Abstract: This disclosure provides systems and methods for tying cyber-security risk analysis to common risk methodologies and risk levels. A method includes identifying (305) a plurality of connected devices (106, 114, 122, 130, 138) that are vulnerable to cyber-security risks and identifying (310) cyber-security risks in the connected devices (106, 114, 122, 130, 138). The method includes assigning (314) a risk level to each of the identified cyber-security risks and comparing (320) the risk levels to a first threshold (202) and to a second threshold (204). The method includes assigning (325) each identified cyber-security risk to a risk classification; (222, 224, 226) and displaying (330) a user interface that includes a notification (220) according to the identified cyber-security risks and the corresponding assigned risk classifications (222, 224, 226).
before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

Published:

— with international search report (Art. 21(3))
APPARATUS AND METHOD FOR TYING CYBER-SECURITY RISK ANALYSIS TO COMMON RISK METHODOLOGIES AND RISK LEVELS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of the filing date of United States Provisional Patent Application 62/149,937, filed February 11, 2015, which is hereby incorporated by reference.

TECHNICAL FIELD

[0002] This disclosure relates generally to network security. More specifically, this disclosure relates to an apparatus and method for tying cyber-security risk analysis to common risk methodologies and risk levels.

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 apparatuses and methods for tying cyber-security risk analysis to common risk methodologies and risk levels. One embodiment includes a method that includes obtaining a first threshold value and a second threshold value associated with cyber-security risks to computing devices in an industrial process control and automation system. The method includes generating a first type of notification when a risk value associated with a specified cyber-security risk exceeds the first threshold value but not the second threshold value. The method includes generating a second type of notification when the risk value associated with the specified cyber-security risk exceeds the first and second threshold values, the second type of notification having a higher priority than the first type of notification.

[0005] Another disclosed method, and corresponding systems and machine-readable media, include identifying a plurality of connected devices, by a risk manager system, that are vulnerable to cyber-security risks. The method includes identifying, by the risk manager system, cyber-security risks in the connected devices. The method includes assigning, by the risk manager system, a risk level to each of the identified cyber-security risks. The method includes, for each identified cyber-security risk, comparing by the risk manager system the assigned risk level to a first threshold and to a second threshold. The method includes based on the comparisons, assigning each identified cyber-security risk to a risk classification by the risk manager system. The method includes displaying, by the risk manager system, a user interface that includes a notification according to the identified cyber-security risks and the corresponding assigned risk classifications. In various embodiments, the first threshold is a risk appetite and the second threshold is a risk tolerance. In various embodiments, the risk manager system also receives the first and second threshold from a user. In various embodiments, the risk manager system assigns identified cyber-security risks with an assigned risk level that is less than both the first threshold and the second threshold to a low-priority classification or a notification classification. In various embodiments, the risk manager system assigns identified cyber-security risks with an assigned risk level that is greater than or equal to the first threshold bus is less than the second threshold to a warning classification. In various embodiments, the risk manager system assigns identified cyber-security risks with an assigned risk level that is greater than or equal to both the first threshold and the second threshold to an alert.
classification. In various **embodiments**, the risk manager system prompts a user for an action in response to displaying the notification.

[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 graphical user interface for tying risk analysis to common risk methodologies and risk levels 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 IOla-IOln. Each plant IOla-IOln 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 IOla-IOln 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 types) 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.
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).

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 contrailers 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.

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 10a-10n, 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.

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.

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).

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 10a-10ln and to control various aspects of the plants 10a-10ln. The enterprise-level controllers 138 can also perform various functions to support the operation and control of components in the plants 10a-10ln. 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.
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. 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.

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 guides a user to mitigate the vulnerabilities. Moreover, a quantification of "cyber-security risk" has little value unless it both aligns with established organizational risk policies and aligns with recognized risk methodologies and standards. In other words, additional context for a risk score is often needed in order to effectively portray what a risk means to an organization.

This is accomplished (among other ways) using a risk manager 154. Among other things, the risk manager 154 supports a technique for tying risk analysis to common risk methodologies and risk levels. The risk manager 154 includes any suitable structure that supports automatic handling of cyber-security risk events. 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.

In some embodiments, how risk matters to an organization is determined through the use of two threshold values: risk appetite and risk tolerance. These thresholds dictate when an organization is capable of absorbing risk and when action needs to be
taken. For example, if below an organization’s risk appetite, a risk is acceptable. If above the risk appetite, the risk should be addressed. The risk tolerance is a higher threshold that determines when a risk has become dangerously high, action should still be taken but now with increased urgency.

[0035] Within the risk manager 154, risk appetite and risk tolerance can denote user-configurable parameters that are used as the thresholds for risk item notifications, and these can be defined for each type or classification of risk. In some embodiments, the values of risk appetite and risk tolerance are used as threshold points for alarming and notification. When below the risk appetite, items are of low priority. When above the risk appetite but below the risk tolerance, the items become warnings. Above the risk tolerance, the items become alerts.

[0036] 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.

[0037] Figure 2 illustrates an example graphical user interface 200 for tying risk analysis to common risk methodologies and risk levels according to this disclosure. In this user interface 200, different colors or other indicators could be used to represent these different conditions. For example, blue can represent risk items with risk values below the risk appetite, yellow can represent risk items with risk values above the risk appetite and below the risk tolerance, and red can represent risk items with risk values above the risk tolerance. The graphical user interface 200 also includes various summaries that identify different types of notifications by zone, by area, and by
This figure illustrates a risk appetite 202 (also referred to herein as the first threshold) and a risk tolerance 204 (also referred to herein as a second threshold) in a "risk by zone" area 210. As shown in this example, some risks in particular zones are below the risk appetite 202, and so indicate a low priority. Some risks in particular zones are above the risk appetite 202 but below the risk tolerance 204, and so indicate a warning. Some risks in particular zones are above both the risk appetite 202 and the risk tolerance 204, and so indicate an alert.

Figure 2 also illustrates a notification area 220. The risk appetite and risk threshold values can be utilized to trigger notifications, warnings, and alerts. For example, low-priority items below the risk appetite 202 may require no action but could result in a general notification 222. In this example, general notification 222 is displayed as a circle, and can be in a particular color, such as blue. Items above the risk appetite but below the risk tolerance may require action and therefore trigger a warning notification and prompt a user for action. In this example, warning 224 is displayed as a triangle, and can be in a particular color, such as orange. Above the risk tolerance can trigger an alert notification with a higher urgency and priority. In this example, warning 226 is displayed as an inverted triangle, and can be in a particular color, such as red. Each of these indicators can display the number of notifications, warnings, or alerts that have been detected. Of course, in different implementations, different shapes or colors may be used according to the user or designer's preference. In various embodiments, the system can receive a user input such as a selection of one of the notifications and, in response, will display details of the corresponding notifications, warnings, or alerts.

The configuration of the risk appetite and risk tolerance thresholds may preclude the need to alter the consistent elements of risk quantification (vulnerability and threat). It also adds an organization-specific context that determines what a risk score means, rather than trying to change the risk score itself. The risk tolerance threshold can also be adjusted in response to an observed threat level. For instance, during a period of a cyber-incident or relevant disclosure, the overall threat level to an organization is higher, there may be less tolerance to risk, and the risk tolerance threshold can be lowered accordingly.
[0041] Although Figure 2 illustrates one example of a graphical user interface 200 for tying risk analysis to common risk methodologies and risk levels, various changes may be made to Figure 2. For example, the content and arrangement of the graphical user interface 200 are for illustration only. Different gauges, charts, or other indicators could be used to identify items related to cyber-security.

[0042] Figure 3 illustrates a flowchart of a method 300 in accordance with disclosed embodiments, as can be performed, for example, by risk manager 154 or other device or controller (referred to as the "system" below).

[0043] The system identifies a plurality of connected devices that are vulnerable to cyber-security risks (305). These could be any of the devices or components as illustrated in Figure 1, or others. The devices can each be associated with a zone of a system such as system 100.

[0044] The system identifies cyber-security risks in the connected devices (310).

[0045] The system assigns a risk level (also referred to as a risk value or risk assessment value) to each of the identified cyber-security risks (315).

[0046] For each identified cyber-security risk, the system compares the assigned risk level to a first threshold and to a second threshold (320). The first threshold can be a risk appetite and the second threshold can be a risk tolerance. The first threshold and second threshold can be threshold values associated with cyber-security risks to computing devices in an industrial process control and automation system. The system can also obtain or receive the first and second threshold, such as by receiving them from a user.

[0047] Based on the comparisons, the system assigns each identified cyber-security risk to a risk classification (325). This can include assigning identified cyber-security risks with an assigned risk level that is less than both the first threshold and the second threshold to a low-priority classification or a notification classification. This can include assigning identified cyber-security risks with an assigned risk level that is greater than or equal to the first threshold bus is less than the second threshold to a warning classification. This can include assigning identified cyber-security risks with an assigned risk level that is greater than or equal to both the first threshold and the second threshold
an alert classification. Of course, this example of the comparison assumes that a
higher risk level means a more severe risk, and other embodiments could use an opposite
notation so that values lower than the thresholds indicate a more severe or alert-level risk.

The system stores these and displays, to a user, a user interface that includes a
notification according to the identified cyber-security risks and the corresponding
assigned risk classifications (330). The notification can include, either by default or in
response to an input from a user, details of each of the identified cyber-security risks.
The notification can include graphical symbols or colors to identify the assigned risk
classifications. The notification can include a total number of identified cyber-security
risks assigned to each classification. The system can prompt a user for an action in
response to displaying the notification. The system can therefore generate a first type of
notification when a risk level or value associated with a specified cyber-security risk
exceeds the first threshold but not the second threshold, and can generate a second type
of notification when the risk level or value associated with the specified cyber-security
risk exceeds both the first and second threshold values, where the second type of
notification has a higher priority than the first type of notification.

Note that the risk manager 154 and/or the graphical user interface 200 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. 62/13,221 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. 62/114,865 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; and

- U.S. Provisional Patent Application No. 62/116,245 entitled "RISK MANAGEMENT IN AN AIR-GAPPED ENVIRONMENT” and corresponding non-

[0050] 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.

[0051] 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.

[0052] 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:
   identifying (305), by a risk manager system (154), a plurality of connected devices (106, 114, 122, 130, 138) that are vulnerable to cyber-security risks;
   identifying (310), by the risk manager system (154), cyber-security risks in the connected devices (106, 114, 122, 130, 138);
   assigning (314), by the risk manager system (154), a risk level to each of the identified cyber-security risks;
   for each identified cyber-security risk, comparing (320) by the risk manager system (154) the assigned risk level to a first threshold (202) and to a second threshold (204);
   based on the comparisons, assigning (325), by the risk manager system (154), each identified cyber-security risk to a risk classification; (222, 224, 226); and
   displaying (330), by the risk manager system (154), a user interface that includes a notification (220) according to the identified cyber-security risks and the corresponding assigned risk classifications (222, 224, 226).

2. The method of claim 1, wherein the first threshold (202) is a risk appetite and the second threshold (204) is a risk tolerance.

3. The method of claim 1, wherein the risk manager system (154) also receives the first and second threshold (202, 204) from a user.

4. The method of claim 1, wherein the risk manager system (154) assigns identified cyber-security risks with an assigned risk level that is less than both the first threshold (202) and the second threshold (204) to a low-priority classification or a notification classification (222).

5. The method of claim 1, wherein the risk manager system (154) assigns identified cyber-security risks with an assigned risk level that is greater than or equal to the first threshold (202) but is less than the second threshold (204) to a warning classification (224).
6. The method of claim 1, wherein the risk manager system (154) assigns identified cyber-security risks with an assigned risk level that is greater than or equal to both the first threshold (202) and the second threshold (204) to an alert classification (226).

7. The method of claim 1, wherein the risk manager system (154) prompts a user for an action in response to displaying the notification (220).

8. A risk manager system (154) comprising:
   a controller (156); and
   a display, the risk manager system (154) configured to
   identify (305) a plurality of connected devices (106, 114, 122, 130, 138) that are vulnerable to cyber-security risks;
   identify (310) cyber-security risks in the connected devices (106, 114, 122, 130, 138);
   assign (314) a risk level to each of the identified cyber-security risks;
   for each identified cyber-security risk, compare (320) the assigned risk level to a first threshold (202) and to a second threshold (204);
   based on the comparisons, assign (325) each identified cyber-security risk to a risk classification; (222, 224, 226); and
   display (330) a user interface that includes a notification (220) according to the identified cyber-security risks and the corresponding assigned risk classifications (222, 224, 226).

9. The risk manager system of claim 8, wherein the first threshold (202) is a risk appetite and the second threshold (204) is a risk tolerance.

10. The risk manager system of claim 8, wherein the risk manager system (154) also receives the first and second threshold (202, 204) from a user.

11. The risk manager system of claim 8, wherein the risk manager system (154) assigns identified cyber-security risks with an assigned risk level that is less than both the first threshold (202) and the second threshold (204) to a low-priority
classification or a notification classification (222).

12. The risk manager system of claim 8, wherein the risk manager system (154) assigns identified cyber-security risks with an assigned risk level that is greater than or equal to the first threshold (202) but is less than the second threshold (204) to a warning classification (224).

13. The risk manager system of claim 8, wherein the risk manager system (154) assigns identified cyber-security risks with an assigned risk level that is greater than or equal to both the first threshold (202) and the second threshold (204) to an alert classification (226).

14. The risk manager system of claim 8, wherein the risk manager system (154) prompts a user for an action in response to displaying the notification (220).

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:

   identify (305) a plurality of connected devices (106, 114, 122, 130, 138) that are vulnerable to cyber-security risks;

   identify (310) cyber-security risks in the connected devices (106, 114, 122, 130, 138);

   assign (314) a risk level to each of the identified cyber-security risks, for each identified cyber-security risk, compare (320) the assigned risk level to a first threshold (202) and to a second threshold (204); based on the comparisons, assign (325) each identified cyber-security risk to a risk classification; (222, 224, 226); and

   display (330) a user interface that includes a notification (220) according to the identified cyber-security risks and the corresponding assigned risk classifications (222, 224, 226).
300

305 IDENTIFY CONNECTED DEVICES

310 IDENTIFY CYBER-SECURITY RISKS

315 ASSIGN RISK LEVEL TO EACH IDENTIFIED RISK

320 COMPARE RISK LEVELS TO THRESHOLDS

325 ASSIGN RISKS TO RISK CLASSIFICATIONS

330 DISPLAY USER INTERFACE ACCORDING TO RISKS AND ASSIGNED RISK CLASSIFICATIONS

FIG. 3
A. CLASSIFICATION OF SUBJECT MATTER

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

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 29/06; G06N 5/04; G06F 21/57; G06F 12/14; G06F 21/50; G06F 21/60; G06F 11/00; G06F 21/00; H04L 12/24

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: network, security, risk, notification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>WO 2013-166126 A1 (TAASERA, INC.) 07 November 2013</td>
<td>1-15</td>
</tr>
<tr>
<td></td>
<td>See paragraphs [0084], [0087], [0114], [0175], [0193]; claims 1-19; and figure 4.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See paragraphs [0052]-[0055]; and figures 9, 10.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See paragraphs [0088]-[0097]; claims 1-7; and figures 6-88.</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>US 2014-0130121 A1 (YEE.JANG JAMES LIN) 08 May 2014</td>
<td>1-15</td>
</tr>
<tr>
<td></td>
<td>See abstract; paragraphs [0024]-[0027], [0029]-[0037]; and figures 2, 4-6.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See abstract; claims 1-8; and figures 5-7.</td>
<td></td>
</tr>
</tbody>
</table>

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

03 June 2016 (03.06.2016)

Date of mailing of the international search report

03 June 2016 (03.06.2016)

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. +82-42-481-8571

Authorized officer

KIFM, KI HO

Telephone No. +82-42-481-8691

Form PCT/ISA/210 (second sheet) (January 2015)
## INTERNATIONAL SEARCH REPORT
### Information on patent family members

<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Kr 10-2015-0006042 A</td>
<td>15/01/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 2013-0298192 Al</td>
<td>07/11/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 2013-0298230 Al</td>
<td>07/11/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 2013-0298242 Al</td>
<td>07/11/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 2013-0298243 Al</td>
<td>07/11/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 2013-0298244 Al</td>
<td>07/11/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 2015-0244735 Al</td>
<td>27/08/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 8776180 B2</td>
<td>08/07/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 8850588 B2</td>
<td>30/09/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 8990948 B2</td>
<td>24/03/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 9027125 B2</td>
<td>05/05/2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 9092616 B2</td>
<td>28/07/2015</td>
</tr>
<tr>
<td>us 2010--0125912 Al</td>
<td>20/05/2010</td>
<td>us 8402546 B2</td>
<td>19/03/2013</td>
</tr>
<tr>
<td>us 2014--0082738 Al</td>
<td>20/03/2014</td>
<td>us 2008-0189788 Al</td>
<td>07/08/2008</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 2011-0131658 Al</td>
<td>02/06/2011</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 7908660 B2</td>
<td>15/03/2011</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 8595844 B2</td>
<td>26/11/2013</td>
</tr>
<tr>
<td>us 2014--0130121 Al</td>
<td>08/05/2014</td>
<td>us 2010-0121929 Al</td>
<td>13/05/2010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 8631081 B2</td>
<td>14/01/2014</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us 9189634 B2</td>
<td>17/11/2015</td>
</tr>
<tr>
<td>us 2013--0160119 Al</td>
<td>20/06/2013</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

Form PCT/ISA/2 10 (patent family annex) (January 2015)