption module 148. For example, one or more cryptographic protocols are used to transmit information between the power supply 120 and a powered device. Examples of such cryptographic protocols include, but are not necessarily limited to: a transport layer security (TLS) protocol, a secure sockets layer (SSL) protocol, and so forth. For instance, communications between a power supply 120 and a powered device can use HTTP secure (HTTPS) protocol, where HTTP protocol is layered on SSL and/or TLS protocol.

[0024] In some embodiments, an authentication sequence can be performed between a power supply 120 and a device connected to the power supply 120. For example, the power supply 120 authenticates a coupled I/O device 102, a control module 104, and so forth, by performing an authentication sequence using the authentication module 134 of the controller 128. In other embodiments, a device connected to the power supply 120 can authenticate the power supply 120. For instance, a control module 104 authenticates a coupled power supply 120 by performing an authentication sequence with the authentication module 134 of the controller 128. In further embodiments, one power supply 120 can authenticate another power supply 120. For example, a first power supply 120 authenticates a second (e.g., redundant) power supply 120 by performing an authentication sequence between a first authentication module 134 of the controller 128 of the first power supply 120 and a second authentication module 134 of the controller 128 of the second power supply 120. In some embodiments, the second power supply 120 can also authenticate the first power supply 120.

[0025] It should be noted that while the processor 140 and memory 142 are described with some specificity as part of the controller 128 (e.g., with reference to FIG. 1), this configuration is provided by way of example and is not meant to limit the present disclosure. Thus, one or more of the battery modules 122 can also include a processor, a memory, and so forth (e.g., in addition to or in place of the processor 140 and memory 142 included with the controller 128). In such embodiments, one or more of the battery modules 122 can include one or more authentication modules 122, e.g., where an authentication module 134 employs a processor and a memory (possibly storing one or more keys, certificates, unique identifiers, security credentials, and so on) to authenticate the battery modules 122 to one or more other devices (e.g., other battery modules 122, the controller 128, control elements or subsystems, and so forth) and/or to authenticate other devices (e.g., other battery modules 122, the controller 128, control elements or subsystems, and so on) coupled with the power supply 120.

[0026] In some embodiments, a battery module 122 can authenticate the controller 128 of the power supply 120 and/or a connected device, such as a powered device coupled with

the power supply 120. For example, the battery module 122 authenticates the controller 128 of a power supply 120 and/or a coupled I/O device 102, a control module 104, and so forth, by performing an authentication sequence using an authentication module 134 of the battery module 122. In other embodiments, a powered device connected to a power supply 120 can authenticate one or more of the battery modules 122. For instance, a control module 104 authenticates one or more (e.g., each) battery module 122 of a connected power supply 120 by performing an authentication sequence with the authentication module 134 of the respective battery modules 122.

[0027] In some embodiments, the controller 128 can authenticate one or more of the battery modules 122. For example, the controller 128 authenticates one or more battery modules 122 by performing an authentication sequence between the authentication module 134 of the controller 128 and authentication modules 134 of respective battery modules 122. In further embodiments, one battery module 122 can authenticate another battery module 122. For example, a first battery module 122 authenticates a second battery module 122 by performing an authentication sequence between a first authentication module 134 of the first battery module 122 and a second authentication module 134 of the second battery module 122. In some embodiments, the second battery module 122 can also authenticate the first battery module 122.

[0028] The power supply 120 can be used with an industrial control system. For example, with reference to FIG. 2, an example industrial control system 100 is described in accordance with the present disclosure. In embodiments, the industrial control system 100 may comprise an industrial control system (ICS), a programmable automation controller (PAC), a supervisory control and data acquisition (SCADA) system, a distributed control system (DCS), programmable logic controller (PLC), and industrial safety system certified to safety standards such as IEC1508, or the like. The industrial control system 100 uses a communications control architecture to implement a distributed control system that includes control elements or subsystems, where the subsystems are controlled by one or more controllers distributed throughout the system. For example, one or more I/O modules 102 are connected to one or more control modules 104. The

industrial control system 100 is configured to transmit data to and from the I/O modules 102. The I/O modules 102 can comprise input modules, output modules, and/or input and output modules. For instance, input modules can be used to receive information from input sensors in the process, while output modules can be used to transmit instructions to output actuators. For example, an I/O module 104 can be connected to a process sensor 106 (e.g., illumination, radiation, gas, temperature, electrical, magnetic, and/or acoustic sensor) for measuring pressure in piping for a gas plant, a refinery, and so forth and/or connected to a process actuators 108 (e.g., control valve, hydraulic actuator, magnetic actuator, motor, solenoid, electrical switch, transmitter, or the like).

[0029] In implementations, the I/O modules 102 can be used to control systems and collect data in applications including, but not necessarily limited to: industrial processes, such as manufacturing, production, power generation, fabrication, and refining; infrastructure processes, such as water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, and large communication systems; facility processes for buildings, airports, ships, and space stations (e.g., to monitor and control Heating, Ventilation, and Air Conditioning (HVAC) equipment and energy consumption); large campus industrial process plants, such as oil and gas, refining, chemical, pharmaceutical, food and beverage, water and wastewater, pulp and paper, utility power, mining, metals; and/or critical infrastructures.

[0030] In implementations, an I/O module 102 can be configured to convert analog data received from the sensor 106 to digital data (e.g., using Analog-to-Digital Converter (ADC) circuitry, and so forth). An I/O module 102 can also be connected to an actuator 108 and configured to control one or more operating characteristics of the actuator 108, such as speed, torque, and so forth. Further, the I/O module 102 can be configured to convert digital data to analog data for transmission to the actuator 108 (e.g., using Digital-to-Analog (DAC) circuitry, and so forth). In implementations, one or more of the I/O modules 102 can comprise a communications module configured for communicating via a communications sub-bus, such as an Ethernet bus, an H1 field bus, a Process Field

Bus (PROFIBUS), a Highway Addressable Remote Transducer (HART) bus, a Modbus, and so forth. Further, two or more I/O modules 102 can be used to provide fault tolerant and redundant connections for a communications sub-bus.

[0031] Each I/O module 102 can be provided with a unique identifier (ID) for distinguishing one I/O module 102 from another I/O module 102. In implementations, an I/O module 102 is identified by its ID when it is connected to the industrial control system 100. Multiple I/O modules 102 can be used with the industrial control system 100 to provide redundancy. For example, two or more I/O modules 102 can be connected to the sensor 106 and/or the actuator 108. Each I/O module 102 can include one or more ports that furnish a physical connection to hardware and circuitry included with the I/O module 102, such as a printed circuit board (PCB), and so forth.

[0032] One or more of the I/O modules 102 can include an interface for connecting to other networks including, but not necessarily limited to: a wide-area cellular telephone network, such as a 3G cellular network, a 4G cellular network, or a Global System for Mobile communications (GSM) network; a wireless computer communications network, such as a Wi-Fi network (e.g., a Wireless LAN (WLAN) operated using IEEE 802.11 network standards); a Personal Area Network (PAN) (e.g., a Wireless PAN (WPAN) operated using IEEE 802.15 network standards); a Wide Area Network (WAN); an intranet; an extranet; an internet; the Internet; and so on. Further, one or more of the I/O modules 102 can include a connection for connecting an I/O module 102 to a computer bus, and so forth.

[0033] The control modules 104 can be used to monitor and control the I/O modules 102, and to connect two or more I/O modules 102 together. In embodiments of the disclosure, a control module 104 can update a routing table when an I/O module 102 is connected to the industrial control system 100 based upon a unique ID for the I/O module 102. Further, when multiple redundant I/O modules 102 are used, each control module 104 can implement mirroring of informational databases regarding the I/O modules 102 and update them as data is received from and/or transmitted to the I/O modules 102. In some

implementations, two or more control modules 104 are used to provide redundancy. For added security, the control modules 104 can be configured to perform an authentication sequence or handshake to authenticate one another at predefined events or times including, but not necessarily limited to: startup, reset, installation of a new control module 104, replacement of a control module 104, periodically, scheduled times, and so forth. Further, the control modules 104 can be configured to perform an authentication at random (e.g., pseudorandom) time intervals.

[0034] Data transmitted by the industrial control system 100 can be packetized, i.e., discrete portions of the data can be converted into data packets comprising the data portions along with network control information, and so forth. The industrial control system 100 can use one or more protocols for data transmission, including a bit-oriented synchronous data link layer protocol such as High-Level Data Link Control (HDLC). In some embodiments, the industrial control system 100 implements HDLC according to an International Organization for Standardization (ISO) 13239 standard, or the like. Further, two or more control modules 104 can be used to implement redundant HDLC. However, it should be noted that HDLC is provided by way of example only and is not meant to be restrictive of the present disclosure. Thus, the industrial control system 100 can use other various communications protocols in accordance with the present disclosure.

[0035] One or more of the control modules 104 can be configured for exchanging information with components used for monitoring and/or controlling the instrumentation connected to the industrial control system 100 via the I/O modules 102, such as one or more control loop feedback mechanisms/controllers. In implementations, a controller can be configured as a microcontroller/Programmable Logic Controller (PLC), a Proportional-Integral-Derivative (PID) controller, and so forth. In embodiments of the disclosure, the I/O modules 102 and the control modules 104 include network interfaces, e.g., for connecting one or more I/O modules 102 to one or more controllers via a network 110. In implementations, a network interface can be configured as a Gigabit Ethernet interface for connecting the I/O modules 102 to a Local Area Network (LAN).

Further, two or more control modules 104 can be used to implement redundant Gigabit Ethernet.

[0036] However, it should be noted that Gigabit Ethernet is provided by way of example only and is not meant to be restrictive of the present disclosure. Thus, a network interface can be configured for connecting the control modules 104 to other various networks including, but not necessarily limited to: a wide-area cellular telephone network, such as a 3G cellular network, a 4G cellular network, or a GSM network; a wireless computer communications network, such as a Wi-Fi network (e.g., a WLAN operated using IEEE 802.11 network standards); a PAN (e.g., a WPAN operated using IEEE 802.15 network standards); a WAN; an intranet; an extranet; an internet; the Internet; and so on. Additionally, a network interface can be implemented using a computer bus. For example, a network interface can include a Peripheral Component Interconnect (PCI) card interface, such as a Mini PCI interface, and so forth. Further, the network 110 can be configured to include a single network or multiple networks across different access points.

[0037] Referring now to FIG. 3, the industrial control system 100 can receive electrical power from multiple sources. For example, AC power is supplied from a power grid 112 (e.g., using high voltage power from AC mains). AC power can also be supplied using local power generation (e.g., an on-site turbine or diesel local power generator 114). A power supply 116 is used to distribute electrical power from the power grid 112 to automation equipment of the industrial control system 100, such as controllers, I/O modules, and so forth. Another power supply 118 is used to distribute electrical power from the local power generator 114 to the automation equipment. The industrial control system 100 also includes an additional (backup) power supply 120 configured to store and return DC power using multiple battery modules 122. For example, the power supply 120 functions as a UPS. In embodiments of the disclosure, multiple power supplies 116, 118, and/or 120 are distributed (e.g., physically decentralized) within the industrial control system 100.

[0038] In some embodiments, one or more power supplies 116, 118, and/or 120 are provided at the level of a cabinet. For example, one power supply 120 is used to provide backup power to a control module 104 and its associated I/O modules 102. In other embodiments, one power supply 120 is used to provide backup power to a control module 104, and another power supply 120 is used to provide backup power to an associated I/O module 102 (e.g., where the I/O module 102 and the control module 104 are physically separated by some distance within a facility, where electrical isolation is maintained between the I/O module 102 and the control module 104, and so forth).

[0039] The power supplies 116, 118, and/or 120 can also be configured to power field devices, such as the sensor 106 and/or the actuator 108 described with reference to FIG. 2. For example, one or more of the power supplies 116 and 118 includes an AC-to-DC (AC/DC) converter for converting AC (e.g., as supplied by AC mains) to DC for transmission to the actuator 108 (e.g., in an implementation where the actuator 108 is a DC motor or other DC actuator). Further, two or more power supplies 116, 118, and/or 120 used to provide redundancy can be connected to automation equipment of the industrial control system 100 using a separate (redundant) power backplane for each power supply 120.

[0040] Referring to FIG. 4, the power supply 120 includes multiple battery modules 122. In embodiments of the disclosure, each battery module 122 comprises a lithium-ion battery cell 124. For example, a battery module 122 is implemented using a one and one-half volt (1.5V) lithium-ion battery cell, a three volt (3V) lithium-ion battery cell, and so forth. In some embodiments, the power supply 120 includes between eight (8) and ten (10) battery modules 122 stacked together. However, a stack of between eight (8) and ten (10) battery modules 122 is provided by way of example only and is not meant to limit the present disclosure. In other embodiments, fewer than eight (8) or more than ten (10) battery modules 122 are stacked together.

[0041] Further, it should be noted that although the battery modules 122 are described as including lithium-ion battery cells 124, systems and techniques of the present disclosure

can use other rechargeable battery, storage, and/or accumulator technologies including, but not necessarily limited to: lead-acid batteries, alkaline batteries, nickel-cadmium batteries, nickel-metal hydride batteries, lithium-ion polymer batteries, lithium sulfur batteries, thin film lithium batteries, potassium-ion batteries, sodium-ion batteries, nickel-iron batteries, nickel-hydrogen batteries, nickel-zinc batteries, lithium-air batteries, lithium iron phosphate batteries, lithium-titanate batteries, zinc bromide batteries, vanadium redox batteries, sodium-sulfur batteries, molten salt batteries, silver-oxide batteries, and so forth.

[0042] Each of the battery modules 120 includes a real-time battery monitor 126, which can be implemented using, for example, a printed circuit board (PCB). In embodiments of the disclosure, the battery monitors 126 are used by the controller 128 (e.g., a microcontroller) that operates the battery cells 124. For example, each battery monitor 126 provides diagnostic information for each respective battery cell 124 to the controller 128. Diagnostic information includes, but is not necessarily limited to: the operating voltage of a battery cell 124, the operating current of a battery cell 124 (e.g., in amperes), units of electrical charge into a battery cell 124 (e.g., in coulombs), units of electrical charge out of a battery cell 124 (e.g., in coulombs), the age of a battery cell 124 (e.g., in units of time, in number of charge/discharge cycles, etc.), and so forth.

[0043] In some embodiments, each battery monitor 126 is separately connected to the controller 128. In other embodiments, multiple battery monitors 126 are connected to a shared communications channel, such as a serial bus, connected to the controller 128. The battery monitors 126 are also connected to a power regulator 130 (e.g., including a transformer), which receives electrical power from an external power supply, such as the power supply 116 and/or the power supply 118. The battery cells 124 are charged using electrical energy supplied from the power regulator 130. Electrical energy is discharged from the battery cells 124 using another power regulator 132, which can be used to adjust one or more output characteristics of the electrical energy supplied by the battery cells 124, such as voltage.

[0044] In embodiments of the disclosure, each battery module 122 comprises a support frame with a foil-wrapped battery cell 124, where multiple support frames can be stacked so that the battery cells 124 remain sealed, while allowing for expansion and contraction of the battery cells 124 within the foil. In embodiments of the disclosure, the PCB comprising the battery monitor 126 is also encased with the battery cell 124 in the support frame. Further, the PCB is powered by the battery cell 124 and configured to limit the current into and out of each battery cell 124. For example, the battery monitor 126 includes an electronic signal switching device (e.g., two (2) field-effect transistors (FETs) connected in series in the manner of an analog switch) that prevents energy from being stored in the battery and/or returned from the battery without authorization from the battery monitor 126. In this manner, electrical connection to a battery cell 124 is prevented when the terminals of the battery cell 124 are connected to an unintended electrical path (e.g., short circuited). Further, electrical connection to a battery cell 124 is prevented when the battery monitor 126 is inactive (e.g., when there is no charge in the battery cell 124). In this example, the battery modules 122 are at least partially charged when they are inserted into the power supply 120.

[0045] In embodiments of the disclosure, the battery modules 122 are stacked and connected using electrical contacts (e.g., electrical connectors) disposed on each support frame. The electrical connectors are electrically connected to the battery cells 124 (e.g., via the battery monitor PCB) and can be disposed on the support frame without wires extending from the support frame (which would otherwise require soldered connections to a battery cell 124). For example, a snap-fit electrical connector is provided on one support frame (e.g., disposed on a top surface of a support frame) that mates with a corresponding snap-fit electrical connector on another support frame (e.g., disposed on a bottom surface of another support frame). The electrical connectors can be configured to increase the surface area of contact between electrical connectors and/or to provide self-alignment of the electrical connectors (e.g., by configuring a portion of one electrical connector for insertion into another electrical connector).

[0046] In embodiments of the disclosure, the electrical connectors are geometrically arranged (e.g., positioned, sized, etc.) to prevent multiple battery modules 122 from being connected together in an unintended manner. For instance, one electrical contact can be oriented generally upwardly with respect to a support frame, while another electrical contact can be oriented generally downwardly with respect to the support frame. In other embodiments, visual cues are provided for aligning two battery modules 122 (e.g., color-coding, indicia, etc.).

[0047] Further, the power supply 120 can include slots, channels, tracks, and so forth to provide mechanical registration for the battery modules 122, such as for aligning the electrical connectors of one battery module 122 with mating electrical connectors of another battery module 122 and/or with electrical connectors to the power supply 120. For example, a battery module 122 includes tabs or posts configured for insertion into respective tracks of a housing of the power supply 120, and providing alignment of the battery modules 122 with respect to the housing. Further, the controller 128 can associate a unique physical identification (ID) with each battery module 122 to uniquely identify each battery module 120 coupled in a particular sequence and/or at a particular position with respect to the housing of the power supply 120.

[0048] In embodiments of the disclosure, the power supply 120 is constructed for cabinet mounting, rack mounting, wall mounting, and so forth. The housing of the power supply 120 can be constructed of a rigid, insulating material, such as acrylonitrile butadiene styrene (ABS) or another plastic material, which can be used to contain the energy that would otherwise be released in the event of a battery cell failure. Further, the housing can be configured to contain, or at least substantially contain, chemical battery cell components, such as lithium, that may be released due to a battery failure. Additionally, the components contained in the power supply 120 can be electrically isolated from one another. For example, signals to the controller 128 are galvanically isolated from the battery monitors 126 and battery cells 124. Further, the controller 128 and the power regulator 130 are electrically and/or fault isolated from the battery modules 122 and the power regulator 132 (e.g., using separate transformers, optical isolators, and so forth).

[0049] Referring now to FIG. 5, the controller 128 is connected to the industrial control system 100 (e.g., via the network 110). In embodiments of the disclosure, the controller 128 implements security and/or diagnostics at the controller level and/or at the level of each battery module 122. A controller 128, including some or all of its components, can operate under computer control. For example, a processor 140 can be included with or in a controller 128 to control the components and functions of controllers 128 described herein using software, firmware, hardware (e.g., fixed logic circuitry), manual processing, or a combination thereof. The terms “controller,” “functionality,” “service,” and “logic” as used herein generally represent software, firmware, hardware, or a combination of software, firmware, or hardware in conjunction with controlling the controllers 128. In the case of a software implementation, the module, functionality, or logic represents program code that performs specified tasks when executed on a processor (e.g., central processing unit (CPU) or CPUs). The program code can be stored in one or more computer-readable memory devices (e.g., internal memory and/or one or more tangible media), and so on. The structures, functions, approaches, and techniques described herein can be implemented on a variety of commercial computing platforms having a variety of processors.

[0050] The processor 140 provides processing functionality for the controller 128 and can include any number of processors, micro-controllers, or other processing systems, and resident or external memory for storing data and other information accessed or generated by the controller 128. The processor 140 can execute one or more software programs that implement techniques described herein. The processor 140 is not limited by the materials from which it is formed or the processing mechanisms employed therein and, as such, can be implemented via semiconductor(s) and/or transistors (e.g., using electronic integrated circuit (IC) components), and so forth.

[0051] The controller 128 also includes the memory 142. The memory 142 is an example of tangible, computer-readable storage medium that provides storage functionality to store various data associated with operation of the controller 128, such as

software programs and/or code segments, or other data to instruct the processor 140, and possibly other components of the controller 128, to perform the functionality described herein. Thus, the memory 142 can store data, such as a program of instructions for operating the power supply 120 (including its components), and so forth. In embodiments of the disclosure, the memory 142 can store a unique identifier 136 and/or a security credential 138 for the power supply 120. It should be noted that while a single memory 142 is described, a wide variety of types and combinations of memory (e.g., tangible, non-transitory memory) can be employed. The memory 142 can be integral with the processor 140, can comprise stand-alone memory, or can be a combination of both. The memory 142 can include, but is not necessarily limited to: removable and non-removable memory components, such as random-access memory (RAM), read-only memory (ROM), flash memory (e.g., a secure digital (SD) memory card, a mini-SD memory card, and/or a micro-SD memory card), magnetic memory, optical memory, universal serial bus (USB) memory devices, hard disk memory, external memory, and so forth. In implementations, the power supply 120 and/or the memory 142 can include removable integrated circuit card (ICC) memory, such as memory provided by a subscriber identity module (SIM) card, a universal subscriber identity module (USIM) card, a universal integrated circuit card (UICC), and so on.

[0052] The controller 128 includes a communications interface 150. The communications interface 150 is operatively configured to communicate with components of the power supply 120. For example, the communications interface 150 can be configured to transmit data for storage in the controller 128, retrieve data from storage in the controller 128, and so forth. The communications interface 150 is also communicatively coupled with the processor 140 to facilitate data transfer between components of the power supply 120 and the processor 140, e.g., for communicating inputs to the processor 140 received from a device communicatively coupled with the controller 128 and/or communicating outputs to a device communicatively coupled with the controller 128, such as the battery monitors 126. For example, the communications interface 150 is implemented using a shared communications channel, such as a serial bus, to connect the processor to multiple battery monitors 126.

[0053] In embodiments of the disclosure, the controller 128 is configured for two-way communication with the battery monitors 126. For example, the controller 128 collects diagnostic information (e.g., status information and/or reliability information regarding the battery cells 124) from the battery monitors 126. The controller 128 also operates the battery modules 122, e.g., instructing the battery modules 122 to store and return electrical energy supplied from the power supply 116, the power supply 118, and so forth. It should be noted that while the communications interface 150 is described as a component of a controller 128, one or more components of the communications interface 150 can be implemented as external components communicatively coupled to the controller 128 via a wired and/or wireless connection. The controller 128 can also comprise and/or connect to one or more input/output (I/O) devices (e.g., via the communications interface 150) including, but not necessarily limited to: a display, a mouse, and so on. For example, the controller 128 can be connected to a display device, such as a multi-color (e.g., tri-color) light emitting diode (LED) (e.g., the indicator light 144), which can indicate the status of the power supply 120.

[0054] The communications interface 150 and/or the processor 140 can be configured to communicate with a variety of different networks 110, including, but not necessarily limited to: a wide-area cellular telephone network, such as a 3G cellular network, a 4G cellular network, or a global system for mobile communications (GSM) network; a wireless computer communications network, such as a WiFi network (e.g., a wireless local area network (WLAN) operated using IEEE 802.11 network standards); an internet; the Internet; a wide area network (WAN); a local area network (LAN); a personal area network (PAN) (e.g., a wireless personal area network (WPAN) operated using IEEE 802.15 network standards); a public telephone network; an extranet; an intranet; and so on. However, this list is provided by way of example only and is not meant to limit the present disclosure. Additionally, the communications interface 150 can be implemented using a computer bus. For example, a communications interface 150 can include a PCI card interface, such as a Mini PCI interface, and so forth. Further, the communications interface 150 can be configured to communicate with a single network 110 or multiple

networks across different access points. In this manner, the controller 128 is used to communicatively couple the power supply 120 to the industrial control system 100.

[0055] Referring now to FIG. 6, the control elements or subsystems (e.g., the I/O modules 102, the control modules 104, the power supplies 120, and so forth) are connected together by one or more backplanes. For example, control modules 104 can be connected to I/O modules 102 by a communications backplane 152. Further, power supplies 120 can be connected to I/O modules 102 and/or to control modules 104 by a power backplane 154. In embodiments of the disclosure, physical interconnect devices (e.g., switches, connectors, or cables such as, but not limited to, those described in U.S. Patent Publication No. US2015/0296619 A1) are used to connect to the I/O modules 102, the control modules 104, the power supplies 120, and possibly other industrial control system equipment. For example, a cable is used to connect a control module 104 to a network 110, another cable is used to connect a power supply 116 to a power grid 112, another cable is used to connect a power supply 118 to a local power generator 114, and so forth.

[0056] In embodiments of the disclosure, the industrial control system 100 implements a secure control system. For example, the industrial control system 100 includes a security credential source (e.g., a factory 156) and a security credential implementer (e.g., a key management entity 158). The factory 156 is configured to generate a unique security credential (e.g., a key, a certificate, etc., such as the unique identifier 136 and/or the security credential 138). The key management entity 158 is configured to provision the I/O modules 102, the control modules 104, the power supply 116, the power supply 118, and/or the power supply 120 (e.g., including one or more of the multiple battery modules 122 and/or the controller 128) with a unique security credential generated by the factory 156. For instance, an I/O module 102 and an associated power supply 120 can each be provisioned with unique security credentials.

[0057] Then, an authentication process for authenticating the control elements or subsystems implemented in the industrial control system 100 is performed based upon the

unique security credentials. For example, in embodiments, the control module 104 and the power supply 120 are operable to bi-directionally communicate with one another based on the unique security credentials (e.g., based upon the authentication process). Further, in the secure industrial control system 100 disclosed herein, multiple (e.g., every) control elements and subsystems (e.g., I/O modules, power supplies, physical interconnect devices, etc.) of the industrial control system 100 are provisioned with security credentials for providing security at multiple (e.g., all) levels of the industrial control system 100. Still further, the elements can be provisioned with the unique security credentials (e.g., keys, certificates, etc.) during manufacture (e.g., at birth), and can be managed from birth by a key management entity of the industrial control system 100 for promoting security of the industrial control system 100.

[0058] In some embodiments, the control elements or subsystems are connected using controllers connected to or included in physical interconnect devices (e.g., one-wire encryption chips) which allow for implementation of authentication between a component (e.g., a power supply 120) and the physical interconnect device (e.g., cable assembly) connected to that component. For example, microprocessor secure encrypted technology can be built into the cable assembly and keyed to a specific component of the industrial control system 100. This configuration provides security for the industrial control system 100 when a user installs (e.g., plugs) the cable assembly into a component which is not configured to be connected with that cable assembly. In embodiments, a one-wire serial key (e.g., a one-wire embedded key) is implemented in one or more (e.g., each of) the physical interconnect devices.

[0059] In embodiments of the disclosure, communications between elements and/or physical interconnect devices (e.g., cable assemblies) of the industrial control system 100 include an authentication process. The authentication process can be performed for authenticating an element and/or physical interconnect device implemented in the industrial control system 100. In implementations, the authentication process can utilize security credentials associated with the element and/or physical interconnect device for authenticating that element and/or physical interconnect device. For example, the

security credentials can include encryption keys, certificates (e.g., public key certificates, digital certificates, identity certificates, security certificates, asymmetric certificates, standard certificates, non-standard certificates) and/or identification numbers. In embodiments, controllers (e.g., secure microcontrollers) that are included in and/or connected to the components and/or physical interconnect devices of the industrial control system 100 can be configured for performing the authentication process.

[0060] In implementations, multiple control elements or subsystems (e.g., elements and/or physical interconnect devices) of the industrial control system 100 are provisioned with their own unique security credentials. For example, each element of the industrial control system 100 is provisioned with its own unique set(s) of certificates, encryption keys and/or identification numbers when the element is manufactured (e.g., the individual sets of keys and certificates are defined at the birth of the element). The sets of certificates, encryption keys and/or identification numbers are configured for providing/supporting strong encryption. The encryption keys can be implemented with standard (e.g., commercial off-the-shelf (COTS)) encryption algorithms, such as National Security Agency (NSA) algorithms, National Institute of Standards and Technology (NIST) algorithms, or the like.

[0061] In some embodiments, cryptographic keys and certificates can be stored in on-chip memory (OCM), for example, in SRAM of an authentication module. Additionally, sensitive tasks (e.g., tasks with secret information and sometimes even with public information) may have a stack that executes in OCM. For example, cryptographic tasks may be performed in kernel space or application space from stacks locally stored in OCM.

[0062] Based upon the results of the authentication process, the element being authenticated can be activated, partial functionality of the element can be enabled or disabled within the industrial control system 100, complete functionality of the element can be enabled within the industrial control system 100, and/or functionality of the element within the industrial control system 100 can be completely disabled (e.g., no

communication facilitated between that element and other elements of the industrial control system 100).

[0063] In embodiments, the keys, certificates and/or identification numbers associated with an element of the industrial control system 100 can specify the original equipment manufacturer (OEM) of that element. As used herein, the term “original equipment manufacturer” or “OEM” can be defined as an entity that physically manufactures the device (e.g., element) and/or a supplier of the device such as an entity that purchases the device from a physical manufacturer and sells the device. Thus, in embodiments, a device can be manufactured and distributed (sold) by an OEM that is both the physical manufacturer and the supplier of the device. However, in other embodiments, a device can be distributed by an OEM that is a supplier, but is not the physical manufacturer. In such embodiments, the OEM can cause the device to be manufactured by a physical manufacturer (e.g., the OEM can purchase, contract, order, etc. the device from the physical manufacturer).

[0064] Additionally, where the OEM comprises a supplier that is not the physical manufacturer of the device, the device can bear the brand of the supplier instead of brand of the physical manufacturer. For example, in embodiments where an element (e.g., a power supply 120) is associated with a particular OEM that is a supplier but not the physical manufacturer, the element’s keys, certificates and/or identification numbers can specify that origin. During authentication of an element of the industrial control system 100, when a determination is made that an element being authenticated was manufactured or supplied by an entity that is different than the OEM of one or more other elements of the industrial control system 100, then the functionality of that element can be at least partially disabled within the industrial control system 100. For example, limitations can be placed upon communication (e.g., data transfer) between that element and other elements of the industrial control system 100, such that the element cannot work/function within the industrial control system 100. When one of the elements of the industrial control system 100 requires replacement, this feature can prevent a user of the industrial control system 100 from unknowingly replacing the element with a non-homogenous

element (e.g., an element having a different origin (a different OEM) than the remaining elements of the industrial control system 100) and implementing the element in the industrial control system 100. In this manner, the techniques described herein can prevent the substitution of elements of other OEM's into a secure industrial control system 100. In one example, the substitution of elements that furnish similar functionality in place of elements provided by an originating OEM can be prevented, since the substituted elements cannot authenticate and operate within the originating OEM's system. In another example, a first reseller can be provided with elements having a first set of physical and cryptographic labels by an originating OEM, and the first reseller's elements can be installed in an industrial control system 100. In this example, a second reseller can be provided with elements having a second (e.g., different) set of physical and cryptographic labels by the same originating OEM. In this example, the second reseller's elements may be prevented from operating within the industrial control system 100, since they may not authenticate and operate with the first reseller's elements. However, it should also be noted that the first reseller and the second reseller may enter into a mutual agreement, where the first and second elements can be configured to authenticate and operate within the same industrial control system 100. Further, in some embodiments, an agreement between resellers to allow interoperation can also be implemented so the agreement only applies to a specific customer, group of customers, facility, etc.

[0065] In another instance, a user can attempt to implement an incorrectly designated (e.g., mismarked) element within the industrial control system 100. For example, the mismarked element can have a physical indicia marked upon it which falsely indicates that the element is associated with the same OEM as the OEM of the other elements of the industrial control system 100. In such instances, the authentication process implemented by the industrial control system 100 can cause the user to be alerted that the element is counterfeit. This process can also promote improved security for the industrial control system 100, since counterfeit elements are often a vehicle by which malicious software can be introduced into the industrial control system 100. In embodiments, the authentication process provides a secure air gap for the industrial control system 100,

ensuring that the secure industrial control system is physically isolated from insecure networks.

[0066] The key management entity 158 can be configured for managing cryptographic keys (e.g., encryption keys) in a cryptosystem. This managing of cryptographic keys (e.g., key management) can include the generation, exchange, storage, use, and/or replacement of the keys. For example, the key management entity 158 is configured to serve as a security credentials source, generating unique security credentials (e.g., public security credentials, secret security credentials) for the elements of the industrial control system 100. Key management pertains to keys at the user and/or system level (e.g., either between users or systems).

[0067] In embodiments, the key management entity 158 comprises a secure entity such as an entity located in a secure facility. The key management entity 158 can be remotely located from the I/O modules 102, the control modules 104, and the network 110. For example, a firewall 160 can separate the key management entity 158 from the control elements or subsystems and the network 110 (e.g., a corporate network). In implementations, the firewall 160 can be a software or hardware-based network security system that controls ingoing and outgoing network traffic by analyzing data packets and determining whether the data packets should be allowed through or not, based on a rule set. The firewall 160 thus establishes a barrier between a trusted, secure internal network (e.g., the network 110) and another network 162 that is not assumed to be secure and trusted (e.g., a cloud and/or the Internet). In embodiments, the firewall 160 allows for selective (e.g., secure) communication between the key management entity 158 and one or more of the control elements or subsystems and/or the network 110. In examples, one or more firewalls can be implemented at various locations within the industrial control system 100. For example, firewalls can be integrated into switches and/or workstations of the network 110.

[0068] As described, the secure industrial control system 100 can further include one or more manufacturing entities (e.g., factories 156). The factories 156 can be associated

with original equipment manufacturers (OEMs) for the elements of the industrial control system 100. The key management entity 158 can be communicatively coupled with the manufacturing entity via a network (e.g., a cloud). In implementations, when the elements of the industrial control system 100 are being manufactured at the one or more factories 156, the key management entity 158 can be communicatively coupled with (e.g., can have an encrypted communications pipeline to) the elements. The key management entity 158 can utilize the communications pipeline for provisioning the elements with security credentials (e.g., inserting keys, certificates and/or identification numbers into the elements) at the point of manufacture.

[0069] Further, when the elements are placed into use (e.g., activated), the key management entity 158 can be communicatively coupled (e.g., via an encrypted communications pipeline) to each individual element worldwide and can confirm and sign the use of specific code, revoke (e.g., remove) the use of any particular code, and/or enable the use of any particular code. Thus, the key management entity 158 can communicate with each element at the factory where the element is originally manufactured (e.g., born), such that the element is born with managed keys. A master database and/or table including all encryption keys, certificates and/or identification numbers for each element of the industrial control system 100 can be maintained by the key management entity 158. The key management entity 158, through its communication with the elements, is configured for revoking keys, thereby promoting the ability of the authentication mechanism to counter theft and re-use of components.

[0070] In implementations, the key management entity 158 can be communicatively coupled with one or more of the control elements and sub-systems and/or the network 110 via another network (e.g., a cloud and/or the Internet) and firewall. For example, in embodiments, the key management entity 158 can be a centralized system or a distributed system. Moreover, in embodiments, the key management entity 158 can be managed locally or remotely. In some implementations, the key management entity 158 can be located within (e.g., integrated into) the network 110 and/or the control elements or subsystems. The key management entity 158 can provide management and/or can be

managed in a variety of ways. For example, the key management entity 158 can be implemented/managed: by a customer at a central location, by the customer at individual factory locations, by an external third party management company and/or by the customer at different layers of the industrial control system 100, and at different locations, depending on the layer.

[0071] Varying levels of security (e.g., scalable, user-configured amounts of security) can be provided by the authentication process. For example, a base level of security can be provided which authenticates the elements and protects code within the elements. Other layers of security can be added as well. For example, security can be implemented to such a degree that a component, such as the power supply 120, cannot power up without proper authentication occurring. In implementations, encryption in the code is implemented in the elements, security credentials (e.g., keys and certificates) are implemented on the elements. Security can be distributed (e.g., flows) through the industrial control system 100. For example, security can flow through the industrial control system 100 all the way to an end user, who knows what a module is designed to control in that instance. In embodiments, the authentication process provides encryption, identification of devices for secure communication and authentication of system hardware or software components (e.g., via digital signature).

[0072] In implementations, the authentication process can be implemented to provide for and/or enable interoperability within the secure industrial control system 100 of elements manufactured and/or supplied by different manufacturers/vendors/suppliers (e.g., OEMs). For example, selective (e.g., some) interoperability between elements manufactured and/or supplied by different manufacturers/vendors/suppliers can be enabled. In embodiments, unique security credentials (e.g., keys) implemented during authentication can form a hierarchy, thereby allowing for different functions to be performed by different elements of the industrial control system 100.

[0073] The communication links connecting the components of the industrial control system 100 can further employ data packets, such as runt packets (e.g., packets smaller

than sixty-four (64) bytes), placed (e.g., injected and/or stuffed) therein, providing an added level of security. The use of runt packets increases the level of difficulty with which outside information (e.g., malicious content such as false messages, malware (viruses), data mining applications, etc.) can be injected onto the communications links. For example, runt packets can be injected onto a communication link within gaps between data packets transmitted between a control module 104 and a power supply 120 to hinder an external entity's ability to inject malicious content onto the communication link.

[0074] In embodiments of the disclosure, to initiate an authentication sequence, a first authentication module (e.g., included in a power supply 120, a controller 128 of a power supply 120, a battery module 122 of a power supply 120, a control element or subsystem, such as an I/O device 102, a control module 104, and so forth) is configured to transmit a request datagram to a second authentication module (e.g., included in a power supply 120, a controller 128 of a power supply 120, a battery module 122 of a power supply 120, a control element or subsystem, such as an I/O device 102, a control module 104, and so forth). In implementations, the request datagram includes a first plain text nonce (NonceA), a first device authentication key certificate (CertDAKA) containing a first device authentication key (DAKA), and a first identity attribute certificate (IACA). In some embodiments, the first authentication module is configured to generate the first nonce (NonceA) with a true random number generator (hereinafter "TRNG") and concatenate or otherwise combine the first nonce (NonceA), the first device authentication key certificate (CertDAKA), and the first identity attribute certificate (IACA) to generate the request datagram. In some embodiments, the first device authentication key certificate (CertDAKA) and the first identity attribute certificate (IACA) are locally stored by the first authentication module. For example, the certificates may be stored in a local memory (e.g., ROM, RAM, flash memory, or other non-transitory storage medium) of the first authentication module.

[0075] The second authentication module is configured to validate the request datagram by verifying the first device authentication key certificate (CertDAKA) and the first

identity attribute certificate (IACA) with public keys that are generated by a device lifecycle managements system (DLM) or derived utilizing crypto library functions. In this regard, the public keys may be stored in SRAM or another local memory of the authentication module and used with crypto library functions to verify or cryptographically sign exchanged data, such as the nonces exchanged between the authentication modules. In some embodiments, the second authentication module may verify the certificates with an elliptic curve digital signing algorithm (hereinafter “ECDSA”) or other verification operation. In some embodiments, the second authentication module may be further configured to validate the certificate values from plain text values by verifying the following: certificate type is device authentication key (hereinafter “DAK”) or identity attribute certificate (hereinafter “IAC”) for each certificate; IAC names match, DAK certificate module type matches module type argument; and/or microprocessor serial number (hereinafter “MPSN”) of each certificate in the message payload match each other. In some embodiments, the second authentication module may be further configured to verify the DAK and IAC certificates are not in a local revocation list (e.g., a list or database including revoked and/or invalid certificates). When the second authentication module fails to validate the request datagram, the second authentication module may generate an error message, partially or completely disable the first authentication module, and/or discontinue or restrict communications to/from the first authentication module.

[0076] Responsive to a valid request datagram, the second authentication module is configured to transmit a response datagram to the first authentication module. In implementations, the response datagram includes a second plain text nonce (NonceB), a first signature associated with the first and second nonces (SigB[NonceA||NonceB]), a second device authentication key certificate (certDAKB) containing a second device authentication key (DAKB), and a second identity attribute certificate (IACB). In some embodiments, the second authentication module is configured to generate the second nonce (NonceB) with a TRNG, concatenate or otherwise combine the first nonce (NonceA) and the second nonce (NonceB), and sign the concatenated/combined nonces with a private key (e.g., DAK) that is locally stored by the second authentication module.

The second authentication module is further configured to concatenate or otherwise combine the second nonce (NonceB), the first signature associated with the first and second nonces (SigB[NonceA||NonceB]), the second device authentication key certificate (certDAKB), and the second identity attribute certificate (IACB) to generate the response datagram. In some embodiments, the second device authentication key certificate (CertDAKB) and the second identity attribute certificate (IACB) are locally stored by the second authentication module. For example, the certificates may be stored in a local memory (e.g., ROM, RAM, flash memory, or other non-transitory storage medium) of the second authentication module.

[0077] The first authentication module is configured to validate the response datagram by verifying the second device authentication key certificate (CertDAKB) and the second identity attribute certificate (IACB) with public keys that are locally stored or retrieved from a crypto library utilizing ECDSA or another verification operation. In some embodiments, the first authentication module may be further configured to validate the certificate values from plain text values by verifying the following: IAC & DAK certificates have matching MPSNs, IAC names match, certificate types are correct on both certificates (IAC & DAK), the correct issuer name is on both certificates, DAK module type is the correct type (e.g., communications/control module). In some embodiments, the first authentication module may be further configured to verify the DAK and IAC certificates are not in a local revocation list.

[0078] To validate the response datagram, the first authentication module is further configured to verify the first signature associated with the first and second nonces (sigB[NonceA||NonceB]). In some embodiments, the first authentication module is configured to verify the first signature (sigB[NonceA||NonceB]) by concatenating the first locally stored nonce (NonceA) and the second plaintext nonce (NonceB) received from the second authentication module, verifying the first cryptographic signature (sigB[NonceA||NonceB]) with a public device authentication key (e.g., using DAKB from certDAKB), and comparing the locally generated concatenation of the first nonce and the second nonce with the cryptographically verified concatenation of the first nonce

and the second nonce. When the first authentication module fails to validate the response datagram, the first authentication module may generate an error message, partially or completely disable the second authentication module, and/or discontinue or restrict communications to/from the second authentication module.

[0079] The first authentication module is further configured to transmit an authentication datagram to the second authentication module when the response datagram is valid. In implementations, the authentication datagram includes a second signature associated with the first and second nonces ($\text{sigA}[\text{NonceA}||\text{NonceB}]$). In some embodiments, the first authentication module is configured to sign the locally generated concatenation of the first and second nonces a private key (e.g., DAK) that is locally stored by the first authentication module. When the response datagram is invalid, the authentication datagram may be replaced with a “failed” authentication datagram including a signature associated with the second nonce and an error reporting (e.g., “failure”) message ($\text{sigA}[\text{NonceB}||\text{Error}]$) generated by the first authentication module.

[0080] Responsive to the authentication datagram, the second authentication module may be further configured to transmit a responsive authentication datagram to the first authentication module. In implementations, the responsive authentication datagram includes a signature associated with the first nonce and an error reporting (e.g., “success” or “failure”) message ($\text{sigB}[\text{NonceA}||\text{Error}]$) generated by the second authentication module. In some embodiments, the second authentication module is configured to validate the authentication datagram by verifying the second signature associated with the first and second nonces ($\text{sigA}[\text{NonceA}||\text{NonceB}]$). In some embodiments, the second authentication module is configured to verify the second signature ($\text{sigA}[\text{NonceA}||\text{NonceB}]$) by concatenating the first plaintext nonce (NonceA) received from the first authentication module and the second locally stored nonce (NonceB), verifying the second cryptographic signature ($\text{sigA}[\text{NonceA}||\text{NonceB}]$) with a public device authentication key (e.g., using DAKA from certDAKA), and comparing the locally generated concatenation of the first nonce and the second nonce with the cryptographically verified concatenation of the first nonce and the second nonce. In

addition to the error reporting message, when the second authentication module fails to validate the authentication datagram, the second authentication module may partially or completely disable the first authentication module, and/or discontinue or restrict communications to/from the first authentication module.

[0081] In implementations where the devices employing the authentication modules are arranged according to a “master-slave” configuration, the master (e.g., the first authentication module) may be configured to authenticate each slave. In the event of a failed authentication, the master may at least partially disable or restrict communications to/from the unauthenticated slave. Alternatively, two or more slave modules operating in parallel without a master may authenticate one another, where a failed authentication results in both devices being partially or completely disabled. For example, two or more redundant power supplies 120 can be disabled should they fail to successfully complete the authentication sequence at startup or another predefined time/event.

[0082] Referring now to FIGS. 7 and 8, each power supply 120 or any other industrial element/controller 206 can be at least partially operated according to requests/commands from an action originator 202. In implementations, the action originator 202 is an operator interface 208 (e.g., SCADA and/or HMI), an engineering interface 210 including an editor 212 and a compiler 214, a local application 220, a remote application 216 (e.g., communicating through a network 218 via a local application 220), and so forth. In the authentication path 200 illustrated in FIGS. 7 and 8, the industrial element/controller 206 (e.g., the power supply 120) processes an action request (e.g., request for data, control command, firmware/software update, set point control, application image download, or the like) only when the action request has been signed and/or encrypted by an action authenticator 204. This prevents unauthorized action requests from valid user profiles and further secures the system from unauthorized action requests coming from invalid (e.g., hacked) profiles.

[0083] In embodiments of the disclosure, the action authenticator 204 can be on-site with the action originator 202 (e.g., directly connected device lifecycle management system

(DLM) 222 or secured workstation 226) or remotely located (e.g., DLM 222 connected via the network 218). In general, the action authenticator 204 includes a storage medium with a private key stored thereon and a processor configured to sign and/or encrypt the action request generated by the action originator 202 with the private key. The private key is stored in a memory that may not be accessed via standard operator login. For instance, the secured workstation 226 can require a physical key, portable encryption device (e.g., smart card, RFID tag, or the like), and/or biometric input for access.

[0084] In some embodiments, the action authenticator 204 includes a portable encryption device such as a smart card 224 (which can include a secured microprocessor). In this manner, the entire device (including the privately stored key and processor in communication therewith) can be carried with an operator or user that has authorized access to an interface of the action originator 202. Whether the action authentication node 204 accesses the authentication path 200 via a secured or an unsecured workstation, the action request from the action originator 202 can be securely signed and/or encrypted within the architecture of the portable encryption device (e.g., as opposed to using a potentially less secure workstation or cloud-based architecture). By way of example, an unauthorized person would have to physically take possession of the smart card 224 before being able to authenticate any action requests sent via the action originator 202.

[0085] In some embodiments, multiple layers of security can be employed. For example, the action authenticator 204 can include a secured workstation 226 that may be only accessible to sign and/or encrypt action requests via smart card 224 access. Additionally, the secured workstation 226 may be accessible via a biometric or multifactor cryptography device 228 (e.g., one or more of a fingerprint scanner, an iris scanner, a facial recognition device, and so on). In some embodiments, a multifactor cryptography device 228 can require a valid biometric input before enabling the smart card 224 or other portable encryption device to sign an action request.

[0086] The power supply 120 or any other industrial element/controller 206 being driven by the action originator 202 is configured to receive the signed action request, verify the

authenticity of the signed action request, and perform a requested action when the authenticity of the signed action request is verified. In some embodiments, the industrial element/controller 206 (e.g., the power supply 120) includes a storage medium (e.g., SD/micro-SD card, HDD, SSD, or any other non-transitory storage device) (e.g., the memory 142 of the power supply 120) configured to store the action request (e.g., application image, control command, and/or any other data sent by the action originator). The industrial element/controller 206 further includes a processor (e.g., the processor 140 of the power supply 120) that performs/executes the action request (i.e., performs the requested action) after the signature is verified. In some embodiments, the action request is encrypted by the action originator 202 and/or the action authenticator 204 and must also be decrypted by the processor 140 before the requested action can be performed. In implementations, the industrial element/controller 206 includes a virtual key switch 234 (e.g., a software module running on the processor 140) that enables the processor 140 to perform the requested action only after the action request signature is verified and/or after the action request is decrypted. In some embodiments, each and every action or each one of a selection of critical actions must clear the authentication path before being run on the industrial element/controller 206.

[0087] FIG. 9 depicts a process 300, in accordance with example embodiments, for authenticating an action request in an industrial control system. In implementations, the process 300 can be manifested by the industrial control system 100 (e.g., as described with reference to FIGS. 1 through 6) and/or the authentication path 200 (e.g., as described with reference to FIGS. 7 and 8) of the industrial control system 100. An action request is originated (Block 310). For example, an operator/engineering interface 208/210 and/or a remote/local application interface 216/220 is used to generate and action request. Then, the action request is signed with the action authenticator (Block 320). For instance, action authenticator 204 is used to sign an action request. In some embodiments, the action request can be encrypted with the action authenticator (Block 322). Then, the signed action request is sent (e.g., downloaded) to an industrial element/controller (Block 330). For example, the action request is furnished to the industrial element/controller 206 (e.g., to power supply 120). Next, the authenticity of the signed action request is verified

(Block 340). In some embodiments, the action request can be decrypted with the industrial element/controller (Block 342). For instance, the industrial element/controller 206 can decrypt the action request. Then, a requested action can be performed when the authenticity of the signed action request is verified (Block 350). For example, the power supply 120 performs an action requested by the operator/engineering interface 208, 210 and/or the remote/local application interface 216, 220.

[0088] For enhanced security, the industrial element/controller 206 (e.g., the power supply 120) can be further configured to perform an authentication sequence with the action authenticator 204 (e.g., with a smart card 224) before the requested action is run by the industrial element/controller 206. For example, the so-called “handshake” can be performed prior to Block 350 or even prior to Block 330. In some embodiments, the signature and verification Blocks 320 and 340 can be executed using a more intricate authentication sequence. Additionally, in some embodiments, the authentication sequence can be performed as an additional security measure to augment the simpler signature verification and/or decryption measures.

[0089] In some embodiments, an authentication sequence implemented by the industrial element/controller 206 can include sending a request datagram to the action authenticator 204, e.g., where the request datagram includes a first cryptographic nonce, a first device authentication key certificate (e.g., a first authentication certificate that contains a device authentication key), and a first identity attribute certificate. Then, a response datagram is received from the action authenticator 204, e.g., where the response datagram includes a second nonce, a first signature associated with the first and second nonces, a second device authentication key certificate (e.g., a second authentication certificate that contains a device authentication key), and a second identity attribute certificate. Next, the response datagram can be validated by verifying the first signature associated with the first and second nonces, the second device authentication key certificate, and the second identity attribute certificate. Next, an authentication datagram can be sent to the action authenticator 204 (e.g., when the response datagram is determined to be valid), where the

authentication datagram includes a second signature associated with the first and second nonces.

[0090] Alternatively, the action authenticator 204 can initiate the handshake, in which case the authentication sequence implemented by the industrial element/controller 206 can include receiving a request datagram from the action authenticator 204, e.g., where the request datagram includes a first nonce, a first device authentication key certificate, and a first identity attribute certificate. Next, the request datagram can be validated by verifying the first device authentication key certificate and the first identity attribute certificate. Then, a response datagram can be sent to the action authenticator when the request datagram is valid, e.g., where the response datagram includes a second nonce, a first signature associated with the first and second nonces, a second device authentication key certificate, and a second identity attribute certificate. Next, an authentication datagram from the action authenticator 204 can be received, e.g., where the authentication datagram includes a second signature associated with the first and second nonces. Then, the authentication datagram can be validated, e.g., by verifying the second signature associated with the first and second nonces.

[0091] The handshake or authentication sequence that can be implemented by the industrial element/controller 206 and the action authenticator 204 can be accomplished using one or more of the techniques described above (e.g., with reference to authentication performed by the authentication modules). Further, each of the action originator 202, the action authenticator 204, and the industrial element/controller 206 can include circuitry and/or logic enabled to perform the functions or operations (e.g., steps of method 300 and the authentication sequence) described herein. For example, each of the action originator 202, the action authenticator 204, and the industrial element/controller 206 can include one or more processors that execute program instruction stored permanently, semi-permanently, or temporarily by a non-transitory machine readable medium such as, but not necessarily limited to: a hard disk drive (HDD), solid-state disk (SDD), optical disk, magnetic storage device, flash drive, or SD/micro-SD card.

[0092] Generally, any of the functions described herein can be implemented using hardware (e.g., fixed logic circuitry such as integrated circuits), software, firmware, manual processing, or a combination thereof. Thus, the blocks discussed in the above disclosure generally represent hardware (e.g., fixed logic circuitry such as integrated circuits), software, firmware, or a combination thereof. In the instance of a hardware configuration, the various blocks discussed in the above disclosure may be implemented as integrated circuits along with other functionality. Such integrated circuits may include all of the functions of a given block, system, or circuit, or a portion of the functions of the block, system, or circuit. Further, elements of the blocks, systems, or circuits may be implemented across multiple integrated circuits. Such integrated circuits may comprise various integrated circuits, including, but not necessarily limited to: a monolithic integrated circuit, a flip chip integrated circuit, a multichip module integrated circuit, and/or a mixed signal integrated circuit. In the instance of a software implementation, the various blocks discussed in the above disclosure represent executable instructions (e.g., program code) that perform specified tasks when executed on a processor. These executable instructions can be stored in one or more tangible computer readable media. In some such instances, the entire system, block, or circuit may be implemented using its software or firmware equivalent. In other instances, one part of a given system, block, or circuit may be implemented in software or firmware, while other parts are implemented in hardware.

Conclusion

[0093] Although the subject matter has been described in language specific to structural features and/or process operations, it is to be understood that the scope of the claims should not be limited by the preferred embodiments set forth in the examples, but should be given the broadest interpretation consistent with the description as a whole.

What is claimed is:

1. A control system comprising:
an electrical power source;
an alternating current power supply electrically coupled with the electrical power source;
an uninterruptable power supply electrically coupled with the alternating current power supply for storing and returning electrical energy supplied by the alternating current power supply, the uninterruptable power supply comprising at least one battery module comprising a battery cell and a battery monitor configured to monitor the battery cell, and a controller operatively coupled with the battery module, the controller configured to receive diagnostic information from the battery module; and
at least one control element or subsystem electrically connected to the alternating current power supply, wherein the uninterruptable power supply is configured to return electrical energy to the alternating current power supply to power the at least one control element or subsystem.
2. The control system according to claim 1, wherein the battery monitor is configured to prevent electrical access to the battery cell when at least one of an unintended electrical path is established to terminals of the battery cell or an authentication of a connection to the battery module cannot be established.
3. The control system according to claim 1 or 2, wherein the diagnostic information comprises at least one of an operating voltage of the battery cell, an operating current of the battery cell, an electrical charge associated with the battery cell, or an age associated with the battery cell.
4. The control system according to claim 1, 2 or 3, wherein the battery monitor comprises an electronic signal switching device implemented using a plurality of field-effect transistors connected in series.

5. The control system according to any one of claims 1 to 4, wherein at least one of the battery module or the controller is configured with at least one of a unique identifier or a unique security credential.

6. The control system to any one of claims 1 to 5, wherein the battery module is galvanically isolated from the controller.

7. The control system as recited in claim 6, further comprising an optical isolator for galvanically isolating the battery module from the controller.

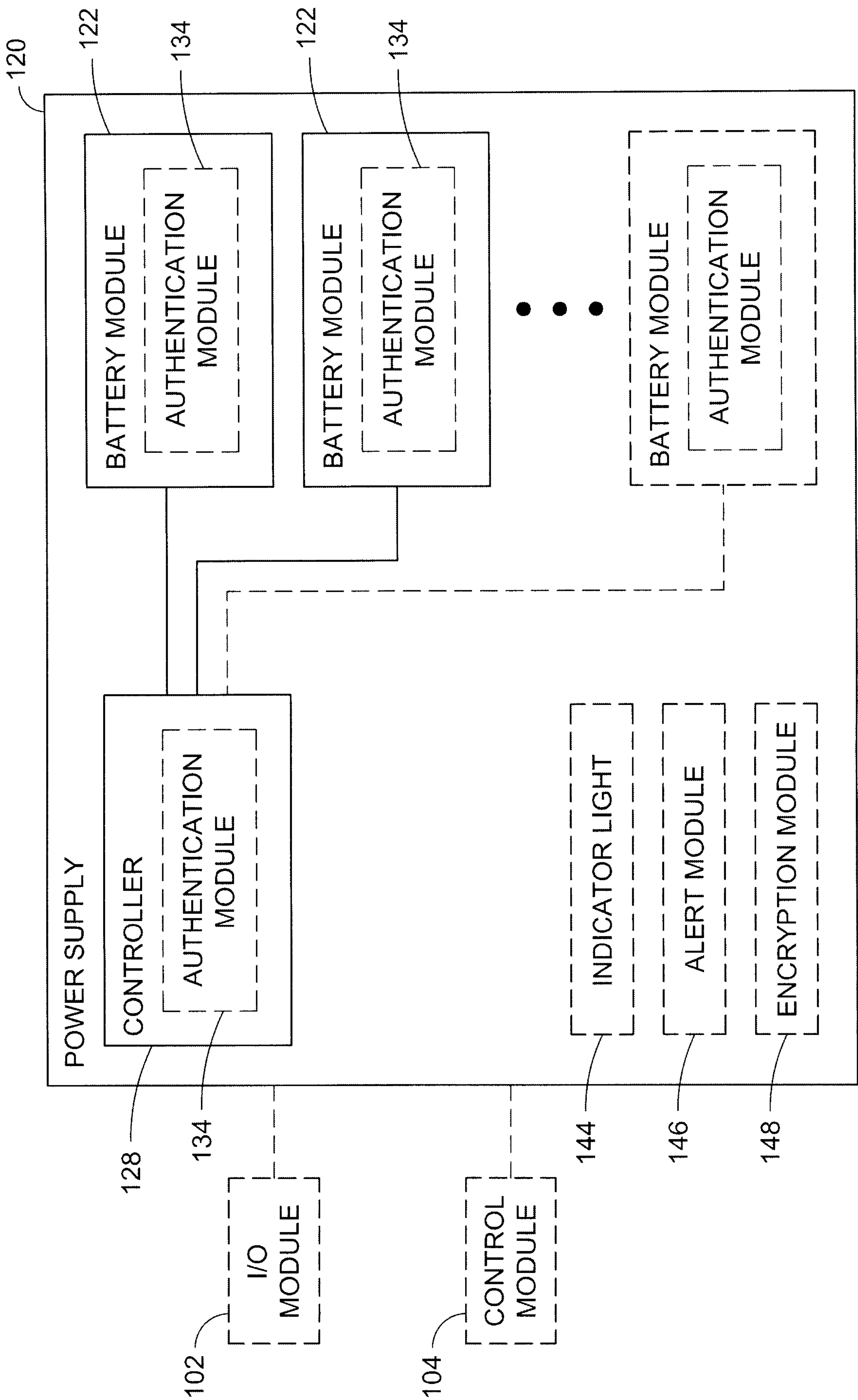


FIG. 1

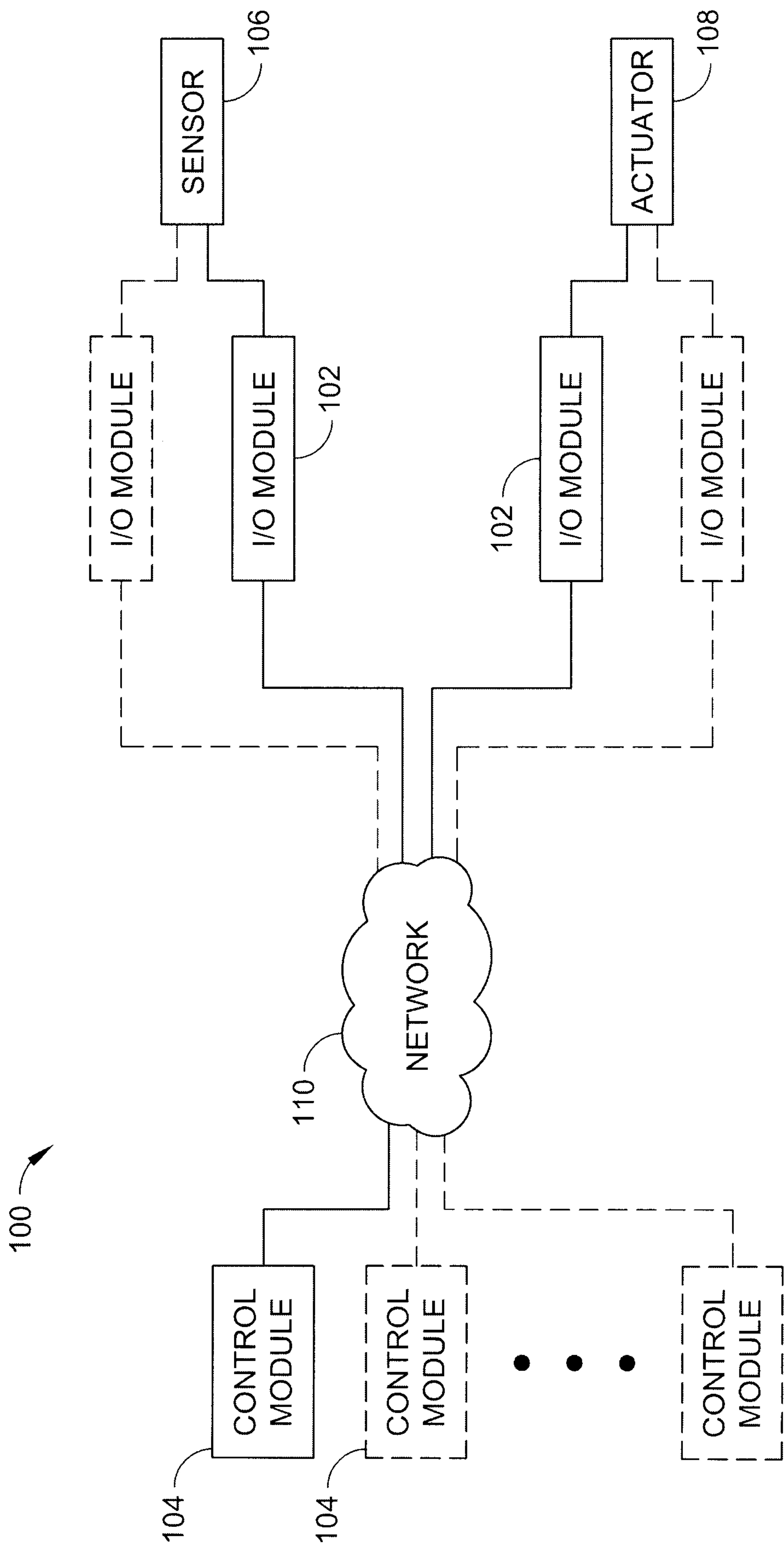


FIG. 2

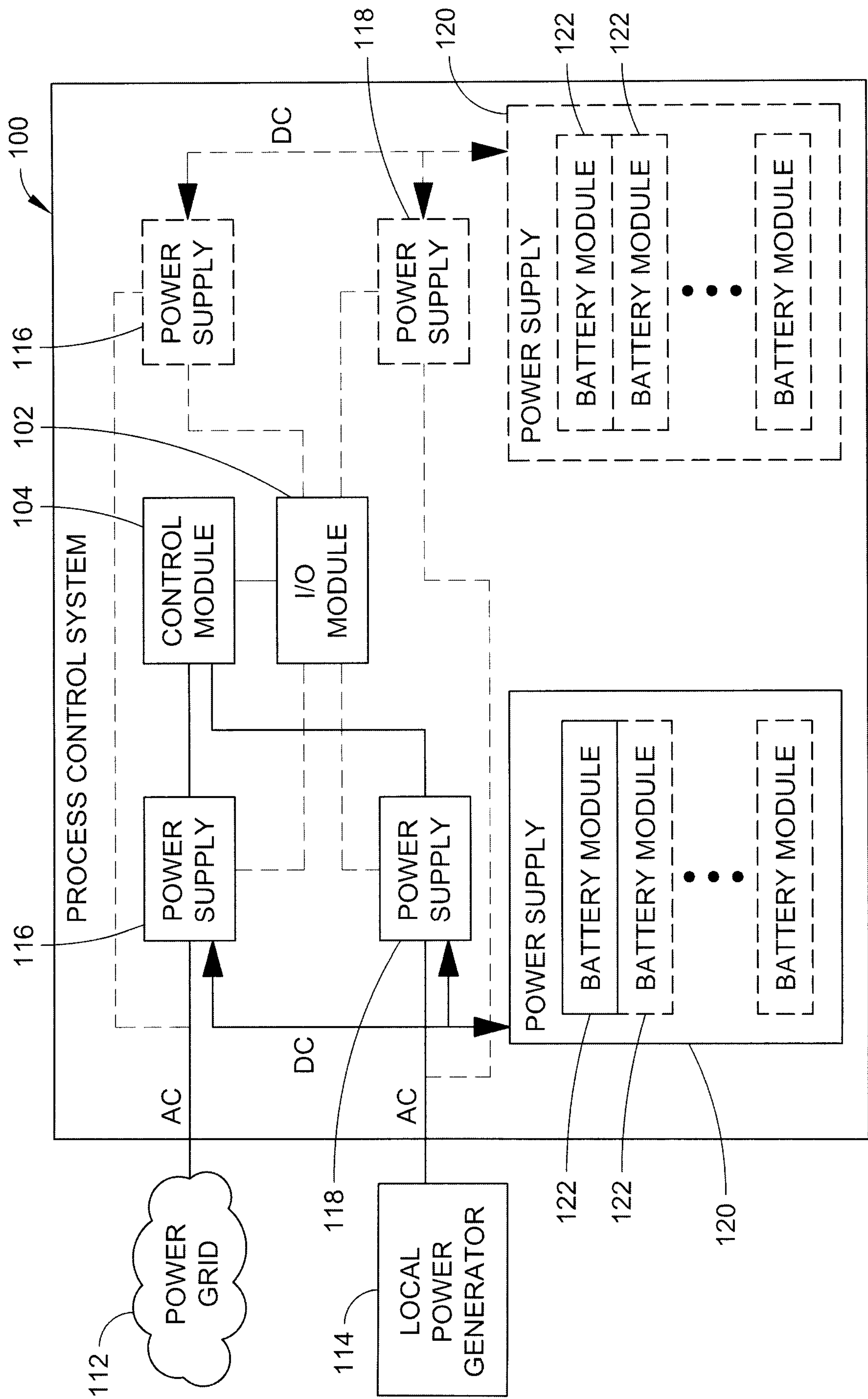
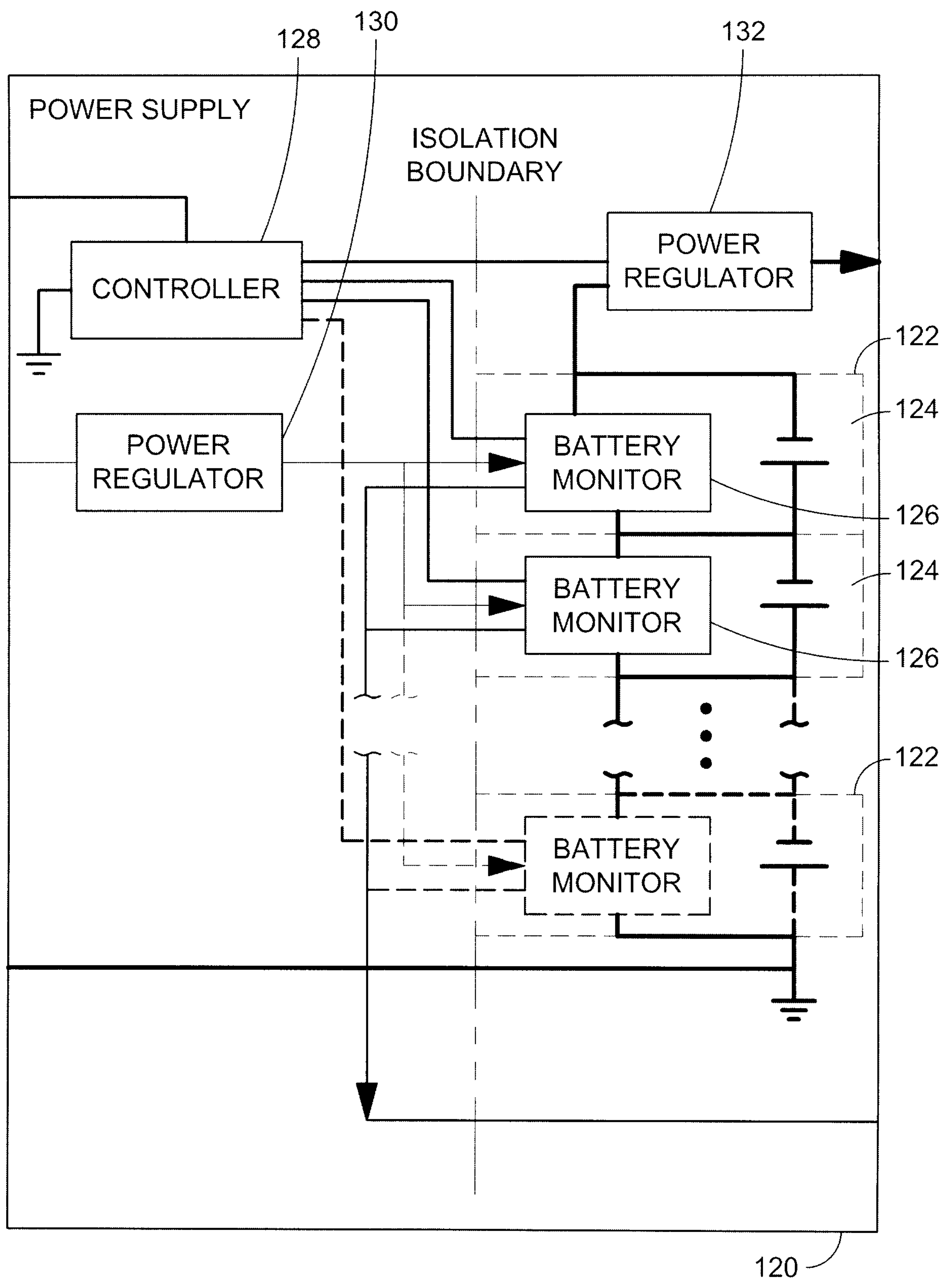


FIG. 3

**FIG. 4**

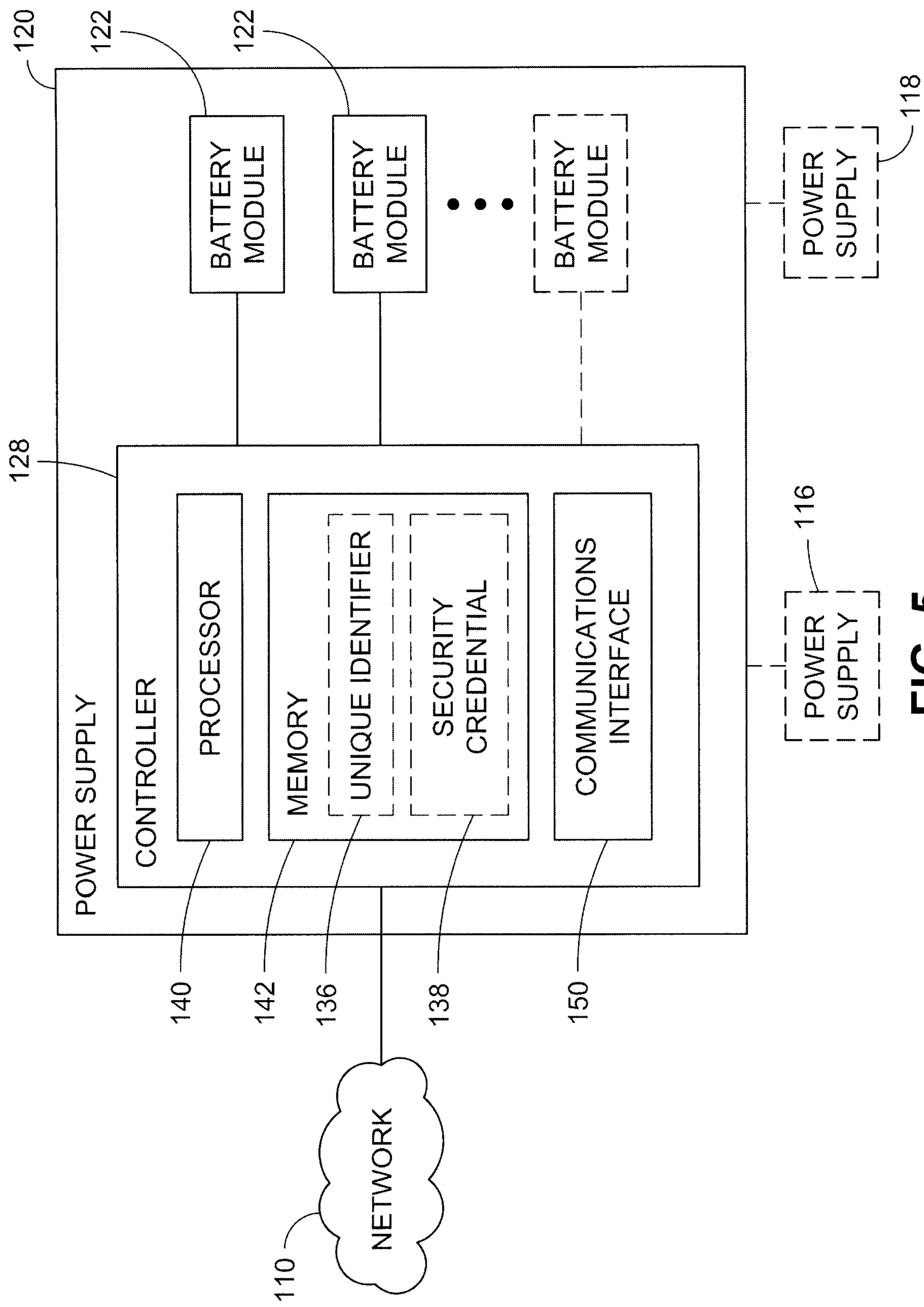


FIG. 5

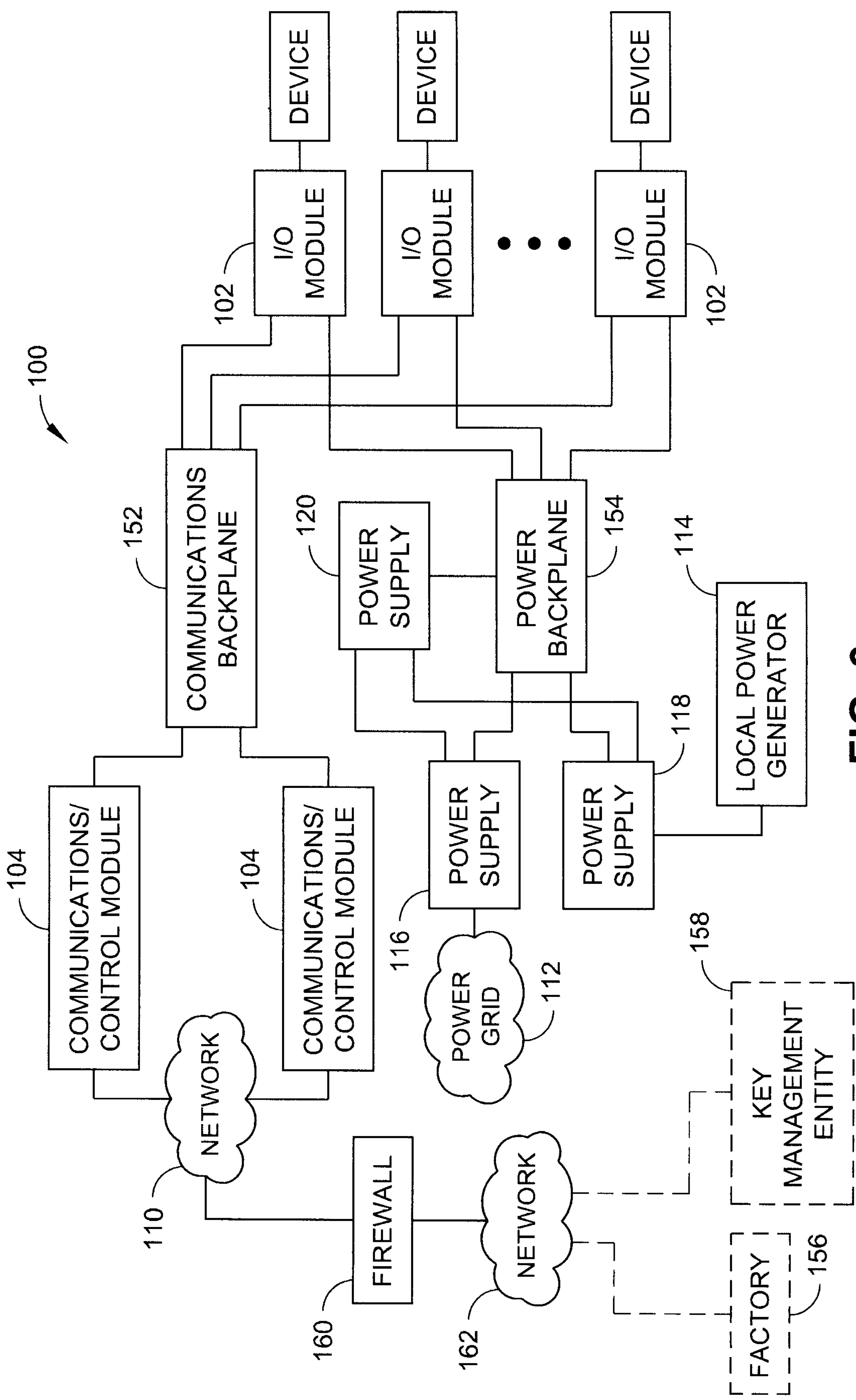


FIG. 6

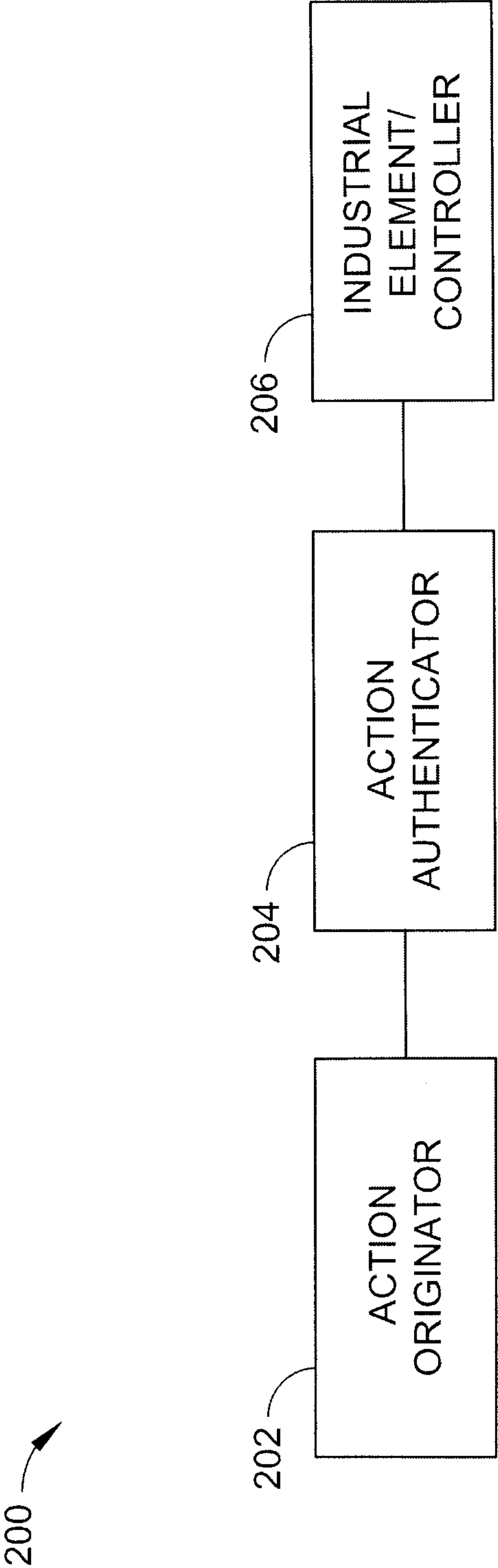


FIG. 7

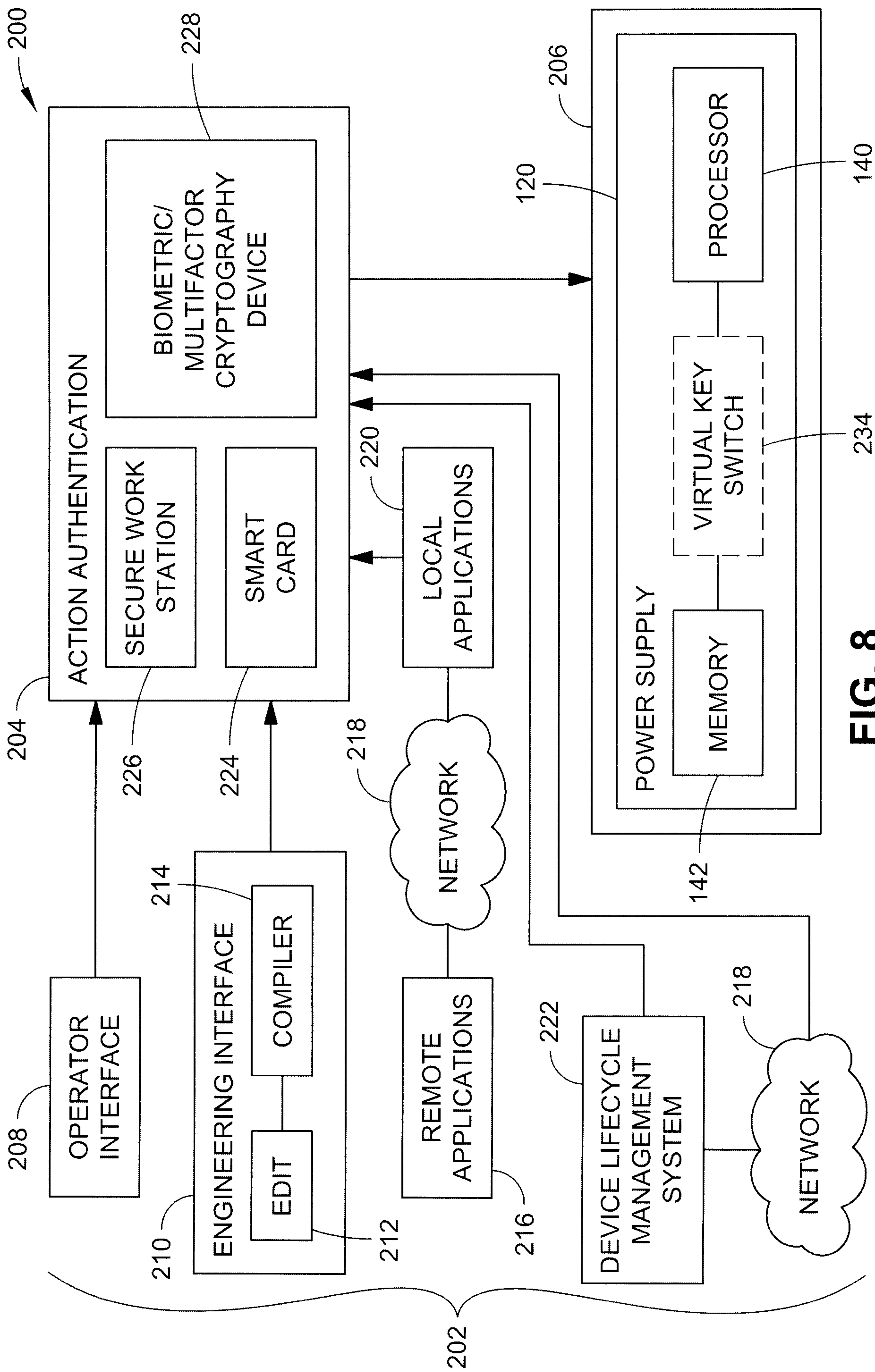
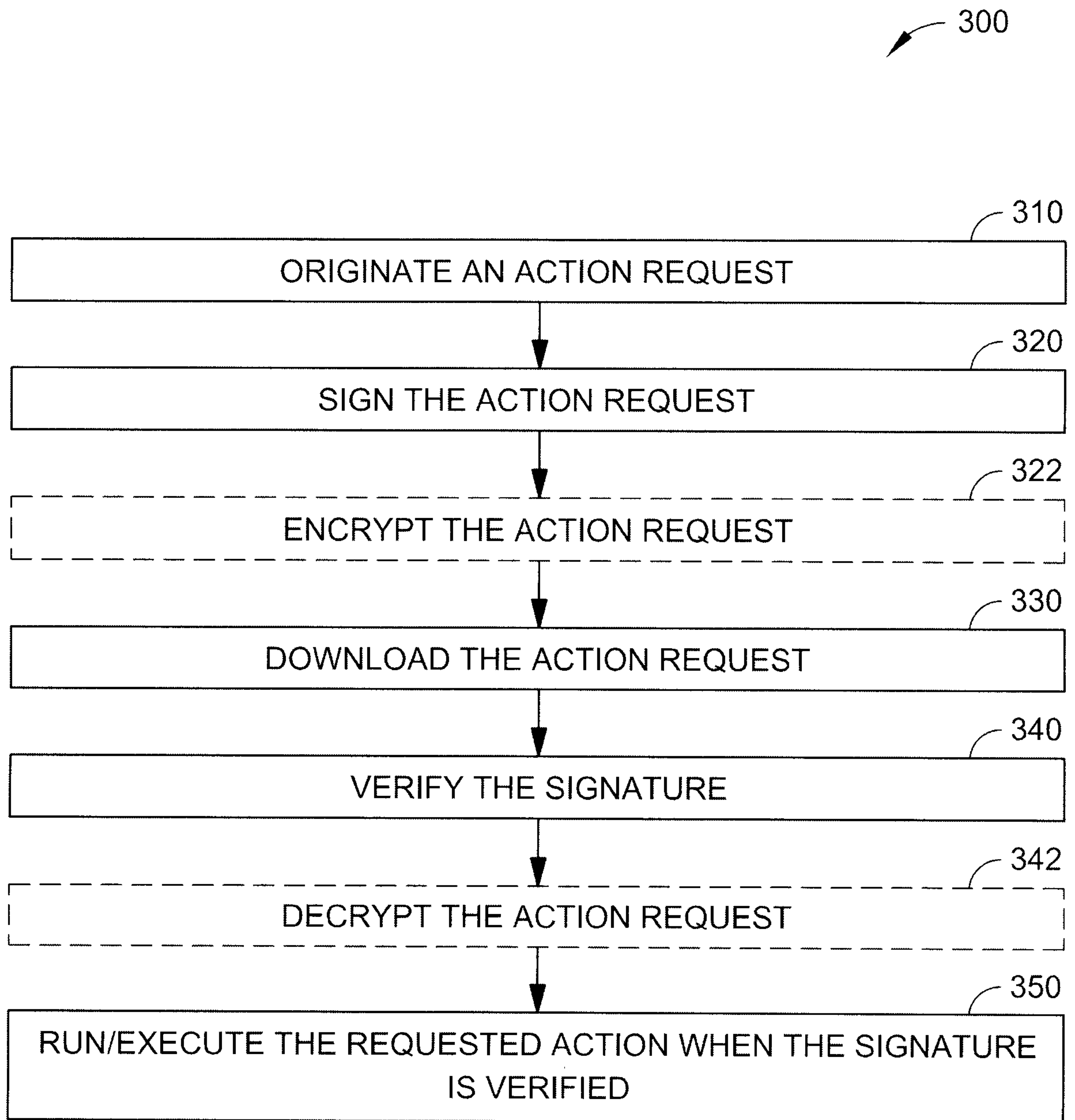


FIG. 8

**FIG. 9**

