

DATA LINK AND METHOD OF FORMING THE SAME

TECHNICAL FIELD

[0001] Various embodiments of this disclosure may relate to a data link. Various embodiments of this disclosure may relate to a method of forming a data link.

BACKGROUND

[0002] There has been a need to provide secure transfer of data between computer systems. Conventional technologies such as information technology (IT) centric firewalls provide policy/rule-based internet protocol (IP) traffic control, while unidirectional data diodes enforce IP data flow direction. A legacy serial port (RS232) provides data link with protocol break.

[0003] There is nascent demand from intended operators as awareness in cybersecurity threats in operational technology (OT) systems increases. Market demand can be seen as end-user driven. Currently, standard off-the-shelf IT security appliances, such as firewalls, are used as stopgap measures.

SUMMARY

[0004] Various embodiments may relate to a data link. The data link may include a transmitter hardware module configured to receive a data stream. The transmitter hardware module may be further configured to convert units in the data stream from having a size of eight data bits to having a size of a predetermined number of data bits before transmitting the data stream in parallel transmission. The size of the predetermined number of data bits may be of any whole number of 7 or less. The data link may also include a receiver hardware module

configured to receive the data stream from the transmitter hardware module. The receiver hardware module may be further configured to convert units in the data stream from having the size of the predetermined number of data bits to having the size of eight data bits. The disabled or unused bits may always be cleared. The data link may further include a pulse detection module configured to detect transmission in the data stream from the transmitter hardware module of one or more units having a size beyond the predetermined number of data bits. The pulse detection module may be configured to emit an alarm indication signal upon detection of the one or more units having the size beyond the predetermined number of data bits. The data link may additionally include a supervisory module configured to provide an alarm upon receiving the alarm indication signal from the pulse detection module.

[0005] Various embodiments may relate to a method of forming a data link. The method may include forming or providing a transmitter hardware module configured to receive a data stream. The transmitter hardware module may be further configured to convert units in the data stream from having a size of eight data bits to having a size of a predetermined number of data bits before transmitting the data stream in parallel transmission. The predetermined number of data bits may be of any whole number of 7 or less. The method may also include forming or providing a receiver hardware module configured to receive the data stream from the transmitter hardware module. The receiver hardware module may be further configured to convert units in the data stream from having the size of the predetermined number of data bits to having the size of eight data bits. The disabled or unused bits may always be cleared. The method may further include forming or providing a pulse detection module configured to detect transmission in the data stream from the transmitter hardware module of one or more units having a size beyond the predetermined number of data bits. The pulse detection module may be configured to emit an alarm indication signal upon detection of the one or more units having the size beyond the predetermined number of data bits. The method may additionally include forming or providing

a supervisory module configured to provide an alarm upon receiving the alarm indication signal from the pulse detection module.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] In the drawings, like reference characters generally refer to the same parts throughout the different views. The drawings are not necessarily drawn to scale, emphasis instead generally being placed upon illustrating the principles of various embodiments. In the following description, various embodiments of the invention are described with reference to the following drawings.

FIG. 1 is a general illustration of a data link according to various embodiments.

FIG. 2 is a general illustration of a method of forming a data link according to various embodiments.

FIG. 3 is a schematic of a data link according to various embodiments.

FIG. 4 is a schematic of a data link including a switch matrix according to various embodiments.

FIG. 5 is a schematic of a data link including a switch matrix and a pattern detector according to various embodiments.

FIG. 6 is a schematic of a data link including anti-tampering and protection features according to various embodiments.

FIG. 7 is a schematic showing a system including a pair of data links according to various embodiments.

DESCRIPTION

[0007] The following detailed description refers to the accompanying drawings that show, by way of illustration, specific details and embodiments in which the invention may be

practised. These embodiments are described in sufficient detail to enable those skilled in the art to practise the invention. Other embodiments may be utilized and structural, logical, and electrical changes may be made without departing from the scope of the invention. The various embodiments are not necessarily mutually exclusive, as some embodiments can be combined with one or more other embodiments to form new embodiments.

[0008] Embodiments described in the context of one of the data links, systems or devices are analogously valid for the other data links, systems or devices. Similarly, embodiments described in the context of a method are analogously valid for a data link/system/device, and vice versa.

[0009] Features that are described in the context of an embodiment may correspondingly be applicable to the same or similar features in the other embodiments. Features that are described in the context of an embodiment may correspondingly be applicable to the other embodiments, even if not explicitly described in these other embodiments. Furthermore, additions and/or combinations and/or alternatives as described for a feature in the context of an embodiment may correspondingly be applicable to the same or similar feature in the other embodiments.

[0010] In the context of various embodiments, the articles “a”, “an” and “the” as used with regard to a feature or element include a reference to one or more of the features or elements.

[0011] In the context of various embodiments, the term “about” or “approximately” as applied to a numeric value encompasses the exact value and a reasonable variance.

[0012] As used herein, the term “and/or” includes any and all combinations of one or more of the associated listed items.

[0013] FIG. 1 is a general illustration of a data link according to various embodiments. The data link may include a transmitter hardware module 102 configured to receive a data stream. The transmitter hardware module 102 may be further configured to convert units in the data stream from having a size of eight data bits (i.e. 1 byte) to having a size of a predetermined

number of data bits before transmitting the data stream in parallel transmission. The size of the predetermined number of data bits may be of any whole number of 7 or less. The data link may also include a receiver hardware module 104 configured to receive the data stream from the transmitter hardware module 102. The receiver hardware module 104 may be further configured to convert units in the data stream from having the size of the predetermined number of data bits to having the size of eight data bits. The disabled or unused bits may always be cleared. The data link may further include a pulse detection module 106 configured to detect transmission in the data stream from the transmitter hardware module 102 of one or more units having a size beyond the predetermined number of data bits. The pulse detection module 106 may be configured to emit an alarm indication signal upon detection of the one or more units having the size beyond the predetermined number of data bits. The data link may additionally include a supervisory module 108 configured to provide an alarm upon receiving the alarm indication signal from the pulse detection module 106.

[0014] In other words, the data link may include a transmitter hardware module 102, a receiver hardware module 104, a pulse detection module 106, and a supervisory module 108. The transmitter hardware module 102 may be configured to change the package size of data from 8 bits to less than 8 bits (e.g. 7 bits) before sending to the receiver hardware module 104. The receiver hardware module 104 may be configured to change the package size of data from the reduced size of less than 8 bits back to the size of 8 bits. The disabled or unused bits may always be cleared. The pulse detection module 106 may be configured to detect data sent by the transmitter hardware module 102 having a package size of more than the reduced size. Upon detection of such data, the pulse detection module 106 may cause the supervisory module 108 to raise an alarm.

[0015] For avoidance of doubt, FIG. 1 is a general illustration of various features of the data link according to various embodiments, and is not intended to limit the arrangement, orientation, shapes, sizes etc. of the various features.

[0016] Various embodiments may seek to address the needs for secured systems in critical infrastructure installations to receive data streams from external, possibly untrusted, systems in a safe manner by introducing transfer content restriction via software check methodology and strict hardware-based content restrictions. Compared to existing technologies such as IT firewall and data diodes, various embodiments may provide both an IP protocol break and restrictive data content transferred unidirectional into secured systems. Compared to legacy serial port/RS232 interfaces, various embodiments may afford much higher speed data transfer for the connecting systems while maintaining the IP protocol break.

[0017] In various embodiments, the predetermined number of data bits may be 7. Pins D0 – D6 of the transmitter hardware module 102 may be used for transmitting the data stream, while pins D0 – D6 of the receiver hardware module 104 may be used for receiving the data stream. The 7 data bits may be transmitted from the transmitter hardware module 102 to the receiver hardware module 104 using 7 data lines. However, it may also be envisioned that, in various other embodiments, the predetermined number of data bits is 6, 5, 4, 3 or 2. In various embodiments, the 2, 3, 4, 5, or 6 data bits may be transmitted using the 7 data lines. In various other embodiments, the 2, 3, 4, 5, or 6 data bits may be transmitted using a number of data lines equal to the predetermined number of data bits. For instance, various embodiments may use 6 data lines for parallel transmission of 6 data bits. The 2 remaining pins of the transmitter hardware module 102 may then be coupled to the pulse detection module 106, and the corresponding 2 pins of the receiver hardware module 104 may then be disabled.

[0018] The supervisory module 108 may also be referred to as a hardware supervisory module. The pulse detection module 106 may also be referred to as a pulse shaping/detection module.

[0019] In various embodiments, the data link may include a parallel channel, e.g. a parallel data bus, electrically connecting or coupling the transmitter hardware module 102 and the receiver hardware module 104. In various embodiments, electrically connecting or coupling a first component and a second component may refer to directly connecting or coupling the first component and the second component, while in other embodiments, it may refer to electrically connecting or coupling via one or more intermediate components, such as a switch matrix. The data bus may include a plurality of data lines electrically connecting the data pins of the transmitter hardware module 102 at one end and the data pins of the receiver hardware module 104 at another end. The data bus may be configured to transmit using parallel transmission data bits equal to the predetermined number of data bits (e.g. 7) at any one time. In other words, the data bus may be configured to transmit data bits equal to the predetermined number of data bits (e.g. 7 data bits) simultaneously. The plurality of data lines may be equal to or more than the predetermined number of data bits. For instance, 7 data lines may be used to transmit 2, 3, 4, 5, 6 or 7 bits. In various embodiments, converting units in the data stream from having a size of eight data bits to having a size of a predetermined number of data bits may refer to changing the data stream such that data bits equal to the predetermined number of data bits may be transmitted via parallel transmission from the transmitter hardware module 102 to the receiver hardware module 104 simultaneously, while converting units in the data stream from having the size of the predetermined number of data bits to having the size of eight data bits may refer to changing the data stream back from a modified condition (when the data stream is in parallel transmission from the transmitter hardware module 102 to the receiver hardware module) to an original condition (prior to the data stream being transmitted into the data link). The disabled

or unused bits may always be cleared. In other words, the receiver hardware module 104 may be configured to convert units in the 2 – 7 bits format to the 8 bits formats, with the disabled or unused bits set to ‘0’. For instance, when the parallel transmission is 7 bit data stream, the receiver hardware module 104 may set the 8th bit to ‘0’.

[0020] In various embodiments, the data link may include a data sink module. The data sink module may be electrically connected or coupled to the transmitter hardware module 102. The data sink module may be configured to provide integrity check on the data stream before the data stream is sent to the transmitter hardware module 102. The data sink module may include a transmit management (Tx mgmnt) module (also referred to as a transmit management software module). The transmit management module may be a software module. The transmit management module may be configured to manage or control transmission of the data stream from the data sink module to the transmit hardware module 102. The transmit management module may also be configured to provide integrity check on the data stream before the data stream is sent to the transmitter hardware module 102. For instance, the transmit management module may be configured to generate a hash for each file transferred to the transmitter hardware module. The data sink module may include a content verification software module, which may be a customized software module that ensures ASCII (American Standard Code for Information Interchange) text only content on the data stream received, and flags error if the data stream includes data other than ASCII text. However, it may be envisioned that, in some embodiments, the content verification software module may also perform other software check on the data stream received, and flag error for illegal content.

[0021] In various embodiments, the data link may also include a data source module. The data source module may be electrically connected or coupled to the receiver hardware module 104. The data source module may be configured to provide integrity check on the data stream received from the receiver hardware module 104. The data source module may include a receive

management (Rx mgmnt) module (also referred to as a receive management software module). The receive management module may be a software module which receives the data stream from the receiver hardware module 104. The receive management module may be configured to perform data stream reconstruction and primary data integrity check functions. For instance, the receive management module may be configured to recalculate a hash for each file received. The receive management module may compare the recalculated hash against the hash calculated by the transmit management module, and may mark the file as a bad file if the recalculated hash does not match with the hash calculated by the transmit management module. The data source module may also include a content verification software module that ensures ASCII text only content on the data stream received from the receive management module, and flags error if the data stream includes data other than ASCII text. However, it may be envisioned that in some embodiments, the content verification software module may also perform other software check on the data stream received, and flag error for illegal content before the data link outputs the data stream. The content verification software in the data source module and the content verification software in the data sink module may be duplicated and may contain the same software check algorithm.

[0022] In various embodiments, the data sink module may serve as an input port of the data link, while the data source module may serve as an output port of the data link. In various embodiments, the data link may be a data transfer device including an input port and an output port. The data sink module may be configured to be connected to a computer or computing device, while the data source module may be configured to be connected to another computer or computing device. The computer or computing device in which the data sink module is connected to and/or the computer device in which the data source module is connected to may be part of a critical infrastructure installation or operational technology system.

[0023] In various embodiments, the receiver hardware module 104 may be configured to prevent from receiving one or more additional data bits in excess of the predetermined number of data bits. For instance, the size of the predetermined number of data bits may be 7. As such, when the receiver hardware module 104 receives a data stream having units of 8 bits, the receiver hardware module 104 may be configured to prevent from receiving the additional data bit (i.e. the 8th bit). The pins of the receiver hardware module 104 corresponding to the one or more additional bits may be disabled to prevent the receiver hardware module 104 from receiving the one or more additional bits. For instance, if the size of the predetermined number of data bits is 7, D7 of the receiver hardware module 104 corresponding to the 8th bit may be disabled.

[0024] In various embodiments, the transmitter hardware module 102 may include a first-in-first-out (FIFO) ring buffer. The transmitter hardware module 102 may also include a serializer/deserializer (SerDes) electrically connected or coupled to the first-in-first-out (FIFO) ring buffer. The transmitter hardware module 102 may also include a direct memory access (DMA) channel electrically connecting or coupling the first-in-first-out (FIFO) ring buffer and the serializer/deserializer (SerDes). The data stream from the data sink module may be provided to the FIFO ring buffer of the transmitter hardware module 102. The FIFO ring buffer of the transmitter hardware module 104 may be configured to hold 8 bits at one time. The byte (8 bits) stored in the FIFO ring buffer of the transmitter hardware module 102 may be sent to the serializer/deserializer (SerDes) via the DMA channel. The serializer/deserializer (SerDes) may be configured to deserialize each byte into 8 constituent bits. Only the predetermined number of data bits (e.g. 7) may be transmitted (e.g. via 7 physical wires) across to the receiver hardware module 104. The 7 electrical signals may be transmitted along the 7 physical wires (i.e. one electrical signal along each line) connecting the transmitter hardware module 102 and the receiver hardware module 104. The one or more additional bits (e.g. the 8th or most significant

bit) may be transmitted to the pulse detector 106. In various embodiments, the receiver hardware module 104 may include a first-in-first-out (FIFO) ring buffer. The receiver hardware module 104 may also include a serializer/deserializer (SerDes) electrically connected or coupled to the first-in-first-out (FIFO) ring buffer. The receiver hardware module 104 may also include a direct memory access (DMA) channel electrically connecting or coupling the first-in-first-out (FIFO) ring buffer and the serializer/deserializer (SerDes). The units in the data stream having the size of the predetermined number of data bits (e.g. 7) received from the transmitter hardware module 102 may be converted to the size of 8 bits before being stored in the FIFO ring buffer. The disabled or unused bits may be cleared before being stored in the FIFO ring buffer.

[0025] In various embodiments, data pins of the transmitter module 102 that are not used to transmit the data bits may be electrically connected or coupled to the pulse detection module 106. In various embodiments, if the predetermined number of bits is 7, a most significant bit (MSB) pin, i.e. the 8th bit pin (data pin D7), of the transmitter hardware module 102 may be electrically connected or coupled to the pulse detection module 106. In other words, data pin D7 of the transmitter hardware module 102 which may not be used for transmission of data bits to the receiver hardware module 104 may be coupled to the pulse detection module 106. Accordingly, the pulse detection module 106 may detect the one or more units having the size beyond the predetermined number of data bits. In various other embodiments, the predetermined number of bits may be any suitable number. The plurality of data lines may be equal to or more than the predetermined number of data bits.

[0026] In various embodiments, the data link may include a switch matrix configured to scramble units in the data stream having the size of the predetermined number of data bits during transmission from the transmitter hardware module 102 to the receiver hardware module 104. The switch matrix may also be referred to as a scrambler module.

[0027] In various embodiments, data pins of the transmitter hardware module 102 (i.e. pins for transmission of the data stream) may be mapped to data pins of the receiver hardware module 104 (i.e. pins for receiving the data stream) using one or more map pattern codes. The switch matrix may be configured to route data bits from the transmitter hardware module 102 to the receiver hardware module 104 based on the one or more map pattern codes. For instance, a map code pattern may electrically connect or couple D0 pin of the transmitter hardware module 102 to D0 pin of the receiver hardware module 104 (to electrically route a data bit from the D0 pin of the transmitter hardware module 102 to the D0 pin of the receiver hardware module 104), D1 pin of the transmitter hardware module 102 to D1 pin of the receiver hardware module 104 (to electrically route a data bit from the D1 pin of the transmitter hardware module 102 to the D1 pin of the receiver hardware module 104), D2 pin of the transmitter hardware module 102 to D2 pin of the receiver hardware module 104 (to electrically route a data bit from the D2 pin of the transmitter hardware module 102 to the D2 pin of the receiver hardware module 104), D3 pin of the transmitter hardware module 102 to D3 pin of the receiver hardware module 104 (to electrically route a data bit from the D3 pin of the transmitter hardware module 102 to the D3 pin of the receiver hardware module 104), D4 pin of the transmitter hardware module 102 to D4 pin of the receiver hardware module 104 (to electrically route a data bit from the D4 pin of the transmitter hardware module 102 to the D4 pin of the receiver hardware module 104), D5 pin of the transmitter hardware module 102 to D5 pin of the receiver hardware module 104 (to electrically route a data bit from the D5 pin of the transmitter hardware module 102 to the D5 pin of the receiver hardware module 104), and D6 pin of the transmitter hardware module 102 to D6 pin of the receiver hardware module 104 (to electrically route a data bit from the D6 pin of the transmitter hardware module 102 to the D6 pin of the receiver hardware module 104). The example map code pattern may be illustrated by Table 1.

Transmitter Hardware Module	Receiver Hardware Module
-----------------------------------	--------------------------------

D0	D0
D1	D1
D2	D2
D3	D3
D4	D4
D5	D5
D6	D6

Table 1

[0028] Another map code pattern may electrically connect or couple D0 pin of the transmitter hardware module 102 to D6 pin of the receiver hardware module 104 (to electrically route a data bit from the D0 pin of the transmitter hardware module 102 to the D6 pin of the receiver hardware module 104), D1 pin of the transmitter hardware module 102 to D5 pin of the receiver hardware module 104 (to electrically route a data bit from the D1 pin of the transmitter hardware module 102 to the D5 pin of the receiver hardware module 104), D2 pin of the transmitter hardware module 102 to D4 pin of the receiver hardware module 104 (to electrically route a data bit from the D2 pin of the transmitter hardware module 102 to the D4 pin of the receiver hardware module 104), D3 pin of the transmitter hardware module 102 to D3 pin of the receiver hardware module 104 (to electrically route a data bit from the D3 pin of the transmitter hardware module 102 to the D3 pin of the receiver hardware module 104), D4 pin of the transmitter hardware module 102 to D2 pin of the receiver hardware module 104 (to electrically route a data bit from the D4 pin of the transmitter hardware module 102 to the D2 pin of the receiver hardware module 104), D5 pin of the transmitter hardware module 102 to D1 pin of the receiver hardware module 104 (to electrically route a data bit from the D5 pin of the transmitter hardware module 102 to the D1 pin of the receiver hardware module 104), and D6 pin of the transmitter hardware module 102 to D0 pin of the receiver hardware module 104 (to electrically route a data bit from the D6 pin of the transmitter hardware module 102 to the D0 pin of the receiver hardware module 104). Other map code patterns may route data bits from the transmitter hardware module 102 to the receiver hardware module 104 via other combinations of pins. The example map code pattern may be illustrated by Table 2.

Transmitter Hardware Module	Receiver Hardware Module
D0	D6
D1	D5
D2	D4
D3	D3
D4	D2
D5	D1
D6	D0

Table 2

In other words, depending on the map code pattern, data bits transmitted from the data pins of the transmitter hardware module 102 may be directed or provided to different data pins of the receiver hardware module 104. The possible number of map pattern codes of different combinations may be 5040 (factorial of 7). In various embodiments, it may be possible to transmit any predetermined number of data bits along the 7 data lines connecting the data pins of the transmitter hardware module 102 and the data pins of the receiver hardware module 104. The possible number of map pattern codes may still be 5040. In yet various other embodiments, it may be possible to transmit the predetermined number of bits along a number of data lines equal to the predetermined number of data bits. For instance, 6 data lines may be used for parallel transmission of 6 data bits. The 2 remaining pins of the transmitter hardware module 102 may then be coupled to the pulse detection module 106, and the corresponding 2 pins of the receiver hardware module 104 may be disabled. The number of permutations possible may then be 720 (factorial of 6).

[0029] The sequence of map pattern codes sent to the switch matrix may be referred to as a scrambling sequence. One map pattern code in the scrambling sequence may be different from another map pattern code in the scrambling sequence. In other words, in the scrambling sequence, the mapping of the data pins of the transmitter hardware module 102 to the data pins of the receiver hardware module 104 may continuously be changing.

[0030] In various embodiments, the switch matrix may be electrically connected or coupled to the supervisory module 108. The scrambling sequence may be sent from the supervisory

module 108 to the switch matrix to scramble the routing or electrical connection/coupling of the data pins of the transmitter hardware module 102 to the data pins of the receiver hardware module 104.

[0031] In various embodiments, the data link may also include a pattern detector configured to detect transmission in the data stream from the transmitter hardware module of the one or more units having the size beyond the predetermined number of data bits before the data stream is received by the switch matrix. In various embodiments, the pattern detector may replace or be the pulse detection module 106. The pattern detector may be configured to detect transmission in the data stream from the transmitter hardware module of one or more units having a size beyond the predetermined number of data bits, and further configured to emit an alarm indication signal upon detection of the one or more units having the size beyond the predetermined number of data bits, similar to the pulse detection module 106. In addition, the pattern detector may be configured to detect electrical patterns on the data lines. The pattern detector may be configured to discriminate against certain electrical patterns, while allowing for the transmission of other electrical patterns. For instance, the pattern detector may discriminate against electrical patterns representing ASCII characters such as capital letters ‘A’ or ‘B’ as illustrated in Table 3 below, but may allow transmission of electrical patterns representing ASCII characters electrical patterns representing other ASCII characters such as small letters ‘a’ or ‘b’.

ASCII char	D0	D1	D2	D3	D4	D5	D6	Pattern Detector Output
a	1	0	0	0	0	1	1	Valid
A	1	0	0	0	0	0	1	Illegal
b	0	1	0	0	0	1	1	Valid
B	0	1	0	0	0	0	1	Illegal

Table 3

[0032] In various embodiments, the data link may include one or more mechanical tamper switches. The data link may also include a tamper detection controller electrically connected to the one or more mechanical tamper switches. The tamper detection controller may also be electrically connected to the supervisory module.

[0033] In various embodiments, the data link module may be one of a pair of data link modules. The data link module may include a dedicated port for connecting to another data link module of the pair of data link modules using a dedicated High Availability (HA) Communication Cable

[0034] FIG. 2 is a general illustration of a method of forming a data link according to various embodiments. The method may include, in 202, forming or providing a transmitter hardware module configured to receive a data stream. The transmitter hardware module may be further configured to convert units in the data stream from having a size of eight data bits to having a size of a predetermined number of data bits before transmitting the data stream in parallel transmission. The predetermined number of data bits may be of any whole number of 7 or less. The method may also include, in 204, forming or providing a receiver hardware module configured to receive the data stream from the transmitter hardware module. The receiver hardware module may be further configured to convert units in the data stream from having the size of the predetermined number of data bits to having the size of eight data bits. The disabled or unused bits may always be cleared. The method may further include, in 206, forming or providing a pulse detection module configured to detect transmission in the data stream from the transmitter hardware module of one or more units having a size beyond the predetermined number of data bits. The pulse detection module may be configured to emit an alarm indication signal upon detection of the one or more units having the size beyond the predetermined number of data bits. The method may additionally include, in 208, forming or providing a supervisory

module configured to provide an alarm upon receiving the alarm indication signal from the pulse detection module.

[0035] In other words, the method may include forming or providing a transmitter hardware module, a receiver hardware module, a pulse detection module and a supervisory module. The transmitter hardware module may be configured to change the package size of data from 8 bits to less than 8 bits (e.g. 7 bits) before sending to the receiver hardware module. The receiver hardware module may be configured to change the package size of data from the reduced size of less than 8 bits back to the size of 8 bits. The disabled or unused bits may always be cleared. The pulse detection module may be configured to detect data sent by the transmitter hardware module having a package size of more than the reduced size. Upon detection of such data, the pulse detection module may cause the supervisory module to raise an alarm.

[0036] For avoidance of doubt, FIG. 2 is not intended to limit the sequence of various steps. For instance, step 202 may occur before, after or at the same time as step 204.

[0037] In various embodiments, the method may include electrically connecting or coupling the transmitter hardware module and the receiver hardware module. The method may also include electrically connecting or coupling the pulse detection module and the transmitter hardware module. The method may include electrically connecting or coupling the supervisory module and the pulse detection module.

[0038] In various embodiments, the method may include providing or forming a data sink module. The method may include electrically connecting or coupling the data sink module and the transmitter hardware module, e.g. via a serial bus. The method may also include electrically connecting or coupling the data sink module and the supervisory module.

[0039] In various embodiments, the method may include providing or forming a data source module. The method may include electrically connecting or coupling the data source module

and the receiver hardware module, e.g. via a serial bus. The method may also include electrically connecting or coupling the data source module and the supervisory module.

[0040] In various embodiments, the receiver hardware module may be configured to prevent from receiving one or more additional data bits in excess of the predetermined number of data bits.

[0041] In various embodiments, the receiver hardware module may include a first-in-first-out ring buffer. The receiver hardware module may also include a serializer/deserializer (SerDes) coupled to the first-in-first-out (FIFO) ring buffer. The receiver hardware module may also include a direct memory access (DMA) channel coupling the first-in-first-out (FIFO) ring buffer and the serializer/deserializer (SerDes).

[0042] In various embodiments, the transmitter hardware module may include a first-in-first-out ring buffer. The transmitter hardware module may also include a serializer/deserializer (SerDes) coupled to the first-in-first-out (FIFO) ring buffer. The transmitter hardware module may also include a direct memory access (DMA) channel coupling the first-in-first-out (FIFO) ring buffer and the serializer/deserializer (SerDes).

[0043] In various embodiments, a most significant bit (MSB) pin of the transmitter hardware module may be electrically connected or coupled to the pulse detection module. The method may include electrically connecting or coupling the MSB pin of the transmitter hardware module to the pulse detection module.

[0044] In various embodiments, the predetermined number of data bits may be any whole number from 2 to 7, e.g. 7. In other words, the predetermined number of data bits may be 2, 3, 4, 5, 6 or 7. The plurality of data lines may be equal to or more than the predetermined number of data bits

[0045] In various embodiments, the method may further include providing or forming a switch matrix configured to scramble units in the data stream having the size of the

predetermined number of data bits during transmission from the transmitter hardware module to the receiver hardware module. The method may include electrically connecting or coupling input ports of the switch matrix to the data pins of the transmitter hardware module. The method may include electrically connecting or coupling output ports of the switch matrix to the data pins of the receiver hardware module.

[0046] In various embodiments, data pins of the transmitter hardware module may be mapped to data pins of the receiver hardware module using one or more map pattern codes.

[0047] In various embodiments, the switch matrix may be electrically connected or coupled to the supervisory module. The supervisory module may be configured to send the one or more map pattern codes to the switch matrix, thereby controlling the scrambling of the units in the data stream. The method may include electrically connecting or coupling the supervisory module to a switch logic of the switch matrix.

[0048] In various embodiments, the method may also include providing or forming a pattern detector configured to detect transmission in the data stream from the transmitter hardware module of the one or more units having the size beyond the predetermined number of data bits before the data stream is received by the switch matrix. The method may include electrically connecting or coupling input ports of the pattern detector to the data pins of the transmitter hardware module. The method may include electrically connecting or coupling output ports of the pattern detector to input ports of the switch matrix. The method may also include electrically connecting or coupling output ports of the switch matrix to data pins of the receiver hardware module.

[0049] In various embodiments, the method may include providing one or more mechanical tamper switches. The method may also include electrically connecting a tamper detection controller to the one or more mechanical tamper switches. The tamper detection controller may also be electrically connected to the supervisory module.

[0050] In various embodiments, the data link module may be one of a pair of data link modules. The data link module may include a dedicated port for connecting to another data link module of the pair of data link modules using a dedicated High Availability (HA) Communication Cable.

[0051] Various embodiments may enforce a strict 7 bit-only ASCII (American Standard Code for Information Interchange) character data flow from the input port to the output port.

[0052] Various embodiments may introduce a break of internet protocol (IP) for the data flow from input port to the output port similar to a legacy serial/RS232 data link with the addition of restricting the transmission to only 7 bit ASCII characters across the data link by coupling each bit independently. Standard IT firewalls and unidirectional data-diodes send data as packets (groups of bits) and rely on internet protocol.

[0053] Various embodiments may relate to a content restrictive data link or data transfer device connecting between computer systems. The targeted application/user case may be for at least one end of the systems being a part of critical infrastructure installations or operational technology (OT) systems.

[0054] Various embodiments may allow for safe and secure transfer of data streams into secure systems by using a layered approach for software-based content checking and physical transfer restriction based on customized hardware that is designed to transfer 7-bit data across the data link.

[0055] Various embodiments may relate to a data forwarder solution.

[0056] FIG. 3 is a schematic of a data link according to various embodiments. The data link may include a transmitter hardware module 302 (also referred to as transmitter module), a receiver hardware module 304 (also referred to as receiver module), a pulse shaping/detection module 306, a hardware (HW) supervisory module 308, a data sink module 310, and a data

source module 312. Various embodiments may also include a minimal man-machine interface (MMI) 314.

[0057] The data sink module 310 may be an off-the-shelf computing module hardware. The data sink module 310 may serve as input port (IN) to the device. The data sink module may include a secure file transfer protocol (sFTP) module 310a, which is an IP network file transfer protocol that enables the data sink module 310 to receive data stream from an external computing device or computer. The data sink module 310 may include a content verification software module 310b, which may be a customized software module that ensures ASCII text only content on the data stream received from the secure file transfer protocol (sFTP) module 310a, and flags error if the data stream includes data other than ASCII text. However, it may be envisioned that, in some embodiments, the content verification software module 310b may also perform other software check on the data stream received from the secure file transfer protocol (sFTP) module 310a, and flag error for illegal content. The data sink module 310 may further include transmit management software module (Tx mgmnt) 310c. The function of the transmit management software module 310c may be to manage transmission of data stream received from content verification software module 310b to the transmitter hardware module 302 and to provide data integrity check. For instance, the transmit management software module 310c may be configured to generate a hash for each file transferred to the transmitter hardware module 302. The secure file transfer protocol (sFTP) module 310a, the content verification software module 310b and the transmit management software module (Tx mgmnt) 310c may reside or may be included in one or more processors or circuit arrangements of the data sink module 310. The data sink module 310 may be electrically connected or coupled to the transmitter hardware module 302.

[0058] The data source module 312 may be an off-the-shelf computing module hardware. The data source module 312 may be electrically connected or coupled to the receiver hardware

module 304. The data source module 312 may include the receive management (Rx mgmnt) software module 312a, which may receive the data stream from the receiver hardware module 304, and which may perform data stream reconstruction as well as primary data integrity check functions on the data stream. For instance, the receive management (Rx mgmnt) software module 312a may recalculate a hash for each file received. The receive management (Rx mgmnt) software module 312a may compare the recalculated hash against the hash calculated by the transmit management software module 310c, and may mark the file as a bad file if the recalculated hash does not match with the hash calculated by the transmit management software module 310c. The data source module 312 may also include a content verification software module 312b that ensures ASCII text only content on the data stream received from the receive management (Rx mgmnt) software module 312a, and flags error if the data stream includes data other than ASCII text. However, it may be envisioned that in some embodiments, the content verification software module 312b may also perform additional content checking of the data stream received from the receive management (Rx mgmnt) software module 312a before releasing the data stream for onwards propagation. The data source module 312 may additionally include a secure file transfer protocol (sFTP) module 312c, which is an IP network protocol that enables the data source module 312 to transmit the data stream received from the content verification software module 312b to an external computing device or computer. The receive management (Rx mgmnt) software module 312a, the content verification software module 312b and the secure file transfer protocol (sFTP) module 312c may reside or may be included in one or more processors or circuit arrangements of the data sink module 310.

[0059] The transmitter hardware module 302 may be a customized hardware that accepts the data stream from data sink module 310 and prepare the data stream for transmission of individual bytes within the data stream using a ring buffer 302a, which may be a part of the transmitter hardware module 302. The data link may include a high speed host serial bus 316

electrically connecting or coupling the data sink module 310 and the transmitter hardware module 302. The data bytes in the ring buffer 302a may be processed in first-in-first-out (FIFO) basis. The ring buffer 302a may be configured to generate or output the signals/data bits in a serial format. The transmitter hardware module 302 may also include a serializer/deserializer (SerDes) 302b. The serializer/deserializer (SerDes) 302b may convert the signals/data bits transmitted serially from the first-in-first-out (FIFO) ring buffer 302a into a parallel form for subsequent parallel transmission. Each byte (8bits) from the ring buffer 302a may be deserialized into 8 constituent bits. In other words, the serializer/deserializer (SerDes) 302b may convert the data stream from the ring buffer 302a for parallel transmission. The transmitter hardware module 302 may also include a direct memory access (DMA) channel 302c coupling the first-in-first-out (FIFO) ring buffer 302a and the serializer/deserializer (SerDes) 302b. Only the predetermined number of bits, e.g. 7 bits, may be transmitted to the receiver hardware module 304 using parallel transmission. The one or additional bits, e.g. the 8th bit, may be transmitted to the pulse detector 306.

[0060] The receiver hardware module 304 may be a customized hardware module that interfaces with the transmitter hardware module 302. The receiver hardware module 304 may be configured to receive the data stream from the transmitter hardware module 302 via parallel transmission. The data link may include a parallel channel 318, e.g. a parallel data bus, electrically connecting or coupling the transmitter hardware module 302 and the receiver hardware module 304. The parallel data bus may include a plurality of data lines extending from the data pins of the transmitter hardware module 302 to the data pins of receiver hardware module 304. The 7 bit electrical signals (using pins D0 – D6) received by the receiver hardware module 304 may be converted to a data byte. The disabled or unused bits may always be cleared before storing in a FIFO ring buffer 304a. The FIFO ring buffer 304a may be part of the receiver hardware module 304. The 8 bits stored in the FIFO ring buffer 304a may be transferred to a

serializer/deserializer (SerDes) 304b as described in more detail below, In addition to data bits, the parallel data bus may also transmit clock (CLK) signals, control (CTRL) signals, and status (STAT) signals between the transmitter hardware module 302 and the receiver hardware module 304. The clock (CLK) signals may synchronise the transmitter hardware module 302 and the receiver hardware module 304. The control (CTRL) signals may indicate the direction of flow of the data stream and may also include handshaking signals between the transmitter hardware module 302 and the receiver hardware module 304. The status (STAT) signals may indicate whether the data bits have been transmitted properly.

[0061] The receiver hardware module 304 may also include a serializer/deserializer (SerDes) 304b, which may convert the data byte (i.e. units in 8 bits) transmitted from the FIFO ring buffer 304a in parallel into a serial form for subsequent serial transmission. In other words, the serializer/deserializer (SerDes) 304b may be configured to convert the data stream that is transmitted in parallel to the receiver hardware module 304 for subsequent serial transmission. The receiver hardware module 304 may also include a direct memory access (DMA) channel 304c coupling the first-in-first-out (FIFO) ring buffer 304a and the serializer/deserializer (SerDes) 304b. The bytes stored in the FIFO ring buffer 304a may be transferred (via the serializer/deserializer (SerDes) 304b) to the data source module 312 (i.e. the receive management (Rx mgmnt) software module 312a) for onwards processing. The receiver hardware module 304 may have its 8th data bit (i.e. D7) physically disabled to prevent any unintended reception of signal. The data link may also include a high speed host serial bus 320 electrically connecting or coupling the receiver hardware module 304 and the data source module 312. The data stream may be transmitted from the receiver hardware module 304 to the data source module 312 via the high speed host serial bus 320.

[0062] The pulse shaping/detection module 306 may be hardware circuitry designed or configured to trigger upon detection of a pulsed voltage signal corresponding to width of at

least one single bit of data transmitted by the transmitter hardware module 302. In order to detect for attempts to transmit a byte containing the 8th bit (most significant bit, MSB), the data pin (D7) of the transmitter hardware module 302 may be fed as input to the pulse shaping/detection module 306. Upon detection of the attempt to transmit the 8th bit, the pulse shaping/detection module 306 may convey or transmit an alarm indication signal to the hardware supervisory module 308. The hardware supervisory module 308 may be configured to provide an alarm upon receiving the alarm indication signal. In various embodiments, the pulse shaping/detection module 306 may be configured to detect for a single pulse.

[0063] It may also be envisioned that in various other embodiments, the pulse shaping/detection module 306 may be replaced by a pattern detector, such as the pattern detector 528 shown in FIG. 5, which may be configured to detect for certain electrical patterns instead of a single pulse.

[0064] The hardware supervisory module 308 may be configured to control, supervise and monitor the overall operational status of the data link. The data link may also include a simple man-machine interface (MMI) 314 electrically connected or coupled to the hardware supervisory module 308. The man-machine interface 314 may be implemented in the form of a front panel mini-liquid crystal display (LCD) display and user input button. The hardware supervisory module 308 may be electrically connected or coupled to the data sink module 310 and/or the data source module 312. Both the data sink module 310 and data source module 312 may periodically report operational status and abnormal alarm to the hardware supervisory module 308 for status display and heartbeat/lifecheck purpose. The electrical connections or coupling between the hardware supervisory module 308 with the data sink module 310 and/or the data source module 312 may allow the hardware supervisory module 308 to assert full system initialization signal to the data sink module 310 and the data source module 312 to bring the system to an initial known operational state.

[0065] In various embodiments, the secure file transfer protocol (sFTP) modules, the content verification software modules 310b, 312b, the transmit management software module (Tx mgmnt) 310c and the receive management (Rx mgmnt) software module 312a may include any suitable code or algorithm to perform the function as described herein.

[0066] In various embodiments, the transmitter hardware module 302, the receiver hardware module 304, the data sink module 310 and the data source module 312 may be implemented via any suitable means. For instance, the transmitter hardware module 302 may be a processor, microcontroller (MCU) or circuit (such as a Field Programmable Gate Arrays (FPGA) or an Application Specific Integrated Circuit (ASIC)), or a part thereof. Likewise, the receiver hardware module 304, the data sink module 310 and the data source module 312 may each be a processor, microcontroller (MCU) or circuit (such as a Field Programmable Gate Arrays (FPGA) or an Application Specific Integrated Circuit (ASIC)), or a part thereof. The data sink module 310 and/or the data source module 312 may be processors or circuits. Alternatively, the data sink module 310 (or/and data source module 312) may be a microcontroller (MCU) in cases in which the software processing or throughput requirements is minimized or off-loaded to external hosts and the interface is simplified. In such a case, User Datagram Protocol (UDP) or Transmission Control Protocol/Internet Protocol (TCP/IP) may be used instead of sFTP.

[0067] Various embodiments may relate to a data link including additional hardware circuitry, such as a switch matrix or a scrambler module, to scramble the data bits during transmission from the transmitter hardware module to the receiver hardware module.

[0068] FIG. 4 is a schematic of a data link including a switch matrix 422 according to various embodiments. In addition to the switch matrix 422, the data link may also include a transmitter hardware module 402, a receiver hardware module 404, and a hardware supervisory module 408. There may also be an external transmit host (Tx host) 424 electrically connected or coupled

to the transmitter hardware module 402, and an external receive host (Rx host) 426 electrically connected or coupled to the receiver hardware module 404.

[0069] The scrambling of bit pattern as received by the receiver hardware module 404 may provide an additional layer of protection to the receive host 426 electrically connected or coupled to the receiver hardware module 404 in the event that the transmitter hardware module 402 and/or the external transmit host (Tx host) 424 is compromised.

[0070] The switch matrix 422 may electrically route each of the data signals (provided by pins D0 - D6 of the transmitter hardware module 402) to the corresponding pins of the receiver hardware module 404, in any combination as determined by a map pattern code. For instance, a map code pattern may electrically connect or couple D0 pin of the transmitter hardware module 402 to D0 pin of the receiver hardware module 404 (to electrically route a data bit from the D0 pin of the transmitter hardware module 402 to the D0 pin of the receiver hardware module 404), D1 pin of the transmitter hardware module 402 to D1 pin of the receiver hardware module 404 (to electrically route a data bit from the D1 pin of the transmitter hardware module 402 to the D1 pin of the receiver hardware module 404), D2 pin of the transmitter hardware module 402 to D2 pin of the receiver hardware module 404 (to electrically route a data bit from the D2 pin of the transmitter hardware module 402 to the D2 pin of the receiver hardware module 404), D3 pin of the transmitter hardware module 402 to D3 pin of the receiver hardware module 404 (to electrically route a data bit from the D3 pin of the transmitter hardware module 402 to the D3 pin of the receiver hardware module 404), D4 pin of the transmitter hardware module 402 to D4 pin of the receiver hardware module 404 (to electrically route a data bit from the D4 pin of the transmitter hardware module 402 to the D4 pin of the receiver hardware module 404), D5 pin of the transmitter hardware module 402 to D5 pin of the receiver hardware module 404 (to electrically route a data bit from the D5 pin of the transmitter hardware module 402 to the D5 pin of the receiver hardware module 404), and D6 pin of the transmitter hardware

module 402 to D6 pin of the receiver hardware module 404 (to electrically route a data bit from the D6 pin of the transmitter hardware module 402 to the D6 pin of the receiver hardware module 404).

[0071] Another map code pattern may electrically connect or couple D0 pin of the transmitter hardware module 402 to D6 pin of the receiver hardware module 404 (to electrically route a data bit from the D0 pin of the transmitter hardware module 402 to the D6 pin of the receiver hardware module 404), D1 pin of the transmitter hardware module 402 to D5 pin of the receiver hardware module 404 (to electrically route a data bit from the D1 pin of the transmitter hardware module 402 to the D5 pin of the receiver hardware module 404), D2 pin of the transmitter hardware module 402 to D4 pin of the receiver hardware module 404 (to electrically route a data bit from the D2 pin of the transmitter hardware module 402 to the D4 pin of the receiver hardware module 404), D3 pin of the transmitter hardware module 402 to D3 pin of the receiver hardware module 404 (to electrically route a data bit from the D3 pin of the transmitter hardware module 402 to the D3 pin of the receiver hardware module 404), D4 pin of the transmitter hardware module 402 to D2 pin of the receiver hardware module 404 (to electrically route a data bit from the D4 pin of the transmitter hardware module 402 to the D2 pin of the receiver hardware module 404), D5 pin of the transmitter hardware module 402 to D1 pin of the receiver hardware module 404 (to electrically route a data bit from the D5 pin of the transmitter hardware module 402 to the D1 pin of the receiver hardware module 404), and D6 pin of the transmitter hardware module 402 to D0 pin of the receiver hardware module 404 (to electrically route a data bit from the D6 pin of the transmitter hardware module 402 to the D0 pin of the receiver hardware module 404).

[0072] Other map code patterns may electrically connect the pins of the transmitter hardware module 402 to the pins of receiver hardware module 404 in various other combinations. The possible number of unique map pattern codes may be 5040 (factorial of 7). In various

embodiments, it may be possible to transmit any predetermined number of bits along the 7 data lines connecting the data pins of the transmitter hardware module 402 and the data pins of the receiver hardware module 404. The possible number of map pattern codes may still be 5040. In yet various other embodiments, it may be possible to transmit the predetermined number of bits along a number of data lines equal to the predetermined number of data bits. For instance, 6 data lines may be used for parallel transmission of 6 data bits. The 2 remaining pins of the transmitter hardware module 402 may then be coupled to the pulse detection module, and the corresponding 2 pins of the receiver hardware module 404 may be disabled. The number of permutations possible may then be 720 (factorial of 6).

[0073] As shown in FIG. 4, the hardware supervisory module 408 may be electrically connected or coupled to the switch matrix 422. More specifically, the hardware supervisory module 408 may be electrically connected or coupled to a switch logic of the switch matrix 422. During operation, the hardware supervisory module 408 may send a scrambling sequence to the switch matrix 422. The scrambling sequence may be a sequence of map pattern code sent to the switch matrix module that will determine the electrical connectivity between the transmitter hardware module 402 and the receiver hardware module 404. Accordingly, the electrical connection between the transmitter hardware module 402 and the receiver hardware module 404 may continuously be changing based on the scrambling sequence. The scrambling sequence provided by the hardware supervisory module 408 may be based on the determination of the operator, according to time schedule and/or based on transmission size.

[0074] FIG. 5 is a schematic of a data link including a switch matrix 522 and a pattern detector 528 according to various embodiments. In addition to the switch matrix 522 and the pattern detector 528, the data link may also include a transmitter hardware module 502, a receiver hardware module 504, and a hardware supervisory module 508. There may also be an external transmit host (Tx host) 524 electrically connected or coupled to the transmitter

hardware module 502, and an external receive host (Rx host) 526 electrically connected or coupled to the receiver hardware module 504. The switch matrix 522 may electrically route each of the data signals (provided by pins D0 - D6 of the transmitter hardware module 502) to the corresponding pins of the receiver hardware module 504, in any combination as determined by a map pattern code. The switch matrix 522 may operate in a similar manner as the switch matrix 422 shown in FIG. 4.

[0075] In addition to the pulse detection module (not shown in FIG. 5) which is configured to detect the unauthorised transmission of excess data bits (e.g. the 8th bit), the pattern detector 528 may be arranged preceding the switch matrix 522. Data bits from the transmitter hardware module 502 may pass through the pattern detector 528 before being transmitted to the switch matrix 522. The pattern detector 528 may be a synchronised transmitter bit pattern detector. As shown in FIG. 5, the pattern detector 528 may be electrically connected or coupled to the hardware supervisory module 508. In various embodiments, the pattern detector 528 may replace or be the pulse detection module. The pattern detector 528 may be implemented using a FPGA implementation or hardware circuitry for bit pattern detection and recognition, depending on the map pattern code combination, while the pulse detection module may be implemented with hardware circuitry. The pattern detector 528 may be implemented using hardware circuitry if only 1 bit is involved in the detection, as such implementation is not complex. However, in other instances which involve pattern detection and recognition of multiple bits, implementation using FPGA may be more practical. The difference between the pulse shaping/detection module 306 in FIG. 3 and the pattern detector 528 may be the wiring circuitry (electrical wires). Various embodiments may include only the pulse detection module 306 (and not the pattern detector 528). Other embodiments may include only the pattern detector 528 (and not the pulse shaping/detection module 306). Yet various other embodiments may include both the pulse shaping/detection module 306 and the pattern detector 528. The

pulse shaping/detection module 306 and/or the pattern/detector 528 may be configured. The pattern detector 528 may recognize, or detect permitted bit patterns and activities along the data lines connected to the pins of the transmitter hardware module 502. The pattern detector 528 may be configured to detect unexpected bit patterns representing specific characters in ASCII character table along the data lines. Accordingly, the pattern detector 528 may be used for discrimination of illegal data transfer attempts.

[0076] Upon detection of unauthorized transmission or unexpected bit patterns, the detector logic of the pattern detector may transmit a detection status/alarm signal to the hardware supervisory module 508, thereby triggering the hardware supervisory module 508 for further action, e.g. to emit an alarm.

[0077] Various embodiments may operate in secured environment. Unauthorized modification to the data link and its constituent hardware modules, configuration data, software modules or firmware may potentially compromise the protection provided by the device. In order to detect for such unauthorized modification, the data link can be delivered with anti-tampering and protection features. FIG. 6 is a schematic of a data link including anti-tampering and protection features according to various embodiments. The data link may include a transmitter hardware module 602, a receiver hardware module 604, a pulse detection module 606, a hardware supervisory module 608, a data sink module 610, a data source module 612, as well as a minimal man-machine interface (MMI) 614. In addition, the data link may also include one or more mechanical tamper switches 630a-c. The one or more mechanical tamper switches 630a-c may be mechanical spring-loaded plungers or lever switches, and may each be attached to a panel of a chassis enclosing the data link. Each of the one or more mechanical tamper switches 630a-c may be mounted in such manner in which the plunger/lever of the switch is depressed when the corresponding monitored panel of the chassis is properly closed. The data link may also include a tamper detection controller (TDC) 632 coupled or electrically connected

to the one or more mechanical tamper switches 630a-c. The tamper detection controller 632 may also be coupled or electrically connected to the hardware supervisory module 608. The electrical contacts of each of the one or more mechanical tamper switches 630a-c may provide an input signal to the tamper detection controller 632 when the corresponding monitored panel has a status change, e.g. when the panel is removed, thereby releasing the plunger/lever of the switch. The tamper detection controller 632 may continuously monitor the electrical contacts of all the mechanical tamper switches 630a-c for any status change and may initiate its Tamper Protection Sequence (TPS) when a status change is detected. Upon detection of the status change, the tamper detection controller 632 may further be required to confirm that the status change is due to a tampering attempt. The Tamper Protection Sequence (TPS) is a series of actions taken by tamper detection controller 632 and hardware supervisory module 608. The first action of the sequence may be to alert the user on the confirmed tampering attempt by the tamper detection controller 632 communicating the tamper status to the hardware supervisory module 608, which would indicate on the minimal man-machine interface (MMI) 614 as a critical alarm. In order to prevent continued operation of the data link after the tampering attempt is confirmed (which may potentially compromise the data transfer and the secured end (i.e. data source module 612) of the device), the TPS may trigger the hardware supervisory module 608 to terminate all data transfer and bring the data sink module 610 and the data source module 612 to a passive standby mode of operation. Under the standby mode of operation, the data link may no longer be able to perform data transfer activities until manual user intervention to perform corrective actions.

[0078] Various embodiments may be operated in high availability (HA), i.e. paired device configuration mode. The paired device configuration mode may improve overall availability of the solution. FIG. 7 is a schematic showing a system including a pair of data links according to various embodiments. The system may include a pair of individual HA-enabled data links, i.e.

redundant data links. The first data link of the pair of data links may include a transmitter hardware module 702a, a receiver hardware module 704a, a pulse detection module 706a, a hardware supervisory module 708a, a data sink module 710a, a data source module 712a, as well as a minimal man-machine interface (MMI) 714a. The second data link of the pair of data links may include a transmitter hardware module 702b, a receiver hardware module 704b, a pulse detection module 706b, a hardware supervisory module 708b, a data sink module 710b, a data source module 712b, as well as a minimal man-machine interface (MMI) 714b. The system may have enhanced functionality that enables each device to be configured with different roles, that as Master-HA or Slave-HA. Each device may include an additional dedicated port for connecting to a partner device using a dedicated HA Communication Cable (HACC) 734. The system may include the HACC 734 electrically connecting or coupling the hardware supervisory module 708a of the first data link and the hardware supervisory module 708b of the second data link. The hardware supervisory module 708a and the hardware supervisory module 708b may play a central role in the HA operation mode. The hardware supervisory module 708a and the hardware supervisory module 708b may monitor and gather operational and health status of various submodules within a device.

[0079] The supervisory module 708a may control the operational mode of the data sink module 710a and the data source module 712a. Likewise, the supervisory module 708b may control the operational mode of the data sink module 710b and the data source module 712b. The operation mode of the data sink module 710a, 710b and the data source module 712a, 712b within a device can either be in active mode or in standby mode. An active mode device (i.e. with the corresponding data sink module and the data source module in active mode) may be able to receive data stream from external machine on the input port (IN) and convey the data stream over to the output port (OUT).

[0080] Conversely, a standby mode device (i.e. with the corresponding data sink module and the data source module in standby mode) may not be able to receive data stream from the external machine. However, the standby mode data sink module and standby data source module may be able to send periodic internet protocol (IP) probe packets to each targeted external machine or device that is connected to the input port (IN) and the output port (OUT) to determine the condition of the communication path to the respective external machine or device. The status of the communication paths may be reported to the hardware supervisory modules 708a, 708b in each device respectively and may collectively form part of the HA operation mode decision logic table.

[0081] The HACC 734 may allow a supervisory module of one device to communicate to its partner device to establish the operational status of the partner device. With information of the health status of itself and that of its partner, the supervisory module may be able to determine the HA operational mode of the device based on a decision logic table.

[0082] Various embodiments may be used for content restrictive data transfer between computer systems of critical infrastructures. Various embodiments may be used for perimeter defence of a computer system while allowing specific data or traffic to traverse. Various embodiments may be used as an intrusion detection mechanism as part of cyber honeypot setup.

[0083] By “comprising” it is meant including, but not limited to, whatever follows the word “comprising”. Thus, use of the term “comprising” indicates that the listed elements are required or mandatory, but that other elements are optional and may or may not be present.

[0084] By “consisting of” is meant including, and limited to, whatever follows the phrase “consisting of”. Thus, the phrase “consisting of” indicates that the listed elements are required or mandatory, and that no other elements may be present.

[0085] The inventions illustratively described herein may suitably be practiced in the absence of any element or elements, limitation or limitations, not specifically disclosed herein.

Thus, for example, the terms “comprising”, “including”, “containing”, etc. shall be read expansively and without limitation. Additionally, the terms and expressions employed herein have been used as terms of description and not of limitation, and there is no intention in the use of such terms and expressions of excluding any equivalents of the features shown and described or portions thereof, but it is recognized that various modifications are possible within the scope of the invention claimed. Thus, it should be understood that although the present invention has been specifically disclosed by preferred embodiments and optional features, modification and variation of the inventions embodied therein herein disclosed may be resorted to by those skilled in the art, and that such modifications and variations are considered to be within the scope of this invention.

[0086] By “about” in relation to a given numerical value, such as for temperature and period of time, it is meant to include numerical values within 10% of the specified value.

[0087] The invention has been described broadly and generically herein. Each of the narrower species and sub-generic groupings falling within the generic disclosure also form part of the invention. This includes the generic description of the invention with a proviso or negative limitation removing any subject matter from the genus, regardless of whether or not the excised material is specifically recited herein.

[0088] Other embodiments are within the following claims and non- limiting examples.

CLAIMS

1. A data link comprising:

a transmitter hardware module configured to receive a data stream, the transmitter hardware module further configured to convert units in the data stream from having a size of eight data bits to having a size of a predetermined number of data bits before transmitting the data stream in parallel transmission, the size of the predetermined number of data bits being of any whole number of 7 or less;

a receiver hardware module configured to receive the data stream from the transmitter hardware module, the receiver hardware module further configured to convert units in the data stream from having the size of the predetermined number of data bits to having the size of eight data bits;

a pulse detection module configured to detect transmission in the data stream from the transmitter hardware module of one or more units having a size beyond the predetermined number of data bits, the pulse detection module configured to emit an alarm indication signal upon detection of the one or more units having the size beyond the predetermined number of data bits;

a supervisory module configured to provide an alarm upon receiving the alarm indication signal from the pulse detection module;

a switch matrix configured to scramble units in the data stream having the size of the predetermined number of data bits during transmission from the transmitter hardware module to the receiver hardware module; and

a pattern detector configured to detect transmission in the data stream from the transmitter hardware module of the one or more units having the size beyond the predetermined number of data bits before the data stream is received by the switch matrix.

2. The data link according to claim 1,

wherein the receiver hardware module is configured to prevent from receiving one or more additional data bits in excess of the predetermined number of data bits.

3. The data link according to claim 1 or claim 2,

wherein the receiver hardware module comprises a first-in-first-out ring buffer.

4. The data link according to any one of claims 1 to 3,

wherein the transmitter hardware module comprises a first-in-first-out ring buffer.

5. The data link according to any one of claims 1 to 4,

wherein a most significant bit pin of the transmitter hardware module is electrically connected to the pulse detection module.

6. The data link according to any one of claims 1 to 5,

wherein the predetermined number of data bits is 7.

7. The data link module according to claim 1,

wherein data pins of the transmitter hardware module is mapped to data pins of the receiver hardware module using one or more map pattern codes.

8. The data link module according to claim 1,

wherein the switch matrix is electrically connected to the supervisory module.

9. A method of forming a data link, the method comprising:

forming a transmitter hardware module configured to receive a data stream, the transmitter hardware module further configured to convert units in the data stream from having a size of eight data bits to having a size of a predetermined number of data bits before transmitting the data stream in parallel transmission, the predetermined number of data bits being of any whole number of 7 or less;

forming a receiver hardware module configured to receive the data stream from the transmitter hardware module, the receiver hardware module further configured to convert units in the data stream from having the size of the predetermined number of data bits to having the size of eight data bits;

providing a pulse detection module configured to detect transmission in the data stream from the transmitter hardware module of one or more units having a size beyond the predetermined number of data bits, the pulse detection module configured to emit an alarm indication signal upon detection of the one or more units having the size beyond the predetermined number of data bits;

providing a supervisory module configured to provide an alarm upon receiving the alarm indication signal from the pulse detection module;

providing a switch matrix configured to scramble units in the data stream having the size of the predetermined number of data bits during transmission from the transmitter hardware module to the receiver hardware module; and

providing a pattern detector configured to detect transmission in the data stream from the transmitter hardware module of the one or more units having the size beyond the predetermined number of data bits before the data stream is received by the switch matrix.

10. The method according to claim 9,

wherein the receiver hardware module is configured to prevent from receiving one or more additional data bits in excess of the predetermined number of data bits.

11. The method according to claim 9 or claim 10,

wherein the receiver hardware module comprises a first-in-first-out ring buffer.

12. The method according to any one of claims 9 to 11,

wherein the transmitter hardware module comprises a first-in-first-out ring buffer.

13. The method according to any one of claims 9 to 12,

wherein a most significant bit pin of the transmitter hardware module is electrically connected to the pulse detection module.

14. The method according to any one of claims 9 to 13,

wherein the predetermined number of data bits is 7.

15. The method according to claim 9,

wherein data pins of the transmitter hardware module is mapped to data pins of the receiver hardware module using one or more map pattern codes.

16. The method according to claim 9,

wherein the switch matrix is electrically connected to the supervisory module.