

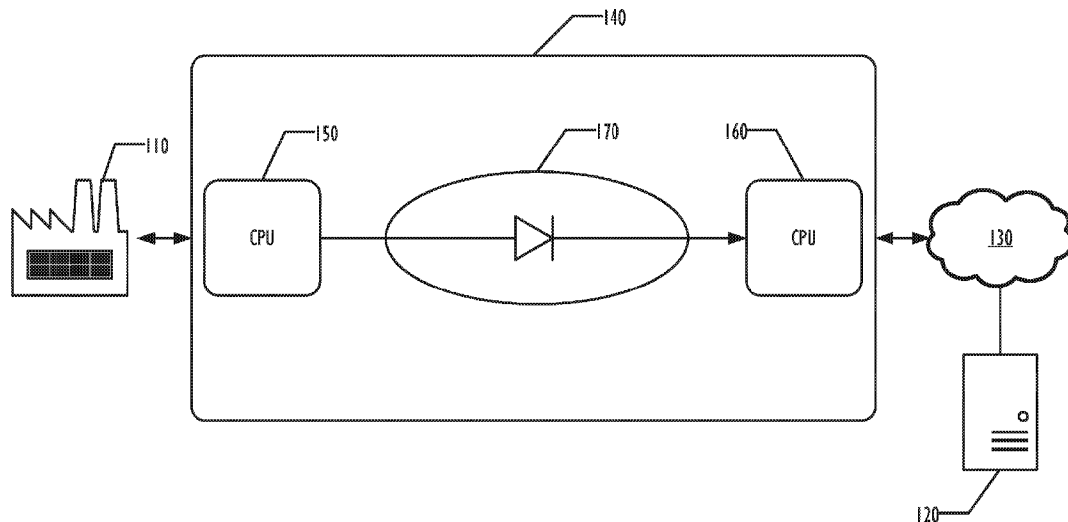


(86) Date de dépôt PCT/PCT Filing Date: 2018/12/18
(87) Date publication PCT/PCT Publication Date: 2019/06/27
(45) Date de délivrance/Issue Date: 2021/01/19
(85) Entrée phase nationale/National Entry: 2020/06/22
(86) N° demande PCT/PCT Application No.: US 2018/066328
(87) N° publication PCT/PCT Publication No.: 2019/126237
(30) Priorité/Priority: 2017/12/22 (US62/609,892)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01),
G06F 13/38 (2006.01), *H04L 12/66* (2006.01),
H04L 29/08 (2006.01)
(72) Inventeurs/Inventors:
DUNN, COLIN PATRICK, US;
LEE, SANG CHEON, US
(73) Propriétaire/Owner:
FEND INCORPORATED, US
(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : DISPOSITIF DE TRANSFERT DE DONNEES UNIDIRECTIONNEL AVEC DETECTION DE SYSTEME
EMBARQUE

(54) Title: ONE-WAY DATA TRANSFER DEVICE WITH ONBOARD SYSTEM DETECTION



(57) Abrégé/Abstract:

A data diode provides a flexible device for collecting data from a data source and transmitting the data to a data destination using one-way data transmission. On-board processing elements allow the data diode to identify automatically the type of connectivity provided to the data diode and configure the data diode to handle the identified type of connectivity.

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
27 June 2019 (27.06.2019)



(10) International Publication Number
WO 2019/126237 A1

(51) International Patent Classification:

H04L 29/06 (2006.01) *G06F 13/38* (2006.01)
H04L 29/08 (2006.01) *H04L 12/66* (2006.01)

(21) International Application Number:

PCT/US2018/066328

(22) International Filing Date:

18 December 2018 (18.12.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/609,892 22 December 2017 (22.12.2017) US

(71) Applicant: **FEND INCORPORATED** [US/US]; 4075
Wilson Blvd, 8th Fl, Arlington, Virginia 22203 (US).

(72) Inventors: **DUNN, Colin Patrick**; 4075 Wilson Blvd, 8th
Fl, Arlington, Virginia 22203 (US). **LEE, Sang Cheon**;
4075 Wilson Blvd, 8th Fl, Arlington, Virginia 22203 (US).

(74) Agent: **SCHAFER, Richard A.**; Blank Rome LLP, 717
Texas Avenue, Suite 1400, Houston, Texas 77002 (US).

(81) Designated States (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

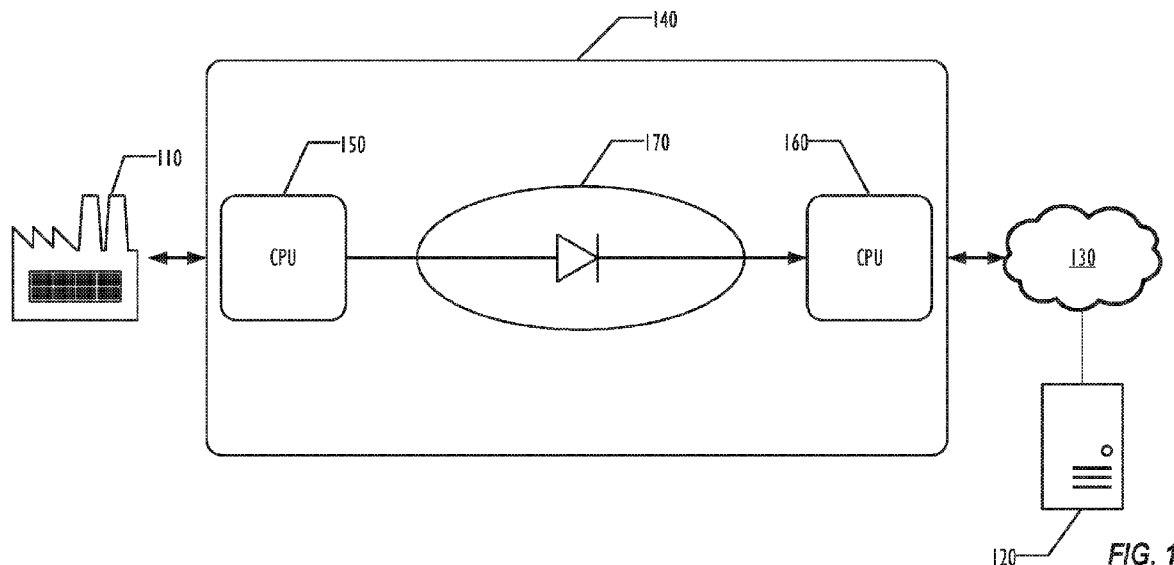
Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

- with international search report (Art. 21(3))

(54) Title: ONE-WAY DATA TRANSFER DEVICE WITH ONBOARD SYSTEM DETECTION



(57) Abstract: A data diode provides a flexible device for collecting data from a data source and transmitting the data to a data destination using one-way data transmission. On-board processing elements allow the data diode to identify automatically the type of connectivity provided to the data diode and configure the data diode to handle the identified type of connectivity.



WO 2019/126237 A1

ONE-WAY DATA TRANSFER DEVICE WITH ONBOARD SYSTEM DETECTION

TECHNICAL FIELD

[0001] The present invention relates to the field of security, and in particular to a compact network device that provides hardware enforced one-way data transfer from a protected data source.

BACKGROUND ART

[0002] Computer and network security is an area of considerable concern. While there is great interest in being able to remotely monitor resources such as industrial facilities across computer networks, lack of security of those monitored resources has required the development of specialized devices that provide defenses against security threats to computers, networks, and other devices in the monitored resources that go beyond the protection of firewalls and other traditional Internet security software and hardware systems. For high security resources, such as those used by government agencies and some commercial facilities, such as computer-controlled industrial facilities, energy, or water utilities, conventional firewall and other security systems may not provide reliable enough protection from undesired intrusions.

[0003] Today, we consider one single, high-value asset to be critical because to lose it would cause widespread disruption (for example: a power plant), but in aggregate, thousands of pieces of commercial equipment represent a similar threat and the number of attack vectors is exponentially higher. Widespread cyberattack of commercial or “subcritical” equipment, from building chillers to sewage pumps, would cause economic disruption and compromise public safety. For example, attacks on the air handlers in a region’s hospital network, the refrigeration equipment at pharmacies and grocery stores, or the chilled water pumps serving Virginia’s data centers could have severe impact.

[0004] For these types of resources, one-way data transfer may be a critical requirement to isolate the protected network from intrusion by malware or other malicious actors outside the protected network. While conventional Internet firewalls and software systems such as

specially configured operating system may be designed to restrict data transfer to unidirectional data flow, software-based one-way data transfer systems are difficult to validate and verify, and may be subject to intentional or inadvertent misconfiguration that may allow data leakage or intrusions in the reverse direction.

[0005] Malicious attacks to date have focused largely on data theft or network disruption, but attacks on physical assets are becoming more frequent. Attackers can compromise IoT devices and, for example, (a) Recruit devices into botnets used for distributed denial of service (DDOS) attacks; (b) Open a back door into a corporate network; or (c) Change operating behavior of the device, leading to device failure or safety concerns.

[0006] Data diode devices have been developed to provide hardware-enforced one-way data transfer, using techniques as simple as severing the receive pin in an RS-232 cable to more complex techniques involving the use of optical cables or opto-isolator components that transfer electrical signals between two isolated circuits with light. An opto-isolator (also called an optocoupler) uses a optical emitter such as an LED that generates light responsive to electrical signals, while an optical sensor such as a phototransistor receives the light and converts the light into electrical signals. Because there is electrical isolation between the two sides of the opto-isolator, this physically enforces one-way communication across the opto-isolator.

[0007] However, because common Internet protocols depend upon two-way communication, a data diode requires additional components beyond an opto-isolator (or a simple serial cable with the receive line interrupted) to allow effective one-way communication.

[0008] Traditional data diodes are used to protect critical infrastructure, such as nuclear reactors or oil refineries by broadcasting equipment status in a one-way manner. These traditional data diodes are expensive and have required customization by skilled implementation teams.

SUMMARY OF INVENTION

[0009] A data diode, comprises a first network interface circuitry, a second network interface circuitry, a one-way data bridge, a first firmware, and a second firmware. The first network interface circuitry comprises a first processing element; a first power connector, coupled to the first processing element for providing power to the first processing element; a first network connector, coupled to the first processing element. The second network interface circuitry, comprises a second processing element; a second power connector, coupled to the second processing element for providing power to the second processing element; and a second network connector, coupled to the second processing element. The one-way data bridge is coupled between the first processing element and the second processing element and allows data flow from the first processing element to the second processing element and physically prohibits data flow from the second processing element to the first processing element. The first firmware comprises instructions that when executed cause the first processing element to automatically determine which of a predetermined plurality of protocols is used for communications via the first network connector; and configure the first processing element to transmit the data across the one-way data bridge to the second processing element responsive to the determination. The second firmware comprises instructions that when executed cause the second processing element to automatically determine which of a predetermined plurality of protocols is used for communications via the second network connector; and configure the second processing element to transmit data received across the one-way data bridge by the second processing element responsive to the determination.

BRIEF DESCRIPTION OF DRAWINGS

[0010] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate an implementation of apparatus and methods consistent with the present invention and, together with the detailed description, serve to explain advantages and principles consistent with the invention. In the drawings,

[0011] Figure 1 is a high-level block diagram illustrating a data diode system according to one embodiment.

[0012] Figure 2 is a block diagram illustrating components of a data diode according to one embodiment.

DESCRIPTION OF EMBODIMENTS

[0013] In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention may be practiced without these specific details. In other instances, structure and devices are shown in block diagram form in order to avoid obscuring the invention. References to numbers without subscripts are understood to reference all instance of subscripts corresponding to the referenced number. Moreover, the language used in this disclosure has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the inventive subject matter, resort to the claims being necessary to determine such inventive subject matter. Reference in the specification to “one embodiment” or to “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiments is included in at least one embodiment of the invention, and multiple references to “one embodiment” or “an embodiment” should not be understood as necessarily all referring to the same embodiment.

[0014] Although some of the following description is written in terms that relate to software or firmware, embodiments can implement the features and functionality described herein in software, firmware, or hardware as desired, including any combination of software, firmware, and hardware. References to daemons, drivers, engines, modules, or routines should not be considered as suggesting a limitation of the embodiment to any type of implementation.

[0015] The terms “a,” “an,” and “the” are not intended to refer to a singular entity unless explicitly so defined, but include the general class of which a specific example may be used for illustration. The use of the terms “a” or “an” may therefore mean any number that is at least one, including “one,” “one or more,” “at least one,” and “one or more than one.”

[0016] The term “or” means any of the alternatives and any combination of the alternatives, including all of the alternatives, unless the alternatives are explicitly indicated as mutually exclusive.

[0017] The phrase “at least one of” when combined with a list of items, means a single item from the list or any combination of items in the list. The phrase does not require all of the listed items unless explicitly so defined.

[0018] As used herein, the term “a computer system” can refer to a single computer or a plurality of computers working together to perform the function described as being performed on or by a computer system.

[0019] In this description, the term “couple” or “couples” means either an indirect or direct wired or wireless connection. Thus, if a first device couples to a second device, that connection may be through a direct connection or through an indirect connection via other devices and connections. The recitation “based on” means “based at least in part on.” Therefore, if X is based on Y, X may be a function of Y and any number of other factors.

[0020] As used herein, the term “processing element” can refer to a single hardware processing element or a plurality of hardware processing elements that together may be programmed to perform the indicated actions. The hardware processing elements may be implemented as virtual hardware processing elements of a virtual programmable device hosted on a physical hardware device. Instructions that when executed program the processing element to perform an action may program any or all of the processing elements to perform the indicated action. Where the processing element is one or more multi-core processors, instructions that when executed program the processing element to perform an action may program any or all of the multiple cores to perform the indicated action.

[0021] As used herein, the term “malware” can refer to any software used to disrupt operation of a programmable device, gather sensitive information, or gain access to private systems or networks. Malware includes computer viruses (including worms, Trojan horses, etc.), Bots, ransomware, spyware, adware, scareware, and any other type of malicious program.

[0022] As used herein, the term “medium” can refer to a single physical medium or a plurality of media that together store the information described as being stored on the medium.

[0023] As used herein, the term “memory” can refer to a single memory device or a plurality of memory devices that together store the information described as being stored on

the medium. The memory may be any type of storage device, including random access memory, read-only memory, optical and electromechanical disk drives, etc.

[0024] FIG. 1 is a block diagram illustrating the use of a data diode according to one embodiment. In this example, a data source 110, such as a factory or other protected facility, is to provide data to a destination 120, such as a monitoring server. In some implementations, either or both of the source 110 and destination 120 may be directly connected to the data diode 140, or may be connected to the data diode 140 by one or more networks, such as the cloud network 130 illustrated FIG. 1. Although a single source 110 and a single destination 120 are illustrated in FIG. 1 for clarity of the drawing, the data diode 140 may support one-way communications from multiple sources 110 and multiple destinations 120 as desired. In the example illustrated in FIG. 1, the source is directly connected to the data diode 140 and connected to destination 120 that is a server connected via a cloud network 130; however, the data diode 140 may be connected at the source to any type of equipment, directly or indirectly, with or without an intervening network of any type. Similarly, the data diode 140 may be connected at the destination to any type of equipment, directly or indirectly, with or without an intervening network of any type.

[0025] Data diode 140 provides assurance that the data provided by source 110 is sent one-way only, physically preventing data from the destination 120 or elsewhere from reaching source 110. Data diode 140 generally comprises an onboard processing element 150 that communicates with source 110, an onboard processing element 160 that communicates with cloud 130, and a one-way coupler 170 that physically ensures that data passes only from processing element 150 to processing element 160, and not from processing element 160 to processing element 150. Processing elements 150 and 160 are programmed to allow the same data diode 140 to work with any of multiple protocols on either the source or destination side of the data diode, allowing a single model of the data diode 140 to be used in various environments without major configuration effort to accommodate various protocols.

[0026] FIG. 2 is a block diagram illustrating an example layout of the components of data diode 140 according to one embodiment. In this figure, certain common elements have been omitted for clarity of the drawing, but one of skill in the art would understand that those elements would be present in operable embodiment. Connections are illustrated as logical connections between elements, and one of skill in the art would understand that connections

between elements in the figure may involve multiple electrical traces instead of the single connector used to illustrate the connections between elements in the figure.

[0027] In one embodiment, a circuit board 200 may provide a base for mounting and connecting various components. Although identified as separate components by their function, one of skill in the art would understand that components illustrated as separate components may be combined into integrated components and that components illustrated as a single component may be split into separate components as desired.

[0028] The data diode 140 is comprised of two portions that communicate with each other in a one-way manner across one or more one way data bridges that enforce one-way communication. In some embodiments, photocouplers (also known as optocouplers or optical isolators) may be used for this purpose. In other embodiments, a laser and a photodetector may be used instead of an optocoupler. In other embodiments, an infrared transmitter and receiver may be used. In other embodiments, non-optical technique may be used, such as an audio speaker and a microphone may be used. In each case, the components provide the ability to enforce the one-way communication physically.

[0029] As illustrated in FIG. 2, a photocoupler 205 provides one-way data bridges between two processing elements 215, 220, with the photocoupler provided for communication from processing element 215 to processing element 220. Although illustrated as providing one-way communication from processing element 215 to processing element 220, other embodiments may configure the photocoupler 205 for one-way communication from processing element 220 to processing element 215.

[0030] No other electrical path connects processing elements 215 and 220. As illustrated in FIG. 2, each “side” of the data diode 140 may have its own power connection through power jacks 225, 230, typically DC power jacks. Although not shown in FIG. 2, in some embodiments each portion of the data diode 140 is implemented with separate grounding, further ensuring there is no path for data to traverse the data diode 140 in the reverse direction from the intended direction.

[0031] Processing elements 215, 220 may be any desired type of processing elements, including processors and microcontrollers. An example processing element may be an ARM®

Cortex® processor from ARM Limited. (ARM and CORTEX are registered trademarks of ARM Limited.) Each of the processing elements 215, 220 must be powerful enough to perform protocol detection and conversion for a plurality of protocols. Each of processing elements 215 may be programmed with firmware code to perform protocol manipulation to allow the processing element 215, 220 to recognize a communication protocol used by the source 110 and destination 120, and process the communication in a way that successfully allows the one-way communication, even if either or both of the communication protocols used by the source 110 or destination 120 require two-way communication. In such a scenario, one or both of processing elements 215, 220 may communicate in a two-way communication with the source 110 or destination 120 to which the processing element 215, 220 is connected, acting as proxy while performing one way communication across the optocoupler 205 between processing elements 215 and 220. In some embodiments, the communication protocol used to communicate between processing elements 215 and 220 may differ from either or both of the communication protocols used by source 110 and destination 120. Preferably, the processing elements 215, 220 are programmed to recognize the communication protocols used by source 110 and destination 120 automatically, allowing the data diode 140 to be coupled between the source 110 and destination 120 without manual configuration by the user or with minimal configuration as desired. Processing elements 215, 220 may contain on-board memory for storing the firmware used for operating the processing elements 215, 220 in some embodiments. In other embodiments, off-chip memory components (not illustrated in FIG. 2) may be provided and coupled to the processing elements 215, 220.

[0032] As illustrated in FIG. 2, the data diode 140 provides a plurality of different type connectors, allowing the data diode 140 to be used in different types of connectivity environments without requiring different models of the data diode 140 that depend upon the desired type of connectivity. As illustrated in FIG. 2, the left side of the figure is configured as the source side for data transport and provides an RS422/RS485 connector 240, a 5 pin connector 235, and an RJ45 connector 255 for Ethernet connection between the processing element 215 and the source 110. Similarly, the right side of the figure is configured as the destination side for data transport and provides a USB connector 295, an RS422/485 connector 290, and an Rj45 connector for Ethernet connections between the processing element 215 and the source 110. In some scenarios, more and one of the connectors on either or both the source or destination portion of the data diode 140 may be operable at the same time. These connector types are illustrative and by way of example only, and other types of connectors may be used

on either side of the data diode 140 in addition to or instead of the connectors illustrated in FIG. 2. In other embodiments, a single connector of any desired type may be provided on either side of the data diode 140, and different numbers and types of connectors may be provided on either side of the data diode 140 as desired.

[0033] Generally, there is two-way communication between any or all of the connectors 235, 240, and 255 and processing element 215, and between any or all of the connectors 295, 290, and 260 and processing element 220. As illustrated in FIG. 2, RS422/485 connector 240 is coupled to processing element 215 with RS422/RS485 interface 285A, while RS422/RS485 connector 290 is coupled to processing element 220 with RS422/RS485 interface 285B. In other embodiments, the processing elements 215, 220 may be capable of interfacing directly with RS422/RS485 connectors 240, 290 without an intermediary interface. As illustrated in FIG. 2, RJ45 connector 255 communicates with processing element 215 via Ethernet controller 245, while RJ45 connector 260 communicates with processing element 220 via IEEE 802.3 interface 80 and Ethernet transceiver 275. but other types of Ethernet coupling of the RJ45 connectors 255, 260 may be used.

[0034] In one embodiment, different components may be used for each “side” of the data diode 140. For example, RJ 45 connector 255 may be implemented in one embodiment with a RB1-125BAG1A connector manufactured by WIZnet, while RJ45 connector 260 may be implemented with a 2-406549-1 connector manufactured by TE Connectivity. In other embodiments, the same components may be used for both sides of the data diode 140.

[0035] In some embodiments, test sockets, such as test sockets 250A and 250B may be used for testing and debugging the hardware or firmware of the data diode 140. LEDs or other indicator devices may be included in the circuits of the data diode 140 to provide information for operation or debugging of the device. In some embodiments, the data diode 140 may include a display screen or a connector for a display screen to provide operational information. Similarly, embodiments of the data diode 140 may include an input device or a connector for an input device to allow information to be input into the device, such as for configuration purposes.

[0036] Each of processing elements 215 and 220 may include memory and firmware loaded into the memory for operation of the processing elements. The firmware comprises

firmware to allow each of the processing elements 215 and 220 to act as a proxy for the source 110 or destination 120, and to manage the one-way communication between them even though either or both of source and destination 110, 120 communicate with the data diode 140 using two-way communication protocols.

[0037] In various embodiments, the firmware loaded into memory on the processing elements 215 and 220 for converting two-way communication to one-way communication may be implemented on one or both processing elements 215 and 220. Embodiments may include firmware that detects the protocol used by source 110 or destination 120 and loads an appropriate conversion firmware module to convert the protocol used by source 110 or destination 120 into a one-way protocol for communicating between the processing elements 215, 220. Communication between the processing elements 215, 220 may be performed according to a standard one-way communication protocol or may be performed in some embodiments using a non-standard one-way protocol specifically designed for the data diode 140. For example, processing element 215 may detect a connection to source 110 that uses a TCP protocol and convert the TCP protocol into a UDP protocol for communicating with the processing element 220, which may then reconvert the UDP protocol into a TCP protocol for communicating with destination 120.

[0038] In one embodiment processing elements 215, 220 are preprogrammed with a plurality of protocol detection and conversion modules, allowing the data diode 140 to be placed into operation in a variety of environment without the need for pre-configuration. In some embodiments, because of the presence of a plurality of types of connectors on both the input and output sides of the data diode 140, the data diode 140 can be used with a connector to the source 110 of one type and a connector to the destination 120 of a different type. In some embodiments, control firmware may sequence between a predefined set of pre-loaded control protocols, such as BACnet, LonTalk, Modbus, DNP3, etc.) and determine what variables may be provided by the source 110, such as run time, system on/off status, temperature, fan speed, etc., and the processing element 215 or 220 may report those metrics across the optocoupler 205 at a predetermined interval or upon changes of the relevant metric. Similarly, in some embodiments, control firmware may sequence between a predefined set of pre-loaded control protocols for communicating with the destination. In some embodiments, one or more of processing elements 215 and 220 may encrypt the data received from the source 110 for delivery in encrypted form to destination 120, further enhancing the protection of the data from

the source 110. Such encryption may be performed using any desired encryption technique, include symmetric and asymmetric encryption techniques.

[0039] In some embodiments, the source side processing element 215 or 220 may attempt to communicate using a preprogrammed sequence of queries until it has determined what protocols the source 110 uses and what variables the source 110 can report.

[0040] Although some embodiments may be implemented with a single circuit board 200 as illustrated in FIG. 2, embodiments may be implemented with two separate circuit boards that are connected by the optocoupler 205. The specific connectors and supporting interface circuits illustrated in FIG. 2 are illustrative and by way of example only, and other connectors and supporting interface circuits may be used. In some embodiments, some of the components illustrated as separate components in FIG. 2 may be combined into one or more integrated components and in some embodiments components illustrated in FIG. 2 may be split into multiple components that together perform the desired function. The arrangement of components on the circuit board 200 of FIG. 2 is illustrative and by way of example only, and other arrangements can be used as desired. For example, in the illustrated embodiment of FIG. 2, the connectors 235, 240, 255, 260, 295, and 290 are on various edges of the circuit board 200, but in some embodiments, all of the connectors may be disposed on a single edge of the circuit board 200.

[0041] The circuit board 200 and the components disposed thereon are typically housed in a protective housing (not shown in the figures), which may be of any desired shape and configuration. For example, the data diode 140 may be housed in a 1U form factor case for mounting in a standard rack. In some embodiments, a transparent window may allow viewing LEDs or other indicators disposed on the circuit board 200 to indicate the state of the data diode 140. Some embodiments may provide a housing (not shown in the figures) that employs tamper-resistant techniques to prevent or detect tampering with the data diode 140. In some embodiments, a plurality of data diodes 140 may be housed in a common housing to act as channels for separate communication paths, where a plurality of links are desired between a single source 110 and a single destination 120, a single source 110 and a plurality of destinations 120, a plurality of sources 110 and a single destination 120, or a plurality of sources 110 and a plurality of destinations 120.

[0042] Although preferably preconfigured to be plugged in and automatically activated, some embodiments may allow configuration of the data diode 140 at the installation site or elsewhere prior to operation. In some embodiments, the data diode 140 is not configurable on-site. In some embodiments, any type of wired or wireless connection technique may be used to connect the data diode 140 to another device, such as mobile device with an appropriate app, for in-field setup or management of the data diode 140 and for collecting information from the data diode 140 regarding its operation. A geolocation module (not shown in FIG. 2) may be incorporated in some embodiments to allow the data diode 140 to report its location as geolocation coordinates based on geolocation data from a global satellite-based navigation system or other geolocation data providers.

[0043] In some embodiments, the data diode 140 may be configured with reporting firmware to allow a cloud-based data collection, display, and analytics platform to collect usage data from the data diode 140 and allow a user to create custom alerts, detect tampering with the data diode 140, and receive recommended actions drawn from predictive analytics.

[0044] The above description is intended to be illustrative, and not restrictive. For example, the above-described embodiments may be used in combination with each other. Many other embodiments will be apparent to those of skill in the art upon reviewing the above description.

We claim:

1. A data diode, comprising:

a first network interface circuitry comprising:

a first processing element;

a first network connector, coupled to the first processing element; and

a second network interface circuitry, comprising:

a second processing element; and

a second network connector, coupled to the second processing element;

a single one-way data bridge coupled between the first processing element and the second processing element that allows data flow from the first processing element to the second processing element and physically prohibits data flow from the second processing element to the first processing element;

a first firmware comprising instructions that when executed cause the first processing element to:

automatically determine that a first protocol of a first predetermined plurality of protocols is used for communications via the first network connector; and

configure the first processing element to receive data using the first protocol and transmit the data across the one-way data bridge to the second processing element responsive to the determination; and

a second firmware comprising instructions that when executed cause the second processing element to:

automatically determine that a second protocol of a second predetermined plurality of protocols is used for communications via the second network connector; and

configure the second processing element to transmit data received across the one-way data bridge by the second processing element using the second protocol, responsive to the determination,

wherein the first protocol is different from the second protocol.

2. The data diode of claim 1, wherein the one-way data bridge is an optocoupler.
3. The data diode of claim 1, wherein the one-way data bridge is an infrared device.
4. The data diode of claim 1, wherein the one-way data bridge is an acoustical device.
5. The data diode of claim 1, further comprising:

a tamper-resistant housing in which is disposed the first network interface circuitry, the second network interface circuitry, the one-way data bridge, the first firmware, and the second firmware.
6. The data diode of claim 5, wherein the tamper-resistant housing comprises a transparent window allowing external viewing of the interior of the tamper-resistant housing.

7. The data diode of claim 1,

wherein the first network interface circuitry comprises a plurality of different network connectors, each coupled to the first processing element, and

wherein the first firmware further comprises instructions that when executed cause the first processing element to identify which of the plurality of different network connectors provides data received by the first processing element and configures the first processing element responsive to the identification.
8. The data diode of claim 1, wherein the first network connector comprises a local area network connector.
9. The data diode of claim 1, wherein the first network connector comprises a point-to-point serial connector.
10. The data diode of claim 1, wherein the first network connector is of a different type than the second network connector.
11. The data diode of claim 1, wherein the second network interface circuitry comprises a plurality of different network connectors, each coupled to the second processing element, and

wherein the second firmware further comprises instructions that when executed cause the second processing element to identify which of the plurality of different network connectors provides data received by the second processing element and configures the second processing element responsive to the identification.

12. The data diode of claim 1,

wherein the first network interface circuitry further comprises a first power connector, coupled to the first processing element for providing power to the first processing element, and

wherein the second network interface circuitry further comprises a second power connector, coupled to the second processing element for providing power to the second processing element.

13. The data diode of claim 1, wherein the first network interface circuitry and the second network interface circuitry are separately grounded.

14. The data diode of claim 1, wherein the instructions that when executed cause the first processing element to automatically determine which of a predetermined plurality of protocols is used for communications via the first network connector comprise instructions that when executed cause the first processing element to sequence between a predefined set of pre-loaded control protocols.

15. The data diode of claim 1, wherein the instructions that when executed cause the second processing element to automatically determine which of a predetermined plurality of protocols is used for communications via the second network connector comprise instructions that when executed cause the second processing element to sequence between a predefined set of pre-loaded control protocols.

16. The data diode of claim 1, wherein the first firmware further comprises instructions that when executed cause the first processing element to encrypt data received via the first network connector.

17. The data diode of claim 1, wherein the second firmware further comprises instructions that when executed cause the second processing element to encrypt data transmitted via the second network connector.
18. The data diode of claim 1, wherein the first firmware comprises instructions to collect data via the first network connector and report the data at a pre-determined interval.
19. The data diode of claim 1, wherein the first firmware comprises instructions to collect data via the first network connector and report the data upon a change in the collected data.
20. The data diode of claim 1, wherein the data diode is not configurable on-site.

