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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 August 2016 (11.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/126573 A1

(51) International Patent Classification:
H04L 12/24 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2016/015890

(22) International Filing Date:
1 February 2016 (01.02.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/113,186 6 February 2015 (06.02.2015) US
14/871,732 30 September 2015 (30.09.2015) US

(71) Applicant: **HONEYWELL INTERNATIONAL INC.** [US/US]; Intellectual Property-Patent Services, 115 Tabor Road, M/S 4D3, P. O. Box 377, Morris Plains, NJ 07950 (US).

(72) Inventors: **TALAMANCHI, Venkata Srinivasulu Reddy**; Honeywell International Inc., Intellectual Property-Patent Services, 115 Tabor Road, M/S 4D3, P. O. Box 377, Morris Plains, NJ 07950 (US). **DIETRICH, Kenneth W.**; Honeywell International INC., Intellectual Property-Patent Services, 115 Tabor Road, M/S 4D3, P. O. Box 377, Morris Plains, NJ 07950 (US). **BOICE, Eric T.**; Honeywell International INC., Intellectual Property-Patent Services, 115 Tabor Road, M/S 4D3, P. O. Box 377, Morris Plains, NJ 07950 (US). **KOWALCZYK, Andrew W.**; Honeywell International INC., Intellectual Property-Patent Services, 115 Tabor Road, M/S 4D3, P. O. Box 377, Morris Plains, NJ 07950 (US). **GADHE, Ganesh P.**; Honeywell International INC., Intellectual Property-Patent Services, 115 Tabor Road, M/S 4D3, P. O. Box 377, Morris Plains, NJ 07950 (US).

(74) Agent: **BEATUS, Carrie**; Honeywell International INC., Intellectual Property-Patent Services, 115 Tabor Road, M/S 4D3, P. O. Box 377, Morris Plains, NJ 07950 (US).

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

[Continued on next page]

(54) Title: INFRASTRUCTURE MONITORING TOOL FOR COLLECTING INDUSTRIAL PROCESS CONTROL AND AUTOMATION SYSTEM RISK DATA

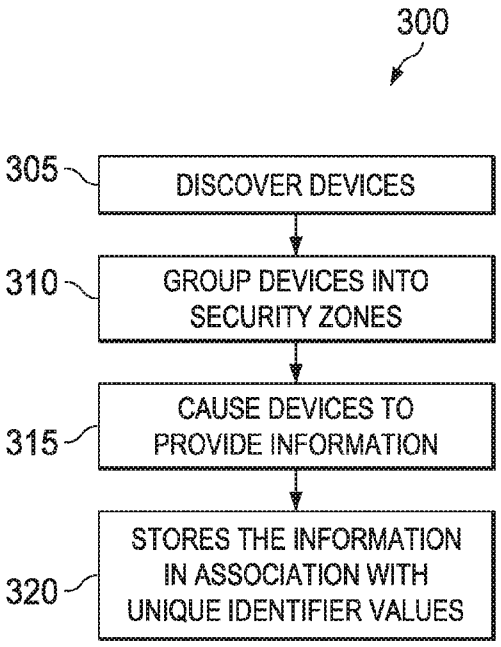

FIG. 3

(57) Abstract: This disclosure provides an infrastructure monitoring tool, and related systems and methods, for collecting industrial process control and automation system risk data, and other data. A method includes discovering (305) multiple devices in a computing system by a risk manager system (154). The method includes grouping (310) the multiple devices (220, 240) into multiple security zones by the risk manager system (154). The method includes, for each security zone, causing (315) one or more devices (220, 240) in that security zone to provide information to the risk manager system (154) identifying alerts and events associated with the one or more devices (220, 240). The method includes storing (320) the information, by the risk manager system (154), in association with unique identifier values, the unique identifier values identifying different types of information.

WO 2016/126573 A1

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

Published:

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

INFRASTRUCTURE MONITORING TOOL FOR COLLECTING INDUSTRIAL PROCESS CONTROL AND AUTOMATION SYSTEM RISK DATA

[0001] This application claims the benefit of the filing date of United States Provisional Patent Application 62/113,186, filed February 6, 2015, which is hereby incorporated by reference.

TECHNICAL FIELD

[0002] This disclosure relates generally to network security. More specifically, this disclosure relates to an infrastructure monitoring tool for collecting industrial process control and automation system risk data.

BACKGROUND

[0003] Processing facilities are often managed using industrial process control and automation systems. Conventional control and automation systems routinely include a variety of networked devices, such as servers, workstations, switches, routers, firewalls, safety systems, proprietary real-time controllers, and industrial field devices. Often times, this equipment comes from a number of different vendors. In industrial environments, cyber-security is of increasing concern, and unaddressed security vulnerabilities in any of these components could be exploited by attackers to disrupt operations or cause unsafe conditions in an industrial facility.

SUMMARY

[0004] This disclosure provides an infrastructure monitoring tool for collecting industrial process control and automation system risk data. A method includes discovering multiple devices in a computing system by a risk manager system. The method includes grouping the multiple devices into multiple security zones by the risk manager system. The method includes, for each security zone, causing one or more devices in that security zone to provide information to the risk manager system identifying alerts and events associated with the one or more devices. The method includes storing the information, by the risk manager system, in association with unique identifier values, the unique identifier values identifying different types of information.

[0005] In some embodiments, the risk manager system uses the System Center Operations Manager (SCOM) infrastructure monitoring software tool from MICROSOFT CORPORATION. In some embodiments, the risk manager system sends configuration data to the one or more devices in each security zone that defines the alerts and events to be provided by each device. In some embodiments, the one or more devices in that security zone provide information to the risk manager system at the time of discovery and also when additional events are later detected. In some embodiments, the one or more devices in that security zone provide information to the risk manager system at preconfigured intervals. In some embodiments, the risk manager system calculates risks based on the stored information by performing queries using the unique identifier values. In some embodiments, the risk manager system also categorizes the information collected from the one or more devices in each security zone to calculate risk values.

[0006] Other technical features may be readily apparent to one skilled in the art from the following figures, descriptions, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] For a more complete understanding of this disclosure, reference is now made to the following description, taken in conjunction with the accompanying drawings, in which:

[0008] FIGURE 1 illustrates an example industrial process control and automation system according to this disclosure;

[0009] FIGURE 2 illustrates an example infrastructure monitoring architecture to collect industrial process control and automation system risk data according to this disclosure; and

[0010] Figure 3 illustrates a flowchart of a process in accordance with disclosed embodiments.

DETAILED DESCRIPTION

[0011] The figures, discussed below, and the various embodiments used to describe the principles of the present invention in this patent document are by way of illustration only and should not be construed in any way to limit the scope of the invention. Those skilled in the art will understand that the principles of the invention may be implemented in any type of suitably arranged device or system.

[0012] FIGURE 1 illustrates an example industrial process control and automation system 100 according to this disclosure. As shown in FIGURE 1, the system 100 includes various components that facilitate production or processing of at least one product or other material. For instance, the system 100 is used here to facilitate control over components in one or multiple plants 101a-101n. Each plant 101a-101n represents one or more processing facilities (or one or more portions thereof), such as one or more manufacturing facilities for producing at least one product or other material. In general, each plant 101a-101n may implement one or more processes and can individually or collectively be referred to as a process system. A process system generally represents any system or portion thereof configured to process one or more products or other materials in some manner.

[0013] In FIGURE 1, the system 100 is implemented using the Purdue model of process control. In the Purdue model, "Level 0" may include one or more sensors 102a and one or more actuators 102b. The sensors 102a and actuators 102b represent components in a process system that may perform any of a wide variety of functions. For example, the sensors 102a could measure a wide variety of characteristics in the process system, such as temperature, pressure, or flow rate. Also, the actuators 102b could alter a wide variety of characteristics in the process system. The sensors 102a and actuators 102b could represent any other or additional components in any suitable process system. Each of the sensors 102a includes any suitable structure for measuring one or more characteristics in a process system. Each of the actuators 102b includes any suitable structure for operating on or affecting one or more conditions in a process system.

[0014] At least one network 104 is coupled to the sensors 102a and actuators 102b. The network 104 facilitates interaction with the sensors 102a and actuators 102b. For example, the network 104 could transport measurement data from the sensors 102a and

provide control signals to the actuators 102b. The network 104 could represent any suitable network or combination of networks. As particular examples, the network 104 could represent an Ethernet network, an electrical signal network (such as a HART or FOUNDATION FIELDBUS network), a pneumatic control signal network, or any other or additional type(s) of network(s).

[0015] In the Purdue model, "Level 1" may include one or more controllers 106, which are coupled to the network 104. Among other things, each controller 106 may use the measurements from one or more sensors 102a to control the operation of one or more actuators 102b. For example, a controller 106 could receive measurement data from one or more sensors 102a and use the measurement data to generate control signals for one or more actuators 102b. Each controller 106 includes any suitable structure for interacting with one or more sensors 102a and controlling one or more actuators 102b. Each controller 106 could, for example, represent a proportional-integral-derivative (PID) controller or a multivariable controller, such as a Robust Multivariable Predictive Control Technology (RMPCT) controller or other type of controller implementing model predictive control (MPC) or other advanced predictive control (APC). As a particular example, each controller 106 could represent a computing device running a real-time operating system.

[0016] Two networks 108 are coupled to the controllers 106. The networks 108 facilitate interaction with the controllers 106, such as by transporting data to and from the controllers 106. The networks 108 could represent any suitable networks or combination of networks. As a particular example, the networks 108 could represent a redundant pair of Ethernet networks, such as a FAULT TOLERANT ETHERNET (FTE) network from HONEYWELL INTERNATIONAL INC.

[0017] At least one switch/firewall 110 couples the networks 108 to two networks 112. The switch/firewall 110 may transport traffic from one network to another. The switch/firewall 110 may also block traffic on one network from reaching another network. The switch/firewall 110 includes any suitable structure for providing communication between networks, such as a HONEYWELL CONTROL FIREWALL (CF9) device. The networks 112 could represent any suitable networks, such as an FTE

network.

[0018] In the Purdue model, "Level 2" may include one or more machine-level controllers 114 coupled to the networks 112. The machine-level controllers 114 perform various functions to support the operation and control of the controllers 106, sensors 102a, and actuators 102b, which could be associated with a particular piece of industrial equipment (such as a boiler or other machine). For example, the machine-level controllers 114 could log information collected or generated by the controllers 106, such as measurement data from the sensors 102a or control signals for the actuators 102b. The machine-level controllers 114 could also execute applications that control the operation of the controllers 106, thereby controlling the operation of the actuators 102b. In addition, the machine-level controllers 114 could provide secure access to the controllers 106. Each of the machine-level controllers 114 includes any suitable structure for providing access to, control of, or operations related to a machine or other individual piece of equipment. Each of the machine-level controllers 114 could, for example, represent a server computing device running a MICROSOFT WINDOWS operating system. Although not shown, different machine-level controllers 114 could be used to control different pieces of equipment in a process system (where each piece of equipment is associated with one or more controllers 106, sensors 102a, and actuators 102b).

[0019] One or more operator stations 116 are coupled to the networks 112. The operator stations 116 represent computing or communication devices providing user access to the machine-level controllers 114, which could then provide user access to the controllers 106 (and possibly the sensors 102a and actuators 102b). As particular examples, the operator stations 116 could allow users to review the operational history of the sensors 102a and actuators 102b using information collected by the controllers 106 and/or the machine-level controllers 114. The operator stations 116 could also allow the users to adjust the operation of the sensors 102a, actuators 102b, controllers 106, or machine-level controllers 114. In addition, the operator stations 116 could receive and display warnings, alerts, or other messages or displays generated by the controllers 106 or the machine-level controllers 114. Each of the operator stations 116 includes any suitable structure for supporting user access and control of one or more components in the system 100. Each of the operator stations 116 could, for example, represent a computing device

running a MICROSOFT WINDOWS operating system.

[0020] At least one router/firewall 118 couples the networks 112 to two networks 120. The router/firewall 118 includes any suitable structure for providing communication between networks, such as a secure router or combination router/firewall. The networks 120 could represent any suitable networks, such as an FTE network.

[0021] In the Purdue model, "Level 3" may include one or more unit-level controllers 122 coupled to the networks 120. Each unit-level controller 122 is typically associated with a unit in a process system, which represents a collection of different machines operating together to implement at least part of a process. The unit-level controllers 122 perform various functions to support the operation and control of components in the lower levels. For example, the unit-level controllers 122 could log information collected or generated by the components in the lower levels, execute applications that control the components in the lower levels, and provide secure access to the components in the lower levels. Each of the unit-level controllers 122 includes any suitable structure for providing access to, control of, or operations related to one or more machines or other pieces of equipment in a process unit. Each of the unit-level controllers 122 could, for example, represent a server computing device running a MICROSOFT WINDOWS operating system. Although not shown, different unit-level controllers 122 could be used to control different units in a process system (where each unit is associated with one or more machine-level controllers 114, controllers 106, sensors 102a, and actuators 102b).

[0022] Access to the unit-level controllers 122 may be provided by one or more operator stations 124. Each of the operator stations 124 includes any suitable structure for supporting user access and control of one or more components in the system 100. Each of the operator stations 124 could, for example, represent a computing device running a MICROSOFT WINDOWS operating system.

[0023] At least one router/firewall 126 couples the networks 120 to two networks 128. The router/firewall 126 includes any suitable structure for providing communication between networks, such as a secure router or combination router/firewall. The networks 128 could represent any suitable networks, such as an FTE network.

[0024] In the Purdue model, "Level 4" may include one or more plant-level

controllers 130 coupled to the networks 128. Each plant-level controller 130 is typically associated with one of the plants 101a-101n, which may include one or more process units that implement the same, similar, or different processes. The plant-level controllers 130 perform various functions to support the operation and control of components in the lower levels. As particular examples, the plant-level controller 130 could execute one or more manufacturing execution system (MES) applications, scheduling applications, or other or additional plant or process control applications. Each of the plant-level controllers 130 includes any suitable structure for providing access to, control of, or operations related to one or more process units in a process plant. Each of the plant-level controllers 130 could, for example, represent a server computing device running a MICROSOFT WINDOWS operating system.

[0025] Access to the plant-level controllers 130 may be provided by one or more operator stations 132. Each of the operator stations 132 includes any suitable structure for supporting user access and control of one or more components in the system 100. Each of the operator stations 132 could, for example, represent a computing device running a MICROSOFT WINDOWS operating system.

[0026] At least one router/firewall 134 couples the networks 128 to one or more networks 136. The router/firewall 134 includes any suitable structure for providing communication between networks, such as a secure router or combination router/firewall. The network 136 could represent any suitable network, such as an enterprise-wide Ethernet or other network or all or a portion of a larger network (such as the Internet).

[0027] In the Purdue model, "Level 5" may include one or more enterprise-level controllers 138 coupled to the network 136. Each enterprise-level controller 138 is typically able to perform planning operations for multiple plants 101a-101n and to control various aspects of the plants 101a-101n. The enterprise-level controllers 138 can also perform various functions to support the operation and control of components in the plants 101a-101n. As particular examples, the enterprise-level controller 138 could execute one or more order processing applications, enterprise resource planning (ERP) applications, advanced planning and scheduling (APS) applications, or any other or additional enterprise control applications. Each of the enterprise-level controllers 138 includes any suitable structure for providing access to, control of, or operations related to

the control of one or more plants. Each of the enterprise-level controllers 138 could, for example, represent a server computing device running a MICROSOFT WINDOWS operating system. In this document, the term "enterprise" refers to an organization having one or more plants or other processing facilities to be managed. Note that if a single plant 101a is to be managed, the functionality of the enterprise-level controller 138 could be incorporated into the plant-level controller 130.

[0028] Access to the enterprise-level controllers 138 may be provided by one or more operator stations 140. Each of the operator stations 140 includes any suitable structure for supporting user access and control of one or more components in the system 100. Each of the operator stations 140 could, for example, represent a computing device running a MICROSOFT WINDOWS operating system.

[0029] Various levels of the Purdue model can include other components, such as one or more databases. The database(s) associated with each level could store any suitable information associated with that level or one or more other levels of the system 100. For example, a historian 141 can be coupled to the network 136. The historian 141 could represent a component that stores various information about the system 100. The historian 141 could, for instance, store information used during production scheduling and optimization. The historian 141 represents any suitable structure for storing and facilitating retrieval of information. Although shown as a single centralized component coupled to the network 136, the historian 141 could be located elsewhere in the system 100, or multiple historians could be distributed in different locations in the system 100.

[0030] In particular embodiments, the various controllers and operator stations in FIGURE 1 may represent computing devices. For example, each of the controllers 106, 114, 122, 130, 138 could include one or more processing devices 142 and one or more memories 144 for storing instructions and data used, generated, or collected by the processing device(s) 142. Each of the controllers 106, 114, 122, 130, 138 could also include at least one network interface 146, such as one or more Ethernet interfaces or wireless transceivers. Also, each of the operator stations 116, 124, 132, 140 could include one or more processing devices 148 and one or more memories 150 for storing instructions and data used, generated, or collected by the processing device(s) 148. Each of the operator stations 116, 124, 132, 140 could also include at least one network

interface 152, such as one or more Ethernet interfaces or wireless transceivers.

[0031] As noted above, cyber-security is of increasing concern with respect to industrial process control and automation systems. Unaddressed security vulnerabilities in any of the components in the system 100 could be exploited by attackers to disrupt operations or cause unsafe conditions in an industrial facility. For example, since process control and automation systems can be used to control industrial processes that are exothermic or that involve toxic chemicals or even nuclear power, a disruption to these processes can cause major economic or safety issues. However, in many instances, operators do not have a complete understanding or inventory of all equipment running at a particular industrial site. As a result, it is often difficult to quickly determine potential sources of risk to a control and automation system.

[0032] This disclosure recognizes a need for a solution that understands potential vulnerabilities in various systems, prioritizes the vulnerabilities based on risk to an overall system, and automatically/logically collects and categorizes this data. This is accomplished (among other ways) by using a risk manager 154. The risk manager 154 includes any suitable structure that supports the collection of industrial process control and automation system risk data. Here, the risk manager 154 includes one or more processing devices 156; one or more memories 158 for storing instructions and data used, generated, or collected by the processing device(s) 156; and at least one network interface 160. Each processing device 156 could represent a microprocessor, microcontroller, digital signal process, field programmable gate array, application specific integrated circuit, or discrete logic. Each memory 158 could represent a volatile or non-volatile storage and retrieval device, such as a random access memory or Flash memory. Each network interface 160 could represent an Ethernet interface, wireless transceiver, or other device facilitating external communication. The functionality of the risk manager 154 could be implemented using any suitable hardware or a combination of hardware and software/firmware instructions.

[0033] FIGURE 2 illustrates an example infrastructure monitoring architecture 200 to collect industrial process control and automation system risk data according to this disclosure. The architecture 200 could be supported or implemented using the risk manager 154. This architecture 200 collects and analyzes risk data associated with an

industrial process control and automation system to identify potential security issues to be resolved.

[0034] Architecture 200 includes, in this example, a server 210, network nodes 220, a rules engine 230, monitoring nodes 240, and a user system 250. Server 210 can be implemented as risk manager 154, or as another server data processing system, having such hardware components as a processing device(s), memory, and a network interface. User system 250, similarly, can be any data processing system configured to communicate with server 210 as described herein, and in particular for configuring the processes described herein, and can be also be implemented as risk manager 154. Note that user system 250, in some embodiments, can be implemented on the same physical system as server 210.

[0035] Server 210, for example as executed by the risk manager 154, collects various data from monitoring nodes 240, such as data from antivirus tools or application whitelisting tools, Windows security events, network security data (including states of switches, routers, firewalls, and intrusion detection/prevention systems), backup status, patching status, and asset policies. Other examples are shown as monitoring nodes 240, including workstations, whitelisting servers, antivirus systems, backup servers, and other security software. Similarly, network nodes 220 can also be monitored. Network nodes 220 can include switches, routers, intrusion prevention systems (IPSes) including firewalls, and other network devices, whether implemented in hardware or software.

[0036] To start monitoring the monitoring nodes 240, a configuration can be loaded into and received by server 210, such as by receiving it from user system 250, loading it from storage, receiving it from another device or process, or otherwise. This configuration can be pushed to the monitoring nodes 240 or network nodes 220 by server 210. The monitoring nodes 240, network nodes 220, and the server 210 know about configuration categories, and each type and subtype of data collection can have its own category identifier. Each node can include software or hardware systems that scan devices for known vulnerabilities on each device or software application (such as out-of-date Windows patches) and monitor the devices continuously for events with security implications (such as virus detections or Windows authentication failures). Areas of monitoring may include, but are not limited to, antivirus, application whitelisting,

Windows security events, network security (including state of switches, routers, firewalls, and intrusion detection/prevention systems), backup status, patching status and asset policies. Each node can translate events generated on its device into alerts and assigns its configuration identifier.

[0037] In some embodiments, the configuration information can include management packs that are used to lay out unique security/risk item data collection and the categorization of data that will be analyzed by the risk manager 154. The management packs can be configured for each category with a unique configuration identifier for each type of data to be collected. This configuration can be extendable. The management pack configuration, which can be transmitted to and executed on each of the nodes, translates events generated by the nodes or other monitored device into alerts/events that are securely sent to the server 210.

[0038] Server 210 can collect or receive this information, analyze the information, and present the information and the analysis results to an operator (such as an administrator), store the information and results, or transmit them to a user system 250. In various embodiments, the alerts/events are categorized and assigned unique identifiers that can be used by the risk manager 154 to poll and query the data for rules engine logic so that the data can be used to calculate risk items to be sent to a risk manager database.

[0039] In various embodiments, rules engine 230 uses data adapters 232 to translate data to and from each of the nodes, as necessary, so that the appropriate data can be sent to each node, and so that the data received from each node can be converted into a consistent format for use by server 210. By converting data into a consistent format, rules engine 154 can present a "dashboard" user interface by which the relative risks from each of the monitored nodes can be easily compared.

[0040] In some embodiments, the architecture 200 is implemented using the System Center Operations Manager (SCOM) infrastructure monitoring software tool from MICROSOFT CORPORATION. The SCOM tool is normally used to provide information for IT support staff to monitor and fix issues that are collected and reported. The risk manager 154 collects security- and process control-related data, and in some embodiments the SCOM tool is used for this unique and specific data collection. In these

embodiments, the risk manager 154 does not use the SCOM tool as an IT support system but rather as a very specific security and risk data collection system to support the risk manager's data organization requirements. Of course, the claimed embodiments are not limited to SCOM implementations unless specifically claimed, and those of skill in the art will appreciate that specific functions or operations described herein as relating to a SCOM tool implementation are not limited to the SCOM tool in particular, but also apply to other implementations of architecture 200 or risk manager 154.

[0041] In the process control and automation system 100, the SCOM tool (or other tool) is used to discover devices in the system 100 and to create a database of those devices, grouping the devices into security zones for further analysis. Once this discovery is completed, a management pack can be pushed or sent to a target device for specific security/risk item data collection. When the management pack is started in the monitoring service on the target device for security/risk, it creates a specific set of data that is sent to the SCOM tool based on preconfigured unique identifier values built into SCOM data packets. This process can be repeated for multiple target devices in the system. The data collected by the SCOM tool is utilized by the risk manager 154 based on the unique identifiers that are built into the data from the data collection points. In various embodiments, the design management packs can be specialized for SCOM product connectors.

[0042] Various data collection methods could be used by the risk manager 154. For example, data adapters 232 can be registered by the SCOM tool, and operational database queries can be made based on specific data collection. Each data adapter 232 can poll information in preconfigured intervals for its specific security/risk item values. Each operational database query can collect polling information in preconfigured intervals for its specific security/risk item values. This categorized and modular approach for collecting, organizing, and utilizing data in the SCOM tool is one factor that makes this a very different and unique use of the system or risk management tools including the SCOM tool. Once this data has been consumed by the risk manager 154, the data is separated and organized, and rules engine 230 can more efficiently calculate risk values using the collected data. Data adapters 232 can be used for respective data categories and can be registered with the SCOM tool, risk manager 154, or server 210. This enables

automation of the data items for use in a modular design, which helps to increase or maximize the system's data collection efficiency.

[0043] Figure 3 illustrates a flowchart of a process 300 in accordance with disclosed embodiments, that can be performed, for example, by risk manager 154, architecture 200, or other device configured to perform as described, including systems that implement some version of SCOM and are modified to perform as described, all of which are referred to generically as the "risk manager system" below.

[0044] The risk manager system discovers multiple devices in a computing system (305). These devices can include any of the devices described above as related to architecture 200 or system 100, including in particular any of the devices related to monitoring nodes 240 or network nodes 220.

[0045] The risk manager system groups the multiple devices into multiple security zones (310). The devices can be grouped into security zones according to, for example, the type of device, the type of risks presented by the devices, the severity of risks presented by the devices, or other similarities. In particular, security zones could include a security zone corresponding to monitoring nodes 240 and a security zone corresponding to network nodes 220.

[0046] For each security zone, the risk manager system causes one or more devices in that security zone to provide information identifying alerts and events associated with the one or more devices and receives this information (315). This can include, for example, by sending management packs or other configuration data to each of the devices that defines the alerts and events to be provided by that device. This information can include industrial process control and automation system risk data. In some cases, a specialized management pack or configuration can alert the risk manager system when there is a change to system software patches. The risk manager system can collect and convert relevant system events into risk alerts, and can get initial information of each device's risk data at discovery and detect additional events and later alert the system as and when those events are detected.

[0047] In various embodiments, this information and other alert data can be collected by a data adapter and polled at configured intervals by the server or rules engine so

that each respective item of information can be calculated by the rules engine.

[0048] The risk manager system stores the information in association with unique identifier values (320), the unique identifier values identifying different types of information. The information, or other event data or alert data, can be queried by the risk manager system using the unique identifier so that the rules engine can calculate risk based on the collected information.

[0049] In some embodiments, a monitoring agent can be installed on some or all of the monitored devices to monitor the device for the security or risk information. For devices where an agent cannot be installed, a server or other dedicated agent can be monitored the risk manager system, for example by reading the network device's configuration.

[0050] Although FIGURE 1 illustrates one example of an industrial process control and automation system 100, various changes may be made to FIGURE 1. For example, a control and automation system could include any number of sensors, actuators, controllers, servers, operator stations, networks, risk managers, and other components. Also, the makeup and arrangement of the system 100 in FIGURE 1 is for illustration only. Components could be added, omitted, combined, or placed in any other suitable configuration according to particular needs. Further, particular functions have been described as being performed by particular components of the system 100. This is for illustration only. In general, control and automation systems are highly configurable and can be configured in any suitable manner according to particular needs. In addition, FIGURE 1 illustrates an example environment in which the functions of the risk manager 154 can be used. This functionality can be used in any other suitable device or system.

[0051] Although FIGURE 2 illustrates one example of an infrastructure monitoring architecture 200 to collect industrial process control and automation system risk data, various changes may be made to FIGURE 2. For example, the functional division of the components and sub-components in FIGURE 2 are for illustration only. Various components or sub-components could be combined, further subdivided, rearranged, or omitted and additional components or sub-components could be added according to particular needs.

[0052] Note that the risk manager 154 and/or the infrastructure monitoring

architecture 200 shown here could use or operate in conjunction with any combination or all of various features described in the following previously-filed and concurrently-filed patent applications (all of which are hereby incorporated by reference):

- U.S. Patent Application No. 14/482,888 entitled "DYNAMIC QUANTIFICATION OF CYBER-SECURITY RISKS IN A CONTROL SYSTEM";
- U.S. Provisional Patent Application No. 62/036,920 entitled "ANALYZING CYBER-SECURITY RISKS IN AN INDUSTRIAL CONTROL ENVIRONMENT";
- U.S. Provisional Patent Application No. 62/113,075 entitled "RULES ENGINE FOR CONVERTING SYSTEM-RELATED CHARACTERISTICS AND EVENTS INTO CYBER-SECURITY RISK ASSESSMENT VALUES" and corresponding non-provisional U.S. Patent Application 14/871,695 of like title (Docket No. H0048932-0115) filed concurrently herewith;
- U.S. Provisional Patent Application No. 62/113,221 entitled "NOTIFICATION SUBSYSTEM FOR GENERATING CONSOLIDATED, FILTERED, AND RELEVANT SECURITY RISK-BASED NOTIFICATIONS" and corresponding non-provisional U.S. Patent Application 14/871,521 of like title (Docket No. H0048937-0115) filed concurrently herewith;
- U.S. Provisional Patent Application No. 62/113,100 entitled "TECHNIQUE FOR USING INFRASTRUCTURE MONITORING SOFTWARE TO COLLECT CYBER-SECURITY RISK DATA" and corresponding non-provisional U.S. Patent Application 14/871,855 of like title (Docket No. H0048943-0115) filed concurrently herewith;
- U.S. Provisional Patent Application No. 62/113,165 entitled "PATCH MONITORING AND ANALYSIS" and corresponding non-provisional U.S. Patent Application 14/871,921 of like title (Docket No. H0048973-0115) filed concurrently herewith;
- U.S. Provisional Patent Application No. 62/113,152 entitled "APPARATUS AND METHOD FOR AUTOMATIC HANDLING OF CYBER-SECURITY RISK EVENTS" and corresponding non-provisional U.S. Patent Application 14/871,503 of like title (Docket No. H0049067-0115) filed concurrently herewith;
- U.S. Provisional Patent Application No. 62/114,928 entitled "APPARATUS AND METHOD FOR DYNAMIC CUSTOMIZATION OF CYBER-SECURITY RISK

ITEM RULES" and corresponding non-provisional U.S. Patent Application 14/871,605 of like title (Docket No. H0049099-0115) filed concurrently herewith;

• U.S. Provisional Patent Application No. 62/114,865 entitled "APPARATUS AND METHOD FOR PROVIDING POSSIBLE CAUSES, RECOMMENDED ACTIONS, AND POTENTIAL IMPACTS RELATED TO IDENTIFIED CYBER-SECURITY RISK ITEMS" and corresponding non-provisional U.S. Patent Application 14/871,814 of like title (Docket No. H0049103-0115) filed concurrently herewith;

• U.S. Provisional Patent Application No. 62/114,937 entitled "APPARATUS AND METHOD FOR TYING CYBER-SECURITY RISK ANALYSIS TO COMMON RISK METHODOLOGIES AND RISK LEVELS" and corresponding non-provisional U.S. Patent Application 14/871,136 of like title (Docket No. H0049104-0115) filed concurrently herewith; and

• U.S. Provisional Patent Application No. 62/116,245 entitled "RISK MANAGEMENT IN AN AIR-GAPPED ENVIRONMENT" and corresponding non-provisional U.S. Patent Application 14/871,547 of like title (Docket No. H0049081-0115) filed concurrently herewith.

[0053] In some embodiments, various functions described in this patent document are implemented or supported by a computer program that is formed from computer readable program code and that is embodied in a computer readable medium. The phrase "computer readable program code" includes any type of computer code, including source code, object code, and executable code. The phrase "computer readable medium" includes any type of medium capable of being accessed by a computer, such as read only memory (ROM), random access memory (RAM), a hard disk drive, a compact disc (CD), a digital video disc (DVD), or any other type of memory. A "non-transitory" computer readable medium excludes wired, wireless, optical, or other communication links that transport transitory electrical or other signals. A non-transitory computer readable medium includes media where data can be permanently stored and media where data can be stored and later overwritten, such as a rewritable optical disc or an erasable memory device.

[0054] It may be advantageous to set forth definitions of certain words and phrases used throughout this patent document. The terms "application" and "program" refer to one or more computer programs, software components, sets of instructions, procedures,

functions, objects, classes, instances, related data, or a portion thereof adapted for implementation in a suitable computer code (including source code, object code, or executable code). The term "communicate," as well as derivatives thereof, encompasses both direct and indirect communication. The terms "include" and "comprise," as well as derivatives thereof, mean inclusion without limitation. The term "or" is inclusive, meaning and/or. The phrase "associated with," as well as derivatives thereof, may mean to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property of, have a relationship to or with, or the like. The phrase "at least one of," when used with a list of items, means that different combinations of one or more of the listed items may be used, and only one item in the list may be needed. For example, "at least one of: A, B, and C" includes any of the following combinations: A, B, C, A and B, A and C, B and C, and A and B and C.

[0055] While this disclosure has described certain embodiments and generally associated methods, alterations and permutations of these embodiments and methods will be apparent to those skilled in the art. Accordingly, the above description of example embodiments does not define or constrain this disclosure. Other changes, substitutions, and alterations are also possible without departing from the spirit and scope of this disclosure, as defined by the following claims.

WHAT IS CLAIMED IS:

1. A method comprising:

discovering (305) multiple devices in a computing system by a risk manager system (154);

grouping (310) the multiple devices (220, 240) into multiple security zones by the risk manager system (154);

for each security zone, causing (315) one or more devices (220, 240) in that security zone to provide information to the risk manager system (154) identifying alerts and events associated with the one or more devices (220, 240); and

storing (320) the information, by the risk manager system (154), in association with unique identifier values, the unique identifier values identifying different types of information.

2. The method of claim 1, wherein the risk manager system (154) uses the System Center Operations Manager (SCOM) infrastructure monitoring software tool from MICROSOFT CORPORATION.

3. The method of claim 1, further comprising sending configuration data to the one or more devices (220, 240) in each security zone that defines the alerts and events to be provided by each device (220, 240).

4. The method of claim 1, wherein the one or more devices (220, 240) in that security zone provide information to the risk manager system (154) at the time of discovery and also when additional events are later detected.

5. The method of claim 1, wherein the one or more devices (220, 240) in that security zone provide information to the risk manager system (154) at preconfigured intervals.

6. The method of claim 1, further comprising calculating risks based on the stored information by performing queries using the unique identifier values.

7. The method of claim 1, further comprising categorizing the information collected from the one or more devices in each security zone to calculate risk values.

8. A risk manager system (154) comprising:

a controller (156); and

a display, the risk manager system (154) configured to

discover (305) multiple devices in a computing system;

group (310) the multiple devices (220, 240) into multiple security zones;

for each security zone, cause (315) one or more devices (220, 240) in that security zone to provide information identifying alerts and events associated with the one or more devices (220, 240); and

store (320) the information in association with unique identifier values, the unique identifier values identifying different types of information.

9. The risk manager system of claim 8, wherein the risk manager system (154) uses the System Center Operations Manager (SCOM) infrastructure monitoring software tool from MICROSOFT CORPORATION.

10. The risk manager system of claim 8, wherein the risk manager system (154) sends configuration data to the one or more devices (220, 240) in each security zone that defines the alerts and events to be provided by each device (220, 240).

11. The risk manager system of claim 8, wherein the one or more devices (220, 240) in that security zone provide information to the risk manager system (154) at the time of discovery and also when additional events are later detected.

12. The risk manager system of claim 8, wherein the one or more devices (220, 240) in that security zone provide information to the risk manager system (154) at preconfigured intervals.

13. The risk manager system of claim 8, wherein the risk manager system (154) calculates risks based on the stored information by performing queries using the unique identifier values.

14. The risk manager system of claim 8, wherein the risk manager system (154) also categorizes the information collected from the one or more devices in each security zone to calculate risk values.

15. A non-transitory machine-readable medium (158) encoded with executable instructions that, when executed, cause one or more processors (156) of a risk manager system (154) to:

discover (305) multiple devices in a computing system;

group (310) the multiple devices (220, 240) into multiple security zones;

for each security zone, cause (315) one or more devices (220, 240) in that security zone to provide information identifying alerts and events associated with the one or more devices (220, 240); and

store (320) the information in association with unique identifier values, the unique identifier values identifying different types of information.

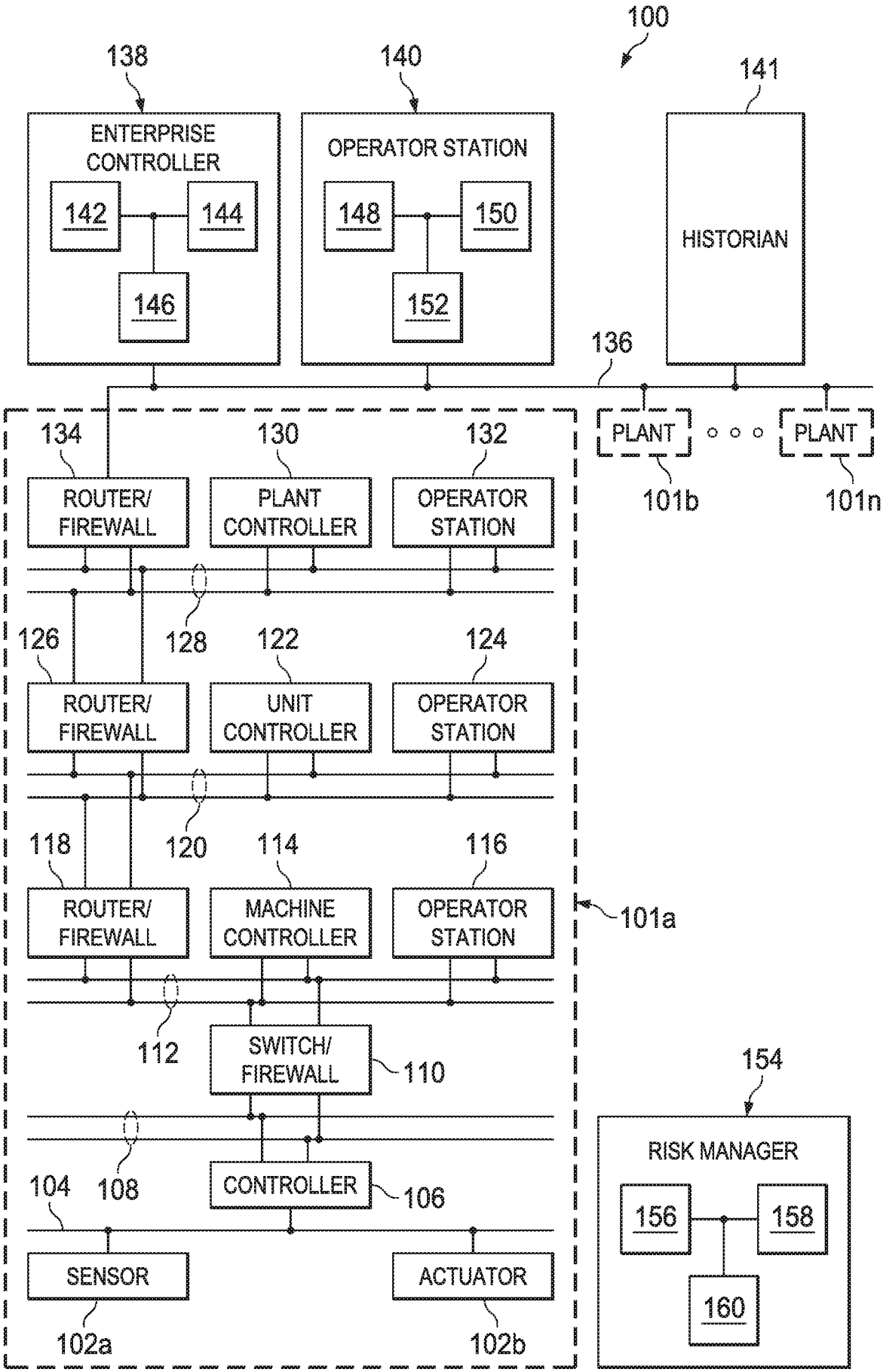
100
138
140
141
ENTERPRISE CONTROLLER
142
144
146
OPERATOR STATION
148
150
152
HISTORIAN
136
PLANT
PLANT
101b
101n
134
130
132
ROUTER/ FIREWALL
PLANT CONTROLLER
OPERATOR STATION
128
126
122
124
ROUTER/ FIREWALL
UNIT CONTROLLER
OPERATOR STATION
120
118
114
116
ROUTER/ FIREWALL
MACHINE CONTROLLER
OPERATOR STATION
101a
112
SWITCH/ FIREWALL
110
154
RISK MANAGER
156
158
160
108
104
CONTROLLER
106
SENSOR
ACTUATOR
102a
102b

FIG. 1

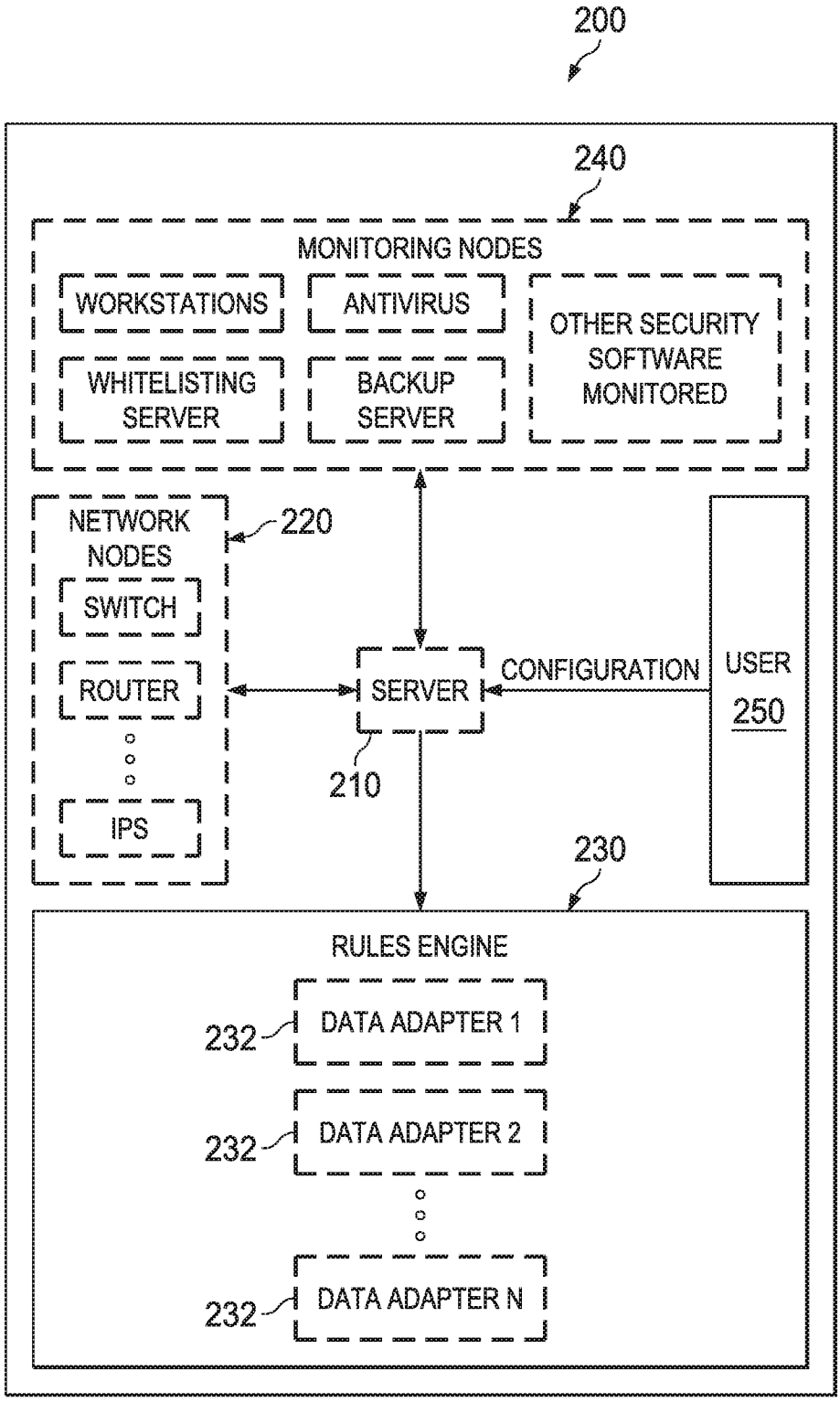
200
240
MONITORING NODES
WORKSTATIONS
ANTIVIRUS
OTHER SECURITY SOFTWARE MONITORED
WHITELISTING SERVER
BACKUP SERVER
NETWORK NODES
220
SWITCH
ROUTER
IPS
SERVER
210
CONFIGURATION
USER
250
230
RULES ENGINE
232
DATA ADAPTER 1
232
DATA ADAPTER 2
232
DATA ADAPTER N

FIG. 2

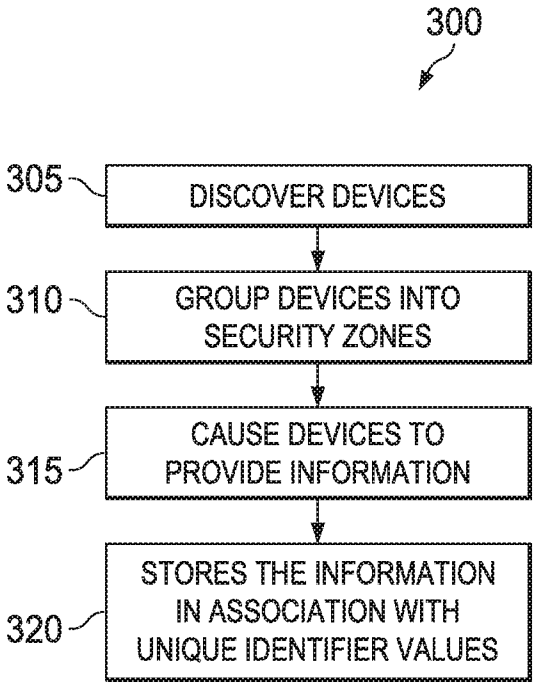
300
305
DISCOVER DEVICES
310
GROUP DEVICES INTO SECURITY ZONES
315
CAUSE DEVICES TO PROVIDE INFORMATION
320
STORES THE INFORMATION IN ASSOCIATION WITH UNIQUE IDENTIFIER VALUES

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/015890

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(2006.01)i, H04L 29/06(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 12/24; G06F 15/16; H04L 9/00; G06F 9/455; H04L 12/803; H04L 12/28; G08B 23/00; H04L 29/06

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: grouping devices, security, zones, risk, manager, SCOM, information, alert, event

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006-0123482 A1 (JEFFREY AARON) 08 June 2006 See paragraphs [0036]-[0037], [0048]-[0049], [0051], [0056]; and figure 1.	1-15
Y	US 2006-0174121 A1 (KOJI OMAE et al.) 03 August 2006 See paragraphs [0008], [0043]-[0047]; and figure 1.	1-15
Y	US 2008-0262822 A1 (JONATHAN C. HARDWICK et al.) 23 October 2008 See paragraphs [0027]-[0031]; and figures 1-2.	2,9
A	KR 10-2014-0097691 A (IDEAWARE INC.) 07 August 2014 See paragraphs [0061]-[0072]; and figures 6-10.	1-15
A	US 2007-0223398 A1 (YUJIN LUO et al.) 27 September 2007 See paragraphs [0009], [0033]-[0036]; and figures 1-2.	1-15

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

☒ See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
13 May 2016 (13.05.2016)	**13 May 2016 (13.05.2016)**

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

Authorized officer
YANG, Jeong Rok
Telephone No. +82-42-481-5709

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2016/015890

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0123482 A1	08/06/2006	US 7549162 B2	16/06/2009
US 2006-0174121 A1	03/08/2006	CN 100583735 C	20/01/2010
		CN 1805332 A	19/07/2006
		EP 1679843 A1	12/07/2006
		EP 1679843 B1	10/10/2012
		JP 2006-197025 A	27/07/2006
		JP 4756865 B2	24/08/2011
		US 7647036 B2	12/01/2010
US 2008-0262822 A1	23/10/2008	US 7996204 B2	09/08/2011
KR 10-2014-0097691 A	07/08/2014	WO 2014-119912 A1	07/08/2014
		WO 2014-119912 A4	02/10/2014
US 2007-0223398 A1	27/09/2007	CN 100340084 C	26/09/2007
		CN 1691603 A	02/11/2005
		DE 602005027458 D1	26/05/2011
		EP 1758304 A1	28/02/2007
		EP 1758304 A4	02/12/2009
		EP 1758304 B1	13/04/2011
		JP 2008-500607 A	10/01/2008
		KR 10-0799222 B1	29/01/2008
		KR 10-2007-0014162 A	31/01/2007
		US 7987360 B2	26/07/2011
		WO 2005-107162 A1	10/11/2005