US009270642B2

(12) **United States Patent**
Rotvold et al.

(10) **Patent No.: US 9,270,642 B2**
(45) **Date of Patent: Feb. 23, 2016**

(54) **PROCESS INSTALLATION NETWORK INTRUSION DETECTION AND PREVENTION**

(75) Inventors: **Eric D. Rotvold**, West Saint Paul, MN (US); **Jeff D. Potter**, Shorewood, MN (US)

(73) Assignee: **Rosemount Inc.**, Eden Prairie, MN (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 190 days.

(21) Appl. No.: **13/272,394**

(22) Filed: **Oct. 13, 2011**

(65) **Prior Publication Data**

US 2013/0094500 A1 Apr. 18, 2013

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04W 12/12	(2009.01)
H04L 29/08	(2006.01)
H04W 84/18	(2009.01)

(52) **U.S. Cl.**
CPC ***H04L 63/0245*** (2013.01); ***H04L 67/12*** (2013.01); ***H04W 12/12*** (2013.01); *H04L 63/0281* (2013.01); *H04L 63/1416* (2013.01); *H04L 67/303* (2013.01); *H04W 84/18* (2013.01)

(58) **Field of Classification Search**
CPC H04W 12/00; H04W 84/18; H04L 67/303; H04L 63/0281
USPC 370/389
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,850,973	B1 *	2/2005	Larson	G05B 19/0426 700/117
6,889,166	B2	5/2005	Zielinski et al.	702/183
7,761,923	B2	7/2010	Khuti et al.	726/27
2001/0017860	A1 *	8/2001	Hata	370/395
2003/0212900	A1 *	11/2003	Liu et al.	713/200
2004/0193943	A1	9/2004	Angelino et al.	
2005/0005093	A1	1/2005	Bartels et al.	713/150
2005/0283823	A1 *	12/2005	Okajo	G06F 21/604 726/1
2006/0080527	A1 *	4/2006	Novack	H04L 9/3263 713/156

(Continued)

FOREIGN PATENT DOCUMENTS

CN	1870518	11/2006
EP	2068215 A2	6/2009

(Continued)

OTHER PUBLICATIONS

Chinese 3rd Official Action dated Jun. 9, 2013 for related application 201220319024.X, 3 pgs. With English Translation.

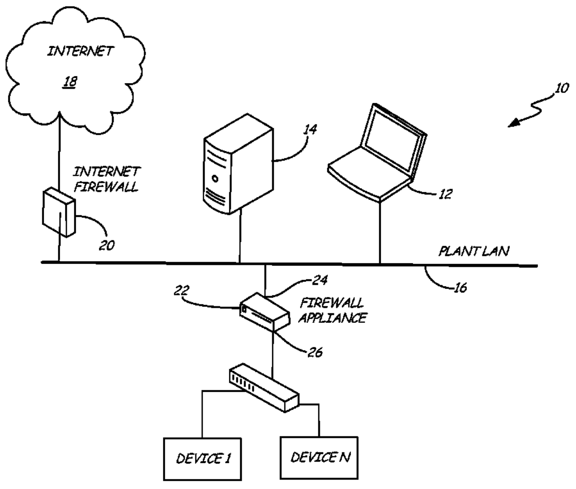
(Continued)

Primary Examiner — Shripal Khajuria
Assistant Examiner — Faisal Choudhury
(74) *Attorney, Agent, or Firm* — Westman, Champlin & Koehler, P.A.

(57) **ABSTRACT**

A process communication device includes a process communication interface for communicating on a process communication loop in accordance with a process communication protocol. A controller is coupled to the process communication interface. A rules store is coupled to the controller, and has at least one process communication packet rule that is based on the process communication protocol. The controller applies the at least one process communication packet rule to at least one process communication packet received from the process communication interface, and generates event information when a process communication packet fails at least one process communication packet rule.

16 Claims, 6 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2007/0199049	A1 *	8/2007	Ziebell	726/3
2007/0199061	A1 *	8/2007	Byres	H04L 41/0806 726/11
2008/0126665	A1 *	5/2008	Burr	G05B 19/042 710/316
2009/0059814	A1 *	3/2009	Nixon et al.	370/254
2010/0257598	A1 *	10/2010	Demopoulos et al.	726/13
2011/0072506	A1 *	3/2011	Law	H04L 63/0227 726/11
2011/0149849	A1 *	6/2011	Brownrig	370/328
2012/0065748	A1 *	3/2012	Nixon et al.	700/73
2012/0079126	A1 *	3/2012	Evans et al.	709/230
2012/0093242	A1 *	4/2012	Wallace et al.	375/259

FOREIGN PATENT DOCUMENTS

JP	2009-070383	4/2009
JP	2011-100443	5/2011

OTHER PUBLICATIONS

Technical Information. HART Communication: Part 4 Communications by Samson.

Technical Datasheet. Tofino™ 9211-ET-HN3: Honeywell Modbus Read-Only Firewall. www.mtl-inst.com.

The Tofino Solution Protects the Network. Oct. 2007. www.controlglobal.com.

Product Data Sheet. 1420 Wireless Gateway. Mar. 2008 by Emerson Process Managment.

Second Office Action from corresponding Chinese patent application No. 201220319024.X dated Mar. 7, 2013.

International Search Report and Written Opinion for the corresponding International patent application No. PCT/US2012/040413 dated Sep. 10, 2012. 13 pages.

Aguinaldo B Batista et al.: "Application Filters for TCP/IP Industrial Automation Protocols". 13 pages.

Rejection Decision dated Aug. 28, 2013 in related Chinese application No. 201220319024.X, with English Translation. 6 pgs.

Office Action from Japanese Application No. 2014-535712, dated Jan. 27, 2015.

Communication pursuant to Rules 161(1) and 162 EPC for European Patent Application No. 12727506.3-1853 dated May 22, 2014, 2 pages.

Office Action from Chinese Patent Application No. 201210227870.3, dated Feb. 10, 2015.

Office Action from Japanese Patent Application No. 2014-535712, dated Sep. 8, 2015.

Office Action from Canadian Patent Application No. 2,851,484, dated Oct. 16, 2015.

Office Action from Russian Patent Application No. 2014118936, dated Sep. 11, 2015.

Office Action from Chinese Patent Application No. 201210227870.3, dated Oct. 26, 2015.

* cited by examiner

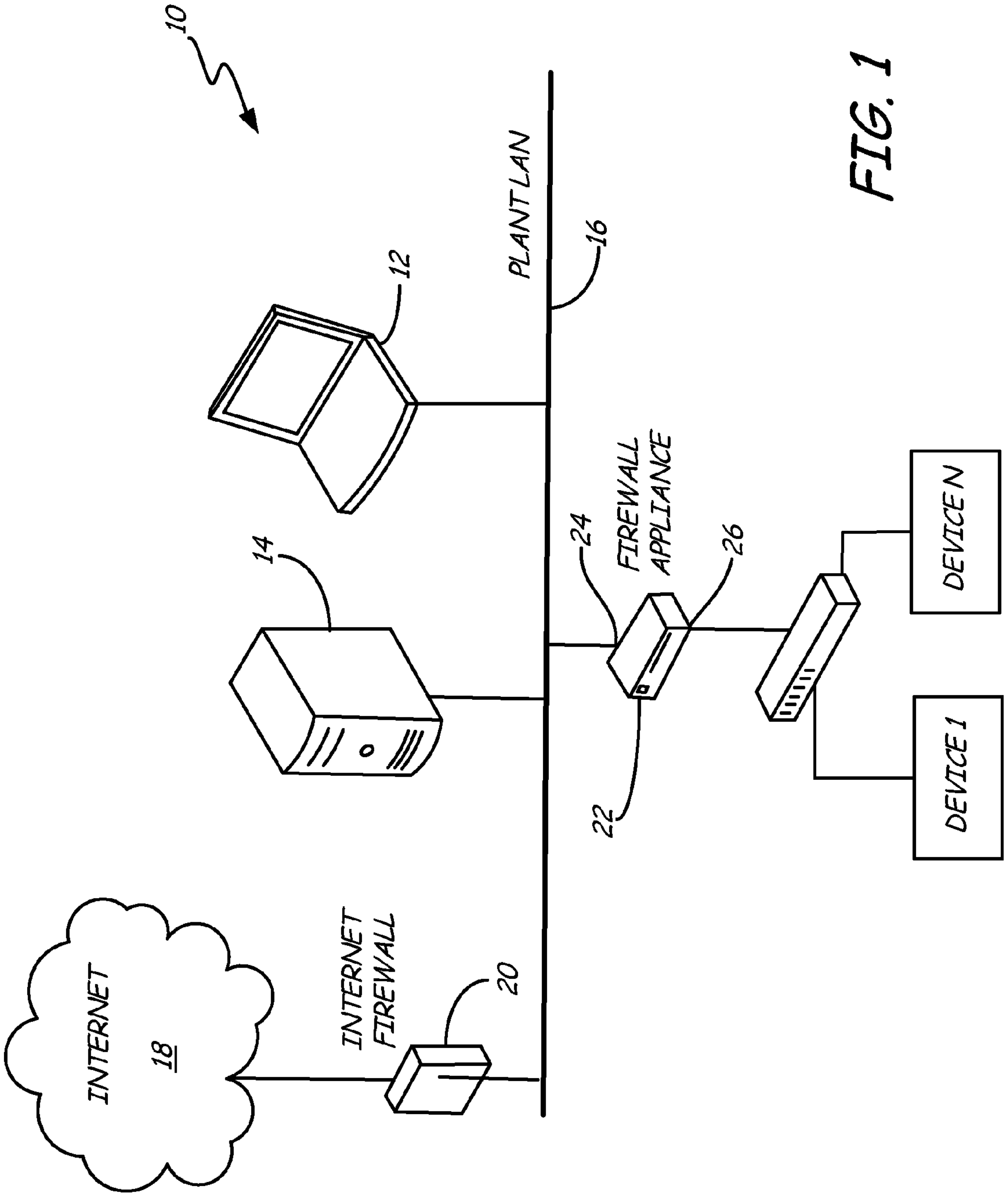

10
INTERNET
18
INTERNET FIREWALL
20
14
12
PLANT LAN
16
FIREWALL APPLIANCE
24
26
22
DEVICE 1
DEVICE N

FIG. 1

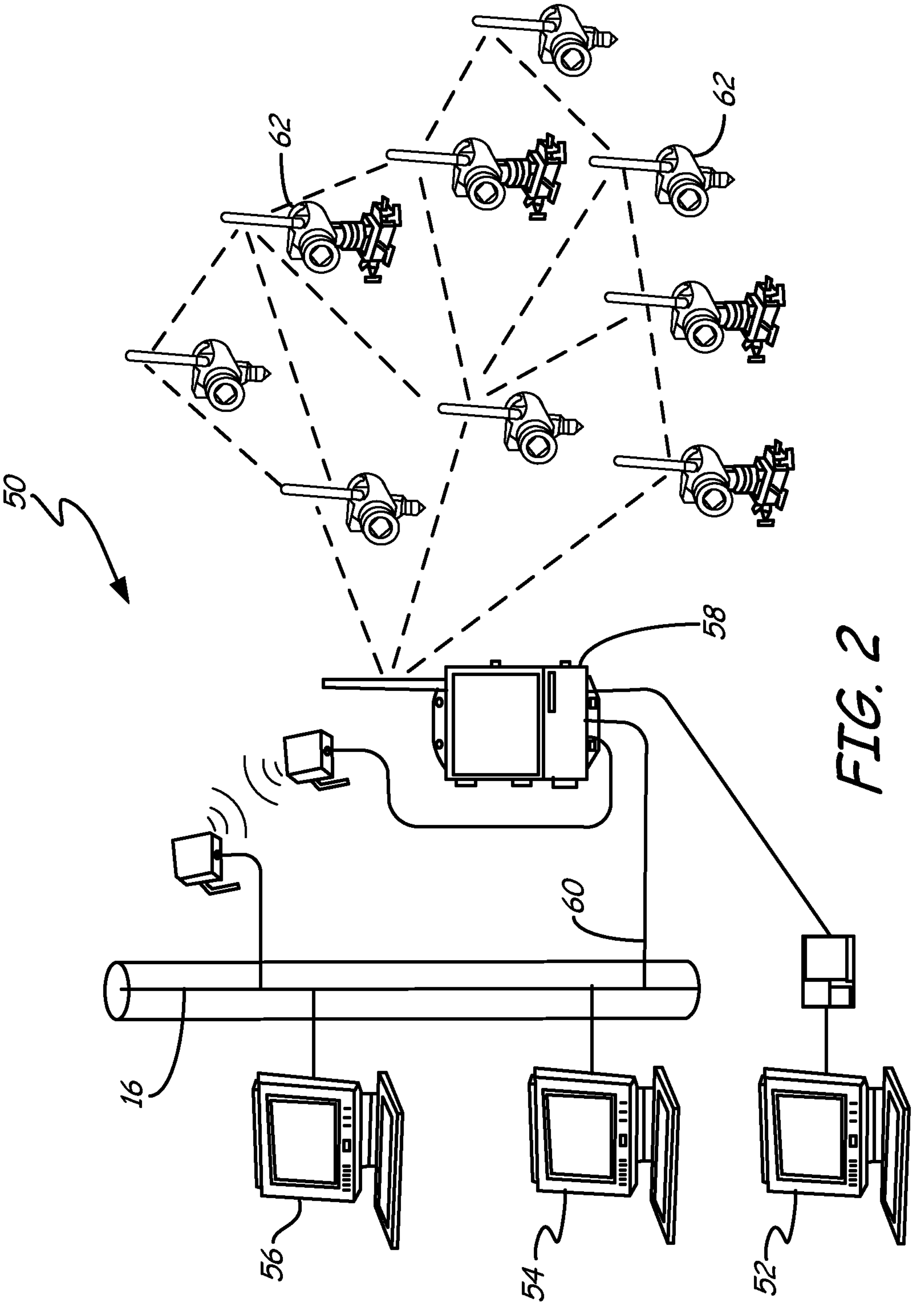


FIG. 2

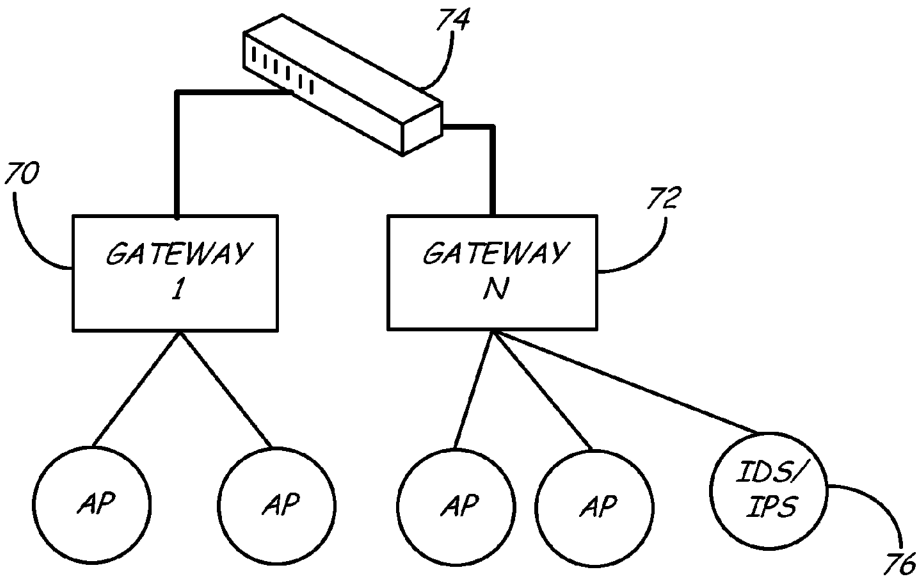


FIG. 3

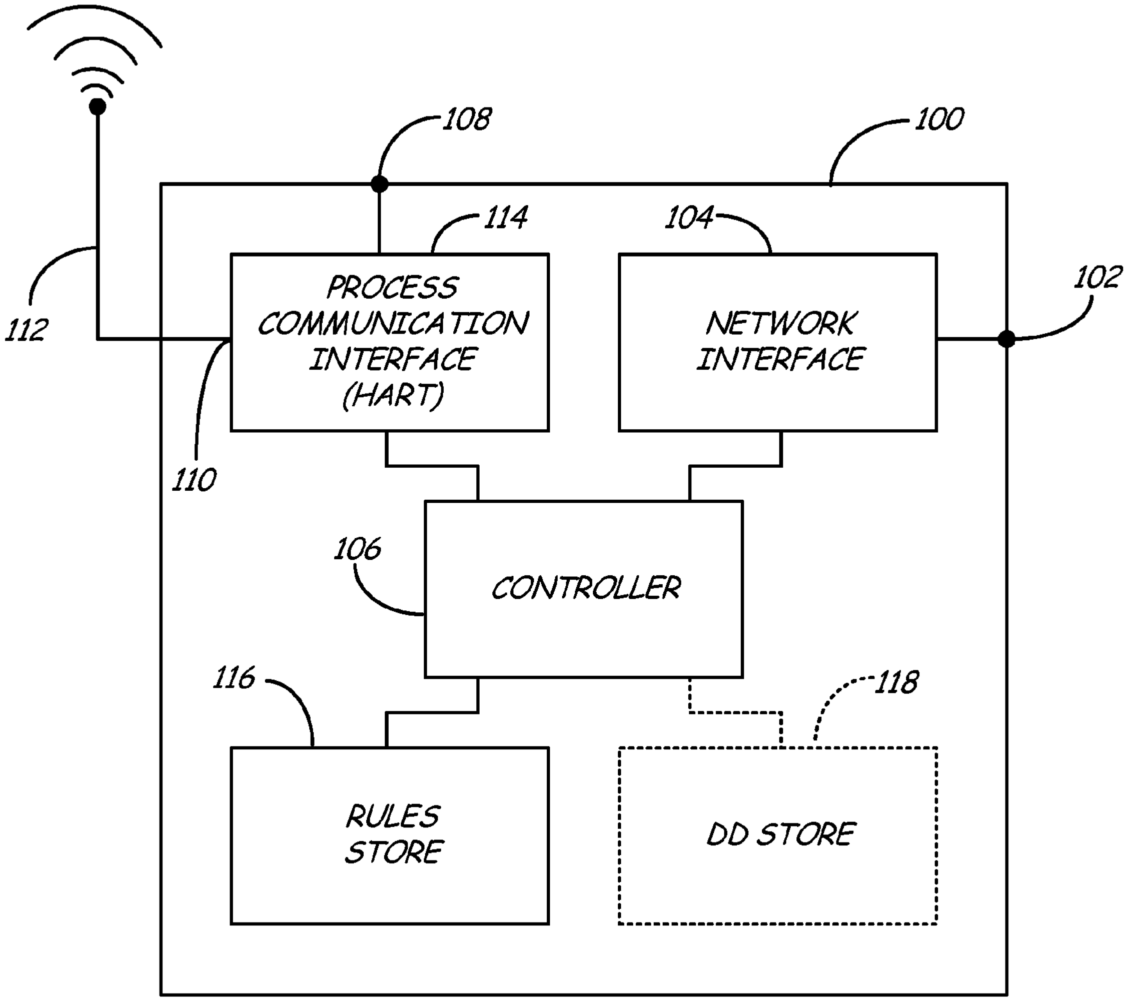

108
100
114
104
102
112
PROCESS COMMUNICATION INTERFACE (HART)
NETWORK INTERFACE
110
106
CONTROLLER
116
118
RULES STORE
DD STORE

FIG. 4

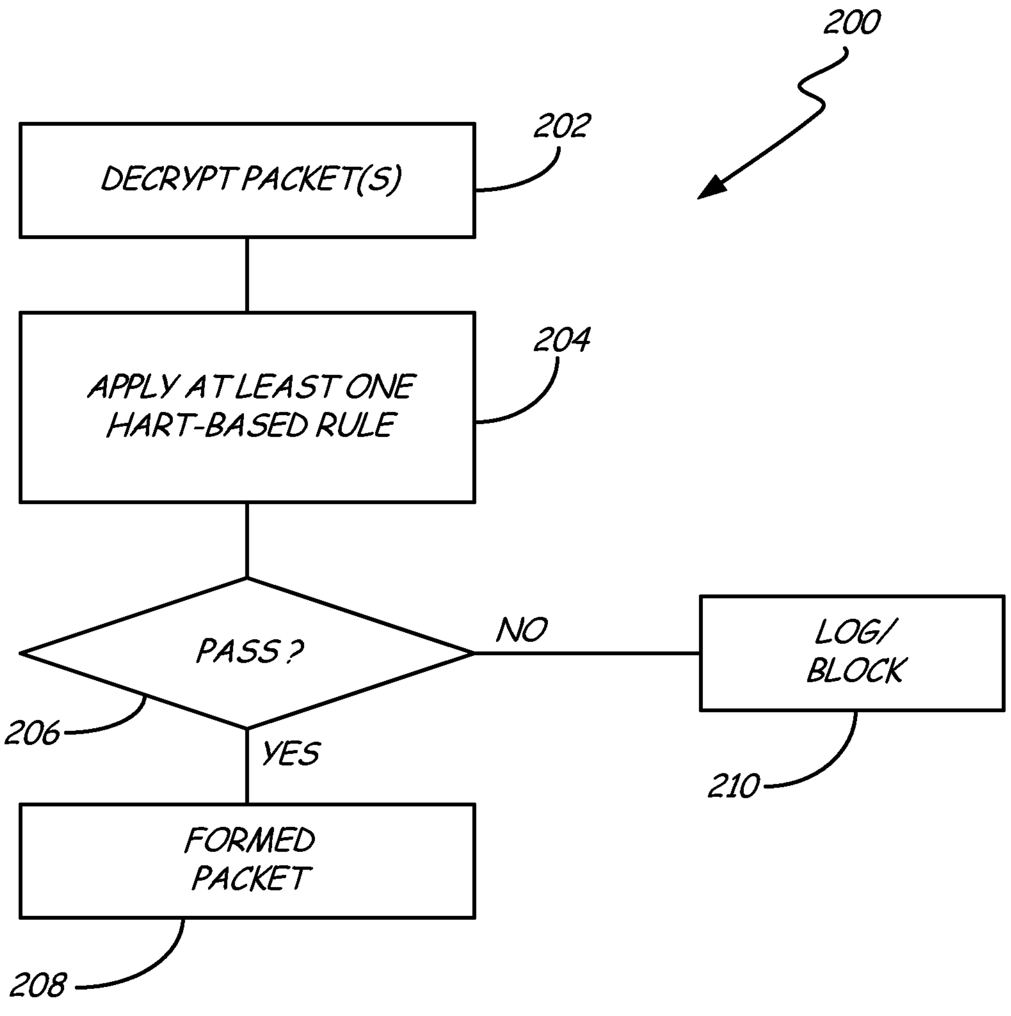

200
DECRYPT PACKET(S)
202
APPLY AT LEAST ONE HART-BASED RULE
204
PASS ?
NO
LOG/ BLOCK
206
YES
210
FORMED PACKET
208

FIG. 5

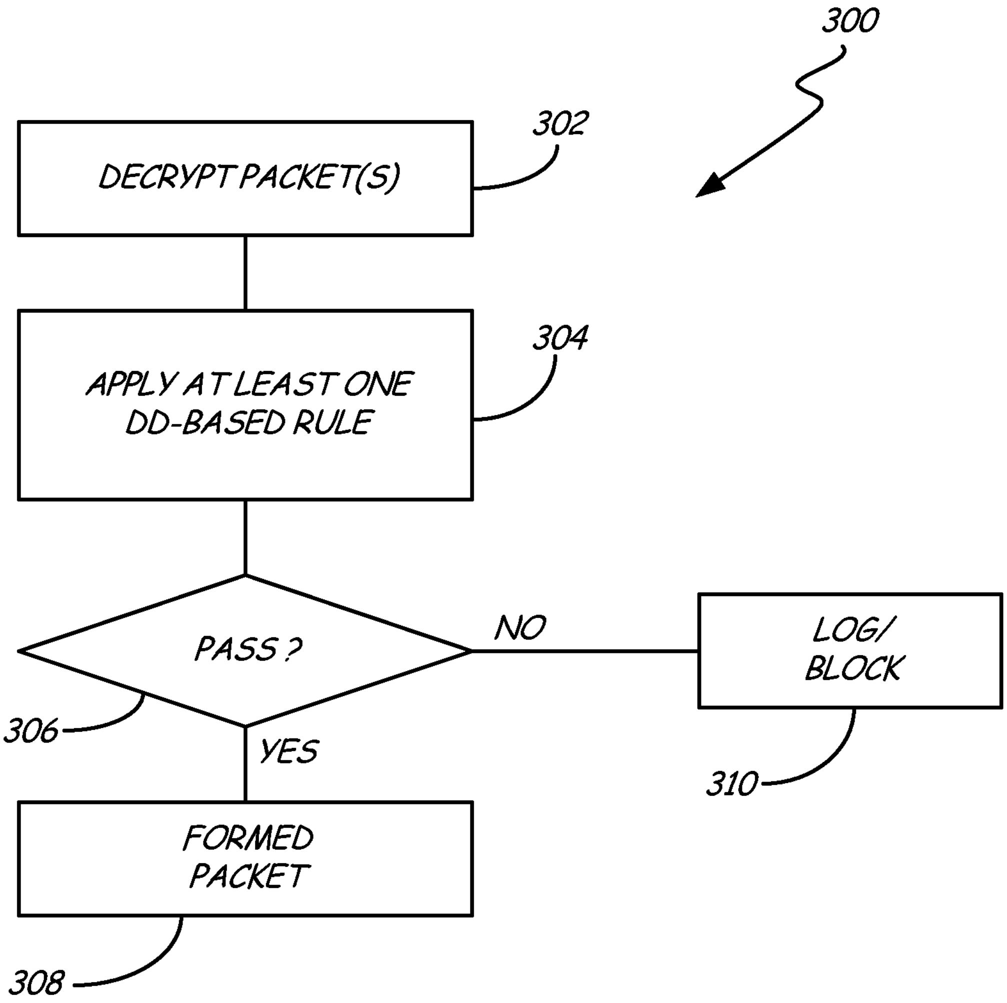

300
DECRYPT PACKET(S)
302
APPLY AT LEAST ONE DD-BASED RULE
304
PASS ?
306
NO
LOG/ BLOCK
310
YES
FORMED PACKET
308

FIG. 6

PROCESS INSTALLATION NETWORK INTRUSION DETECTION AND PREVENTION

BACKGROUND

Modern process installations are used to provide and/or produce a variety of products and materials used every day. Examples of such process installations include petroleum refining installations, pharmaceutical production installations, chemical processing installations, pulp and other processing installations. In such installations, a process control and measurement network may include thousands or even of tens of thousands of various field devices communicating with a control room, and sometimes with one another, to control the process. Given that malfunctions in a given field device could cause the process to go out of control, the physical characteristics, and electrical communication of field devices is generally subject to stringent specifications.

Traditionally, field devices in a given process installation have generally been able to communicate over a process control loop or segment with a control room and/or other field devices via wired connections. An example of a wired process communication protocol is known as the Highway Addressable Remote Transducer (HART®) protocol. HART® communication is one of the primary communication protocols used in the process industries. Recently, it has become possible, and potentially desirable in some cases, to permit process installations access to the Internet. While such a feature provides the ability to interact with the process installation from virtually any connected computer around the globe, it also provides the potential for a malicious entity, such as a hacker, to attempt to influence the process installation without travelling to the physical location of the process installation.

Another recent development with respect to process installations is utilization of wireless communication. Such wireless communication simplifies process installations in that it is no longer required to provide long runs of wires to the various field devices. Moreover, one such wireless protocol, WirelessHART (IEC 62591), expands upon the traditional HART® protocol and provides vastly increased data transfer rates. For example, WirelessHART supports communication up to 250 Kbps. Relevant portions of the Wireless HART® Specification include: HCF_Spec 13, revision 7.0; HART Specification 65—Wireless Physical Layer Specification; HART Specification 75—TDMA Data Link Layer Specification (TDMA refers to Time Division Multiple Access); HART Specification 85—Network Management Specification; HART Specification 155—Wireless Command Specification; and HART Specification 290—Wireless Devices Specification. While wireless communication provides a number of advantages for process installations, it also allows for devices in the physical proximity of the process installation to potentially engage and affect the wireless communication network.

Given the recent connectivity of process installations, it is now vitally important that process communication be protected from intrusion and activities of malicious entities. This applies for process installations that may be connected to the Internet, process installations that employ wireless process communication, or both. Accordingly, providing a process installation with the ability to detect and prevent intrusion upon a process communication loop would further help secure the various process installations that rely upon process communication.

SUMMARY

A process communication device includes a process communication interface for communicating on a process communication loop in accordance with a process communication protocol. A controller is coupled to the process communication interface. A rules store is coupled to the controller, and has at least one process communication packet rule that is based on the process communication protocol. The controller applies the at least one process communication packet rule to at least one process communication packet received from the process communication interface, and generates event information when a process communication packet fails at least one process communication packet rule.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a diagrammatic view of a process communication system in accordance with an embodiment of the present invention.

FIG. **2** is a diagrammatic view of a process communication and control system within which embodiments of the present invention are particularly applicable.

FIG. **3** is a diagrammatic view of another process communication and control environment with which embodiments of the present invention are particularly useful.

FIG. **4** is a diagrammatic view of a process communication security appliance in accordance with an embodiment of the present invention.

FIG. **5** is a flow diagram of a method of providing intrusion detection and prevention in a process installation in accordance with an embodiment of the present invention.

FIG. **6** is a flow diagram of a method of providing intrusion detection and prevention in a process installation in accordance with another embodiment of the present invention.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

Embodiments of the present invention generally leverage specific knowledge of the HART® protocol (both wired and wireless) and/or HART® Device Descriptions (DD's) to monitor process communication network traffic coming into the process communication loop, leaving the process communication loop, or even transiting the process communication loop for anomalies. While embodiments of the present invention are generally described with respect to HART® process communication loops, embodiments of the present invention can be practiced with any suitable process communication protocols that support device descriptions.

The HART® protocol has a hybrid physical layer consisting of digital communication signals superimposed on a standard 4-20 mA analog signal. The data transmission rate is approximately 1.2 Kbps/sec. HART® communication is one of the primary communication protocols in process industries. Both wireless and wired HART® communications share a substantially similar application layer. Moreover, the command content of both wireless and wired HART® communications is identical. Accordingly, while the physical layers may vary, at the application layer, these two process communication protocols are very similar.

Process communication network security on and over HART® networks is important, and becoming more so as HART® network traffic can now be transported over TCP/IP networks as well as wireless networks. Some network security has been provided by devices such as those sold under the trade designation Model 1420 Wireless Gateway from Emerson Process Management, of Chanhassen, Minn. This device provides the ability to authenticate sender and receiver, verify that the data is valid, encrypt process communication data, and manage periodic changes to encryption keys automatically. While the process communication security provided by the Model 1420 is invaluable to modern process communication networks, embodiments of the present invention generally build upon the security provided by the 1420 Wireless Gateway by leveraging additional knowledge about the HART® protocol itself, HART® device descriptions (DD's) or a combination thereof. While embodiments of the present invention are applicable to any device that has access to the process communication, it is preferred that embodiments of the present invention be embodied in either a firewall appliance, a gateway, such as an improved wireless gateway, or an access point type of device.

FIG. **1** is a diagrammatic view of a process communication system **10** in accordance with an embodiment of the present invention. System **10** includes a workstation **12** and server **14** communicatively coupled to one another over plant local area network **16**. Network **16** is coupled to Internet **18** via local area network firewall **20**. Local area network firewall **20** is a well-known device providing only selected TCP/IP traffic therethrough. In the embodiment illustrated in FIG. **1**, a process communication security appliance **22** is coupled to plant LAN **16** by virtue of connection **24**, and is further coupled to devices **1**-*n* via port **26**. Process communication security appliance **22** protects the process communication segments/loops from malicious activity originating over Internet **18** and/or Plant LAN **16**. A processor within process communication security appliance **22** executes software instructions that are able to receive one or more process communication packets and test whether the packet(s) satisfies one or more rules that are based specifically upon HART® process communication rules, device description requirements, or a combination thereof.

FIG. **2** is a diagrammatic view of a process communication and control system **50** within which embodiments of the present invention are particularly applicable. A number of workstations **52**, **54**, and **56** are coupled together via plant LAN **16**. Additionally, a wireless process communication gateway **58** is also coupled to LAN **16** via connection **60**. The arrangement shown in FIG. **2** is the current environment within which the Model 1420 Smart Wireless Gateway operates. Gateway **58** communicates with one or more field devices **62** via WirelessHART® communication. Accordingly, embodiments of the present invention may be practiced using the processor, or other suitable controller, disposed within gateway **58**.

FIG. **3** is a diagrammatic view of another process communication and control environment with which embodiments of the present invention are particularly useful. Specifically, one or more gateways (**1**-*n*) **70**, **72** are communicatively coupled via device **74**. Each gateway can communicate with one or more access points. In accordance with an embodiment of the present invention, one of the access points **76** is configured, through hardware, software, or a combination thereof, to receive process communication packets and inspect the process communication packets to determine if the communication complies with one or more rules that are based on the HART® protocol, Device Descriptions, or a combination thereof. Access point **76** listens to data in the wireless network and inspects packets as they arrive. As a result of inspections, certain aspects of communication traffic can be tracked (source address, arrival rate, known device, new device, join requests, et cetera) and statistics and/or alerts can be provided to the gateway upon detection of events. Embodiments of the present invention also include the utilization of a plurality of gateways and respective access points to provide a redundant pair.

FIG. **4** is a diagrammatic view of a process communication security appliance in accordance with an embodiment of the present invention. Security appliance **100** includes a network interface **102** coupleable to a data communication network, such as an Ethernet-based data communication network. Port **102** is coupled to network interface physical layer **104** to generate and receive data communication packets in accordance with known techniques. Network interface physical layer **104** is coupled to controller **106** which is preferably a microprocessor that includes, or is coupled to, suitable memory, such as random access memory, read-only memory, flash memory, et cetera, to store and execute program instructions. Security appliance **100** also preferably includes a wired process communication port **108** and/or a wireless process communication port **110** coupled to antenna **112**. In embodiments where security appliance **100** is embodied within a wireless access point, no wired process communication port is required. Each of ports **108**, **110** may be coupled to a HART® process communication interface **114**. Interface **114** enables controller **106** to communicate with external devices, such as field devices, using the known HART® protocol. In some embodiments, HART® communication may be provided over an IP network, thus network interface physical layer **104** may also be a source of HART® packets.

In accordance with an embodiment of the present invention, security appliance **100** includes rules store **116**. Optionally, security appliance **100** may include device description store **118**. Rules store **116** includes non-volatile memory that stores one or more rules that may be enforced upon HART® process communication based upon an underlying understanding of the HART® protocol. Rules store **116** enables controller **106** to determine if the construction and/or content of packets in the HART® network are valid. Further, the validity of the source and destination of the packets can be determined. Finally, the content of the packet itself can be analyzed to determine if it is proper. For example, a malformed packet may have a bad cyclic redundancy check, byte count, pay load size, et cetera. If the packet is invalid, security appliance **100** would not forward the packet to the requested destination. Additionally, and/or alternatively, security appliance **100** can store event data related to the detection of the malformed packet, and/or send an appropriate communication to a responsible party. Moreover, controller **106** may track and/or analyze the event data such that if a number of malformed packets are detected from a single source within a specific period of time, controller **106** may determine that an attack is currently active. If so, controller **106** may notify the user and/or a responsible party that the attack may be occurring, along with details of the suspected source of the attack. Further still, controller **106** can act to reject all packets from that source until the user intervenes.

As illustrated in FIG. **4**, security appliance **100** may also include a device description store **118**. With the current state of the art of memory technology, it is economically feasible for store **118** to be large enough to contain device descriptions of all known field devices that communicate in accordance with the HART® protocol as of the date of manufacture for security appliance **100**. Moreover, as new HART®-communicating devices are produced, device description store **118** may be updated dynamically by virtue of data network communication port **102**. Maintaining a comprehensive device description store **118** allows for additional checks and/or tests to be performed upon the process communication packets. For example, if a given process communication packet is from a field device that, according to its device description, is only known to provide a temperature measurement, a packet indicative of a process pressure from such field device would be deemed malicious even if the packet otherwise complied with all rules set forth in rules store **116**.

There are a number of different types of commands that are used in the HART® protocol. These types of commands include universal commands, common practice commands, wireless commands, device family commands, and device-specific commands. With the exception of the device-specific commands, at least some knowledge of commands in each type can be known based upon the HART® specification itself. Moreover, even device-specific commands can be scrutinized if the process communication security appliance contains a device description relative to a particular specific field device.

One example of a rule stored in rules store **116** that can be enforced at the application-layer of a HART® protocol packet is as follows. Since, for a given HART® revision, the byte count relative to each and every command is known, if a packet is indicative of a command, the known byte count can be enforced for the packet. Even for device-specific commands, some rules can be provided. Specifically, the command range can be tested to determine if it is within an allowable range (such as 128-240 and 64768-65021). Further, the total byte count of the packet can be determined and compared with the contents of the byte count field to check for valid agreement.

One of the synergies of embodying the functionality of the process communication security appliance within a gateway, such as the Model 1420, is that the gateway is aware of all individual field devices on the network. Moreover, the gateway has the additional advantage in that it has access to all the information required (specifically decryption keys) to decrypt and inspect all HART® packets. Additionally, the security appliance, preferably embodied within a gateway, can build a database or list of known destination/wireless devices and ensure that only messages for those devices are sent/forwarded. Further still, the security appliance can check and/or allow forwarding of packets only from known/configured sources. Finally, as set forth above, the packet construction itself can be inspected to determine if the header content is proper, if the byte count corresponds with the actual size of the packet, if the CRC checksum is valid, and if the destination address is valid. In addition to these security measures, the processor of the controller of the security appliance can react to dynamic communication changes. Specifically, known neural network and/or artificial intelligence algorithms can be employed to allow controller **106** to essentially learn normal process communication network traffic. Additionally, or alternatively, a set of statistics relative to the network communication and/or various destinations and sources can be maintained. If changes are detected relative to the learned normal communication and/or statistically stored parameters, an alert can be transmitted to a responsible party by virtue of either data communication network port **102** or a process communication port **108**, **110**. Additionally, suspicious patterns of communication can be specifically identified based upon rules. For example, if controller **106** observes a number of destination address requests, where the device ID is simply incremented or decremented with each request, the pattern would appear to be an application searching for a device. Such searching could be considered to be malicious. Further, device address requests that repeatedly increment or decrement an expanded device type may also signify an application searching for a hit. This would also be considered to be a malicious indicator. Further still, destination address requests that include simply incrementing or decrementing message fields, such as command, byte count, data fields, may indicate an application that is attempting to find an available device, and/or disrupt the process communication network. Detection of such a pattern could be considered a malicious indicator.

In the event that a malicious indicator is discovered, it is preferably logged locally in the security appliance. Additionally, the security appliance can include a simple network management protocol or syslog option to report the event and/or additional status information to a responsible party or information technology application. Syslog is a well known logging mechanism used by server type applications to log events/alerts to an external server or database for further analysis.

FIG. **5** is a flow diagram of a method of providing intrusion detection and prevention in a process installation in accordance with an embodiment of the present invention. Method **200** begins at block **202** where a security appliance or process communication gateway receives at least one process communication packet and decrypts the packet. At block **204**, method **200** applies at least one rule against the decrypted packet, where the rule is based on a priori knowledge of the HART protocol. As set forth above, one exemplary rule is that for a given HART command, the byte count of the packet must match that set forth in the HART specification. At step **206**, method **200** determines whether the decrypted packet passed all of the rules applied in block **204**. If all rules were successfully passed, then control passes to block **208** where the packet is forwarded to its intended recipient. If however, the packet failed at least one rule, then control passes to block **210**, where the security event is preferably logged or en event generated, and the packet is blocked from further communication to the intended recipient.

FIG. **6** is a flow diagram of a method of providing intrusion detection and prevention in a process installation in accordance with an embodiment of the present invention. Method **300** begins at block **302** where a security appliance or process communication gateway receives at least one process communication packet and decrypts the packet, as required. At block **304**, method **300** applies at least one rule against the decrypted packet, where the rule is based on a process communication protocol (such as HART or FOUNDATION Fieldbus) device description (DD). As set forth above, one exemplary rule that is based on a device description would be a process variable temperature transmitter providing a process fluid pressure value. At step **306**, method **300** determines whether the decrypted packet passed all of the rules applied in block **304**. If all rules were successfully passed, then control passes to block **308** where the packet is forwarded to its intended recipient. If however, the packet failed at least one rule, then control passes to block **310**, where the security event is preferably logged, and the packet is blocked from further communication to the intended recipient.

Methods **200** and **300** are not mutually exclusive. Instead, the positive result of one method can be provided as the input to the other method to provide process installation intrusion detection and prevention based on both detailed knowledge of the process communication packets and device descriptions.

Although the present invention has been described with reference to preferred embodiments, workers skilled in the art will recognize that changes may be made in form and detail without departing from the spirit and scope of the invention.

What is claimed is:

1. A process communication device comprising:

a process communication interface configured to communicate with at least one field device on a process communication loop in accordance with a process communication protocol;

a controller coupled to the process communication interface;

a rules store coupled to the controller, the rules store having at least one process communication packet rule that is based on the process communication protocol

a device description store coupled to the controller, the device description store having at least one device description related to a process variable measured by the at least one field device and wherein the at least one field device is described by the at least one device description stored in the device description store; and

wherein the controller applies the at least one process communication packet rule and the at least one device description to at least one process communication packet received from the process communication interface, and generates event information when a process communication packet fails the at least one process communication packet rule or if the at least one communication packet is not in accordance with the at least one device description for the at least one field device; and

a network interface coupled to the controller, wherein the controller is configured to forward the process communication packet through the network interface if the process communication packet passes all process communication packet rules.

2. The process communication device of claim **1**, wherein the process communication protocol is the HART® (Highway Addressable Remote Transducer) protocol.

3. The process communication device of claim **1**, wherein the protocol imposes a digital signal on a 4-20 mA analog current signal.

4. The process communication device of claim **1**, wherein the process communication interface is a wired process communication interface.

5. The process communication device of claim **1**, wherein the process communication interface is a wireless process communication interface.

6. The process communication device of claim **5**, wherein the process communication interface is also a wired process communication interface.

7. The process communication device of claim **1**, wherein the controller is configured to decrypt the at least one process communication packet before applying the at least one process communication packet rule.

8. The process communication device of claim **7**, wherein the process communication device is embodied within a process communication gateway.

9. The process communication device of claim **1**, wherein at least one process communication packet rule relates an allowable number of packet bytes to a process communication protocol command contained in the packet.

10. The process communication device of claim **1**, wherein the at least one process communication packet rule includes an allowable command range.

11. The process communication device of claim **1**, wherein the process communication device is embodied within an access point.

12. A method of providing process communication protection, the method comprising;

obtaining at least one process communication packet sent from a field device in accordance with a process communication protocol;

applying at least one rule against the process communication packet, wherein the at least one rule is based on the process communication protocol;

applying at least a second rule against the process communication packet, wherein the at least a second rule is based upon a device description for the field device related to a process variable measured by the at least one field device; and

determining an event based on whether the at least one process communication packet passed each of the at least one rule and at least a second rule; and

selectively forwarding the at least one process communication packet based on whether the at least one process communication packet passed each of the at least one rule.

13. The method of claim **12**, and further comprising logging the event.

14. A process communication device comprising:

a process communication interface configured to communicate with at least one process device on a process communication loop in accordance with a process communication protocol;

a controller coupled to the process communication interface;

a device description store coupled to the controller, the device description store having at least one process communication packet rule that is based on a device description related to a process variable measured by the at least one field device for the at least one process device; and

wherein the controller applies the at least one process communication packet rule to at least one process communication packet received from the process communication interface, and generates event information when a process communication packet fails at least one process communication packet rule; and

a network interface coupled to the controller, wherein the controller is configured to forward the process communication packet through the network interface if the process communication packet passes all process communication packet rules.

15. A method of providing process communication protection, the method comprising;

obtaining at least one process communication packet in accordance with a process communication protocol, wherein the at least one process communication packet carries communication to or from at least one field device;

retrieving a device description from a device description store in a process communication security device which describes the at least one field device related to a process variable measured by the at least one field device;

applying at least one rule against the process communication packet, wherein the at least one rule is based the retrieved device description;

determining an event based on whether the at least one process communication packet passed each of the at least one rule; and

selectively forwarding the at least one process communication packet based on whether the at least one process communication packet passed each of the at least one rule.

16. The method of claim **15**, and further comprising logging the event.

* * * * *