US 20120069846A1

(19) **United States**

(12) **Patent Application Publication**

Edgar et al.

(10) **Pub. No.: US 2012/0069846 A1**

(43) **Pub. Date: Mar. 22, 2012**

(54) **SERIAL COMMUNICATION TAPPING AND TRANSMISSION TO ROUTABLE NETWORKS**

(75) Inventors: **Thomas W. Edgar**, Richland, WA (US); **Sean J. Zabriskie**, Burbank, WA (US); **Eric Y. Choi**, Richland, WA (US)

(73) Assignee: **BATTELLE MEMORIAL INSTITUTE**, Richland, WA (US)

(21) Appl. No.: **12/884,455**

(22) Filed: **Sep. 17, 2010**

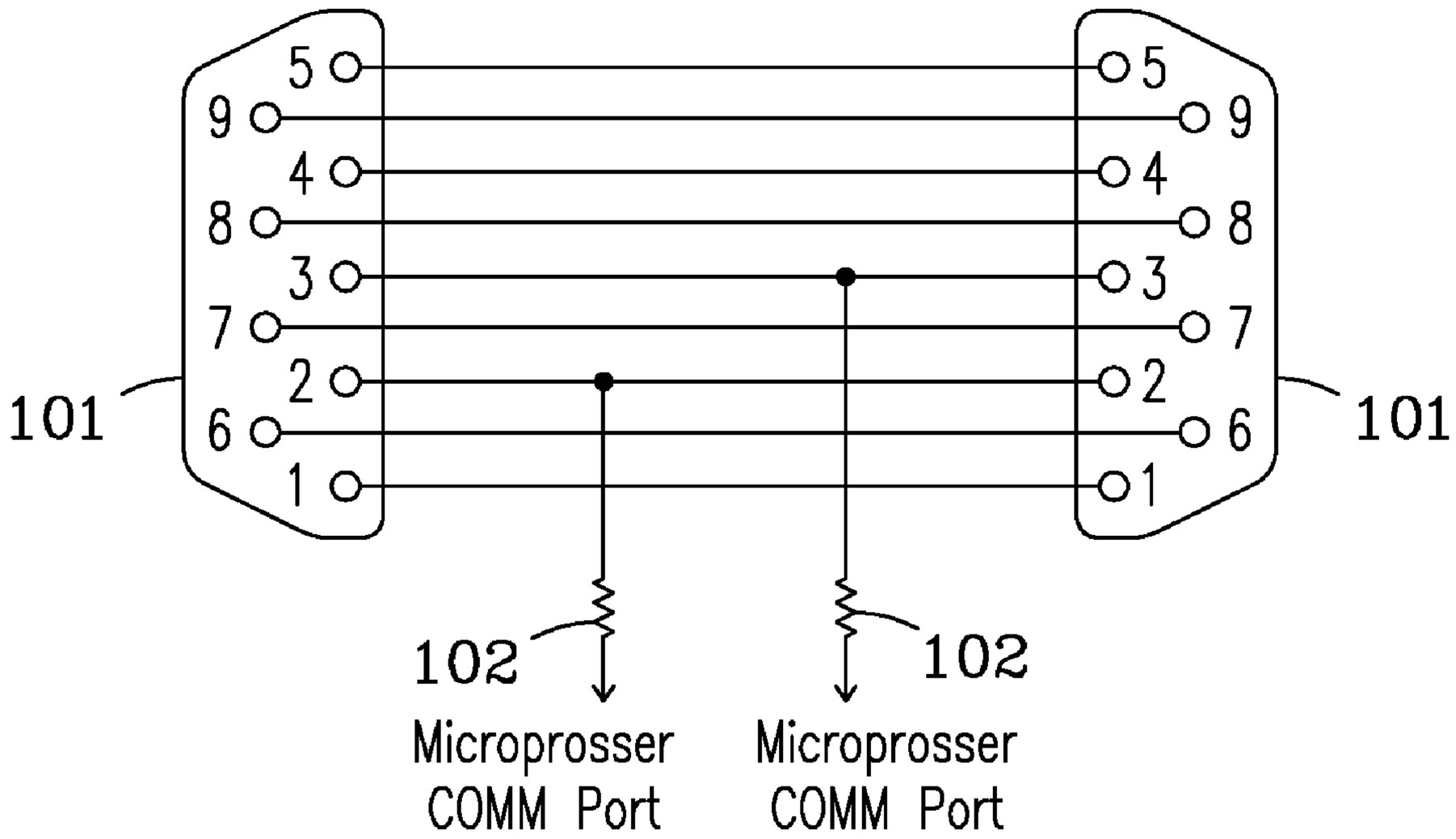
Publication Classification

(51) **Int. Cl.**
H04L 12/28 (2006.01)

(52) **U.S. Cl.** **370/392**

(57) **ABSTRACT**

Apparatuses and methods for tapping serial communications and transforming the serial data into a format appropriate for routable networks are significant for purposes of security and troubleshooting, especially in critical infrastructure networks. Communication taps should be completely passive such that any failure would not interrupt the serial communications. Furthermore, automatic determination of unspecified serial protocol frames allow general implementation across various networks, or across devices within a single network, without the need to customize for each implementation.



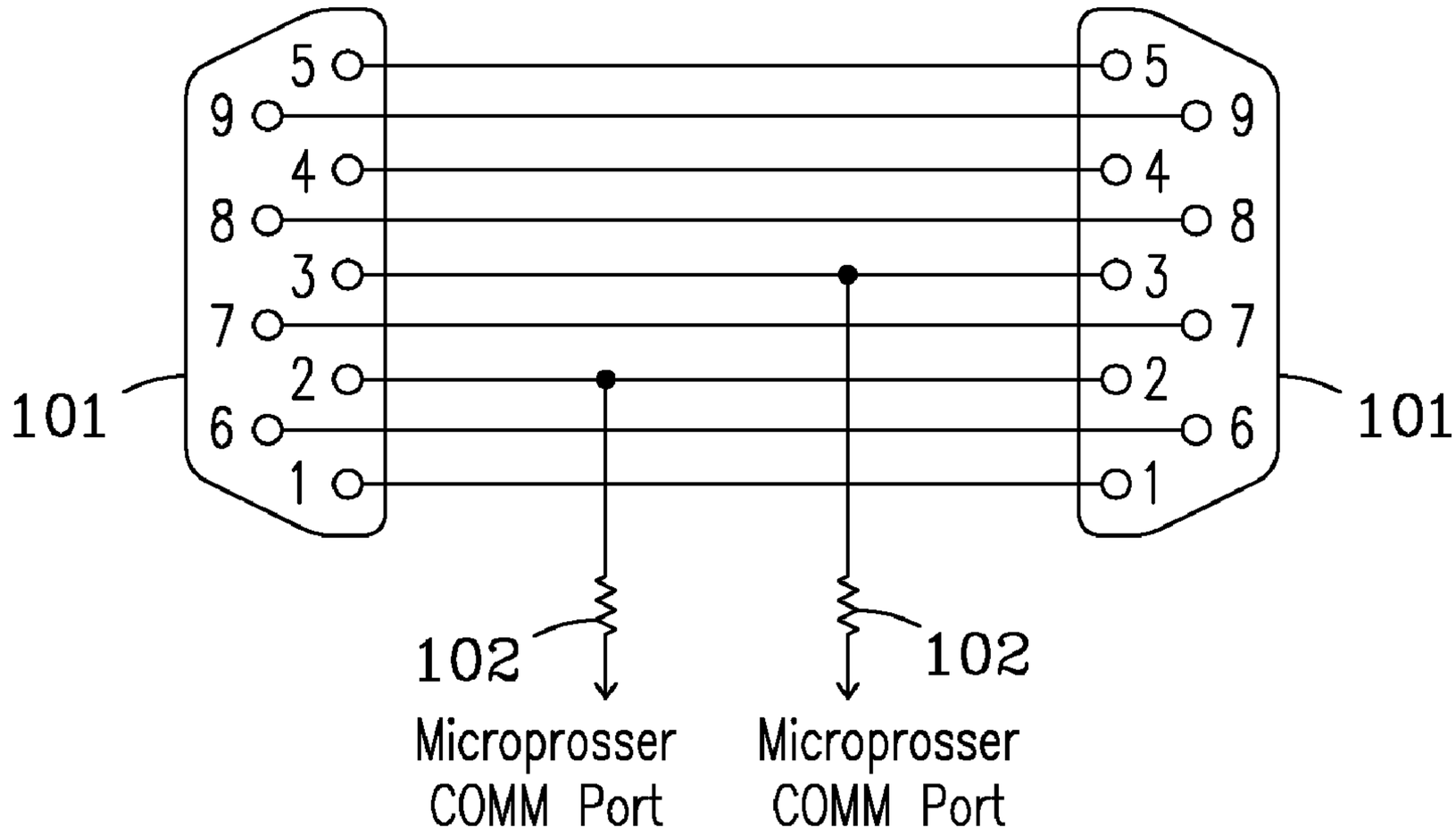

5
9
4
8
3
7
2
6
1
101
101
102
102
Microprosser
COMM Port
Microprosser
COMM Port

Fig. 1

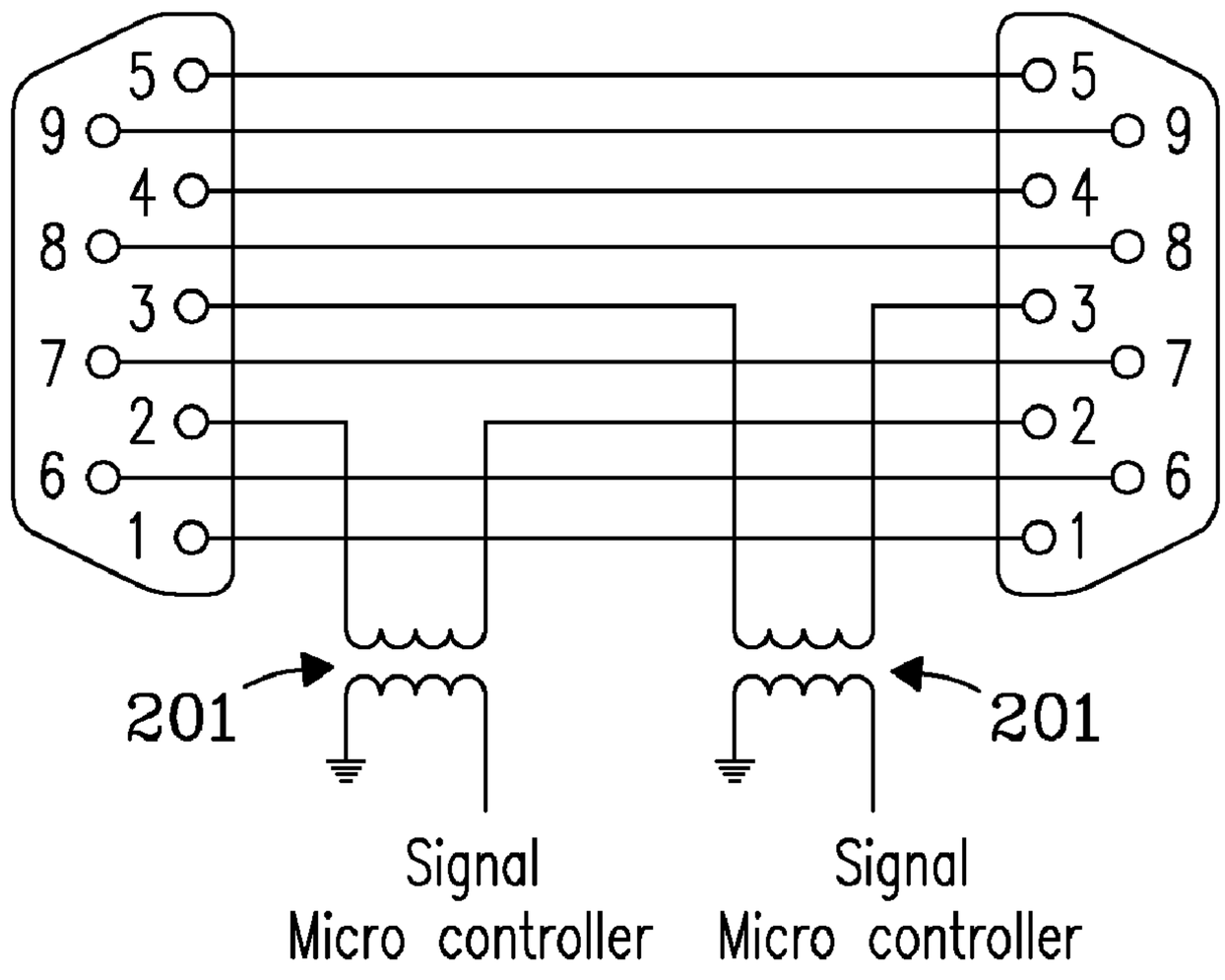

5
9
4
8
3
7
2
6
1
201
201
Signal
Micro controller
Signal
Micro controller

Fig. 2

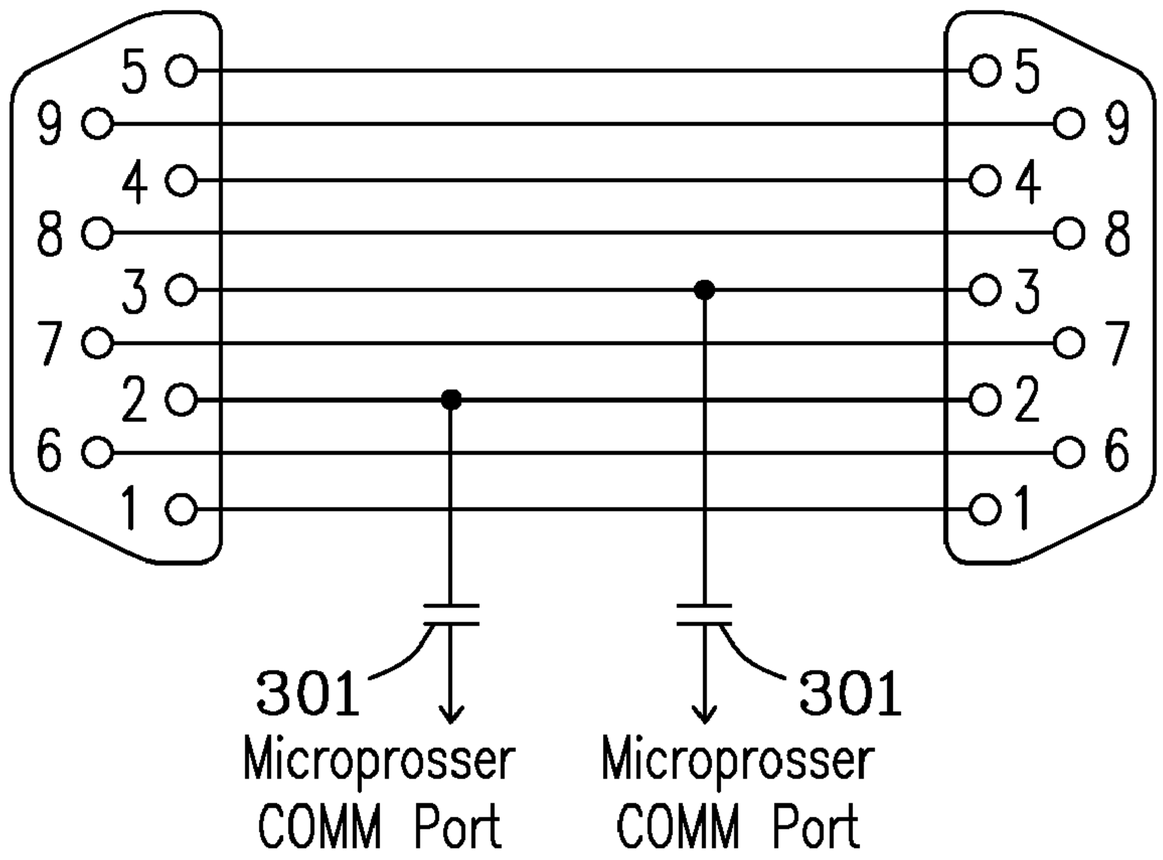

5
9
4
8
3
7
2
6
1
5
9
4
8
3
7
2
6
1
301
Microprosser
COMM Port
301
Microprosser
COMM Port

Fig. 3

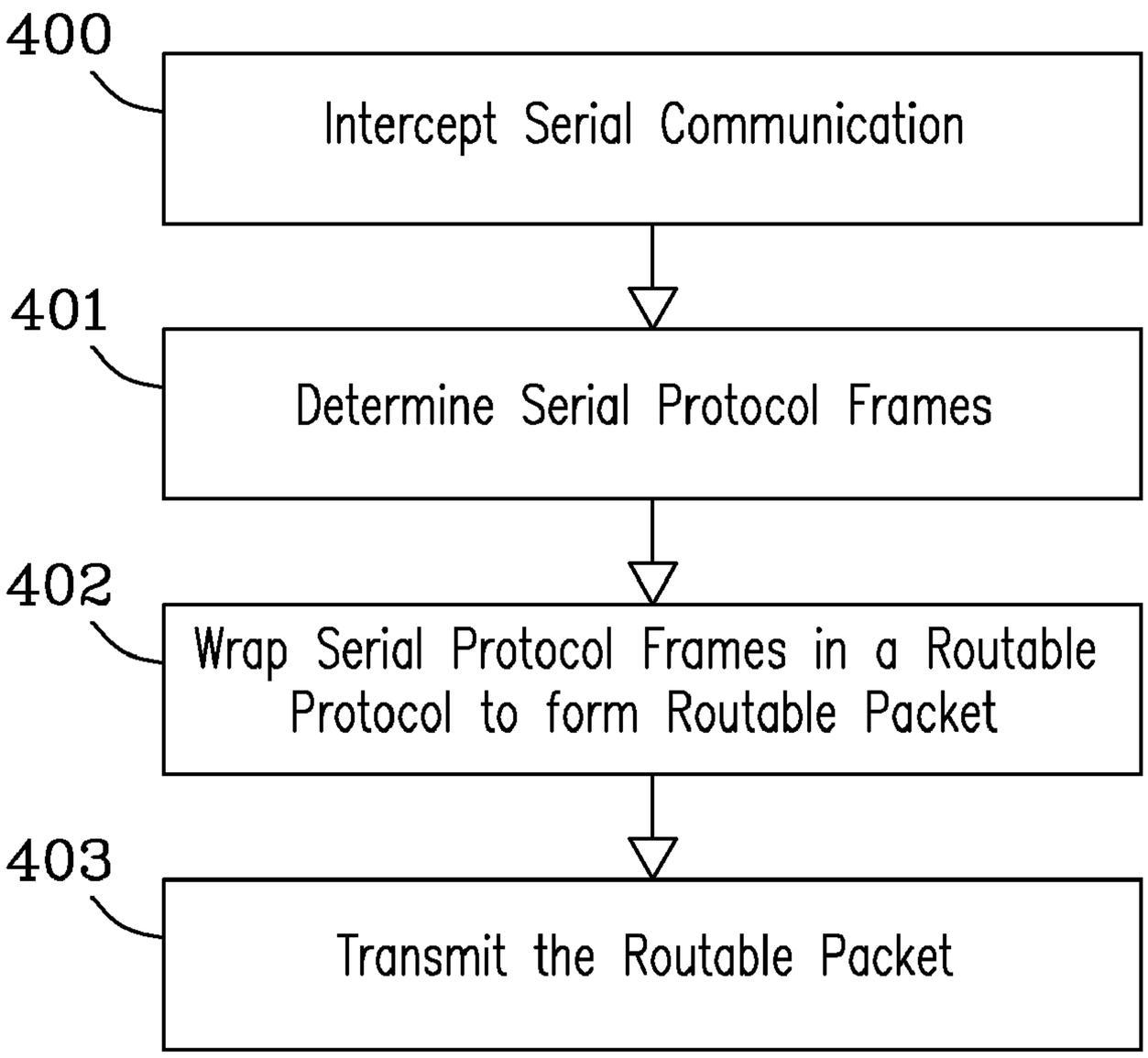

400
Intercept Serial Communication
401
Determine Serial Protocol Frames
402
Wrap Serial Protocol Frames in a Routable Protocol to form Routable Packet
403
Transmit the Routable Packet

Fig. 4

SERIAL COMMUNICATION TAPPING AND TRANSMISSION TO ROUTABLE NETWORKS

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0001] This invention was made with Government support under Contract DE-AC0576RL01830 awarded by the U.S. Department of Energy. The Government has certain rights in the invention.

BACKGROUND

[0002] Critical infrastructure networks still utilize serial communications because of the presence and reliance on legacy systems and because of the slow speed at which the industries upgrade their technology. Because of the electrical, environmental, and operational requirements, traditional IT security and troubleshooting solutions are often unsuitable in these critical systems. For example, many of the legacy devices in critical infrastructure networks cannot support the relatively high computational burden of traditional security and troubleshooting solutions. Furthermore, the security and troubleshooting system cannot introduce any new points of failure in the network. In order to secure these critical infrastructure networks, there is a need for systems and methods of sending serial traffic onto a routable network, where it could be centrally monitored, without adding computational overhead or new points of failure to critical infrastructure networks.

SUMMARY

[0003] The present invention includes apparatuses and methods for tapping serial communications and transforming the serial data into a format appropriate for routable networks. The serial communications tap is completely passive such that any failure would not interrupt the serial communications. Furthermore, embodiments of the present invention adapt automatically and operate without foreknowledge of the serial protocol frames (i.e., the serial protocol frames are unspecified. Therefore, the embodiments can be easily implemented across various networks without the need to customize for each implementation.

[0004] In one embodiment, apparatuses for passively tapping serial communications comprise passive, serial-communications, interception circuitry that includes at least one serial communications pass-through and a processor. Each serial communications pass-through is connected to the processor and is interfaced to a serial communication cable through which the serial communications are transmitted. The processor executes programming to determine serial protocol frames according to characteristics of the serial communications, to wrap the serial protocol frames in a routable protocol, thereby forming a routable packet, and to transmit the routable packets to one or more routable addresses through an interface connecting the processor to a routable network. Preferably, the routable network can be is based on internet protocol (IP) and the one or more routable addresses arc IP addresses.

[0005] The serial communications have serial protocol frames that are unspecified to the apparatus. Preferably, the unspecified serial protocol frames are based on a process control serial protocol. Examples of process control serial protocols include, but are not limited to, distributed network protocol 3 (DNP3) and Modbus.

[0006] The pass-through can comprise a pair of serial ports directly connected to the serial communication cable. In such instances, the interception circuitry must have an impedance greater than that of the serial communication cable. The pass-through can alternatively comprise an inductive coupling. Further still, the pass-through can comprise a capacitive coupling to intercept the serial communications by means of capacitance.

[0007] In some embodiments, the characteristics of serial communications include timing-based signals. In such instances, the processing device can execute further programming to associate timing gaps between the timing-based signals with frame edges that define the serial protocol frames.

[0008] In other embodiments, the characteristics of serial communications include frame synchronization delimiters and length fields and the processing device executes further programming to define the beginning and the length of serial protocol frames according to the frame synchronization delimiters and length fields, respectively.

[0009] In still other embodiments, the characteristics of serial communications include frame synchronization delimiters and frame end delimiters and the processing device executes further programming to define the beginning and the end of serial protocol frames according to the frame synchronization delimiters and frame end delimiters, respectively.

[0010] The characteristics of serial communications can alternatively include time variance between signals and the processing device executes further programming to identify a baseline time gap in the signals and to define statistically significant deviations from the baseline time gap as the beginnings and the ends of serial protocol frames.

[0011] Alternatively, the characteristics of serial communications can include byte frequency and the processing device executes further programming to identify statistically significant occurrences of byte frequency patterns and to define the statistically significant occurrences with the beginnings and the ends of serial protocol frames.

[0012] Still other characteristics of serial communications can include byte frequency as well as time variance between signals and the processing device executes further programming to identify statistically significant occurrences of byte frequency patterns, to identify a baseline time gap in the signals, and to define statistically significant deviations from the baseline time gap combined with statistically significant occurrences of byte patterns as the beginnings and the ends of the serial protocol frames.

[0013] In preferred embodiments, the programming executed by the processing device is stored in storage circuitry and the pass-through, the processor, the storage circuitry, and the interface are assembled as an embedded system. As used herein, an embedded system refers to a device that runs firmware, provides a few dedicated functions, and has real-time computing constraints. It is dedicated to a particular task. By contrast, a general-purpose computer is designed to be flexible and to meet a wide range of end user needs.

[0014] Another embodiment of the present invention includes methods to passively tap serial communications, which have serial protocol frames that arc unspecified, transmitted through a serial communication cable between a source and a receiver. The method, which is executed by a processor, includes passively intercepting the serial communications through a serial communications pass-through connected to the processor and to the serial communication cable

and determining serial protocol frames according to characteristics of the serial communications. Routable packets can then be formed by wrapping the serial protocol frames in a routable protocol and transmitting the routable packets to one or more routable addresses through an interface connecting the processor to a routable network.

[0015] The purpose of the foregoing abstract is to enable the United States Patent and Trademark Office and the public generally, especially the scientists, engineers, and practitioners in the art who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The abstract is neither intended to define the invention of the application, which is measured by the claims, nor is it intended to be limiting as to the scope of the invention in any way.

[0016] Various advantages and novel features of the present invention are described herein and will become further readily apparent to those skilled in this art from the following detailed description. In the preceding and following descriptions, the various embodiments, including the preferred embodiments, have been shown and described. Included herein is a description of the best mode contemplated for carrying out the invention. As will be realized, the invention is capable of modification in various respects without departing from the invention. Accordingly, the drawings and description of the preferred embodiments set forth hereafter are to be regarded as illustrative in nature, and not as restrictive.

DESCRIPTION OF DRAWINGS

[0017] Embodiments of the invention are described below with reference to the following accompanying drawings.

[0018] FIG. **1** is a diagram depicting one embodiment of the present invention in which the pass-through includes a pair of serial ports.

[0019] FIG. **2** is a diagram depicting one embodiment of the present invention in which the pass-through includes an inductive coupling.

[0020] FIG. **3** is a diagram depicting one embodiment of the present invention in which the pass-through includes a capacitive coupling.

[0021] FIG. **4** is a block diagram depicting methods according to embodiments of the present invention.

DETAILED DESCRIPTION

[0022] The following description includes the preferred best mode of one embodiment of the present invention. It will be clear from this description of the invention that the invention is not limited to these illustrated embodiments but that the invention also includes a variety of modifications and embodiments thereto. Therefore the present description should be seen as illustrative and not limiting. While the invention is susceptible of various modifications and alternative constructions, it should be understood, that there is no intention to limit the invention to the specific form disclosed, but, on the contrary, the invention is to cover all modifications, alternative constructions, and equivalents falling within the spirit and scope of the invention as defined in the claims.

[0023] FIGS. **1-4** show a variety of embodiments and aspects of the present invention. Referring first to FIG. **1** a diagram depicts the pass-through interfacing the serial communication cable and the interception circuitry. In this embodiment, the pass through comprises a pair of serial ports **101** directly connected to the serial communication cable. Accordingly, the apparatus is connected in line with the serial communication cable. In such instances, the interception circuitry must have an impedance greater than that of the serial communication cable. The impedance in the interception circuitry can be increased using resistors **102** and/or including components having relatively large impedances. The large impedance in the interception circuitry ensures that the serial communications will still transmit through the serial communications cable in the event that the apparatus fails. In preferred embodiments, the impedance of the interception circuitry is at least 10% higher than that of the serial communication cable.

[0024] Referring to FIG. **2**, the diagram depicts the pass through as an inductive coupling. The inductive coupling can capture the leading and trailing edges of a bit, which are then amplified by components in the interception circuitry, by electromagnetic induction which is the induction of a voltage in one wire based on the change in current flow of through a primary wire. In a particular embodiment, the inductive coupling utilizes a transformer **201**. A coil of wire of the serial signal can be wound on the primary side of the transformer while a passive capture signal can be wound around the secondary side of the transformer. The coupling can be increased by a transformer so the magnetic field of the primary coil will pass through to the secondary coil such that a change in current flow through one coil will induce a voltage in the other.

[0025] Referring to FIG. **3**, the diagram depicts the pass through as a capacitive coupling. The capacitive coupling can comprise a capacitor **301** in series between the serial communications cable and the interception circuitry. In some embodiments, a DC bias can be reintroduced in the interception circuitry to recreate the original serial communication.

[0026] FIG. **4** is a block diagram depicting the steps executed by a processor to tap one or more serial communications and transmit the communications to a centralized location for purposes of security and troubleshooting. Serial communications that have been passively intercepted **400** by a serial communications pass-through connected to the processor can have a serial protocol frame that is unspecified. Accordingly, the processor first determines **401** the serial protocol frames according to characteristics of the serial communications. Once the serial protocol frames are known, routable packets are formed **402** by wrapping the serial protocol frames in a routable protocol. The processor can then transmit **403** the routable packets to one or more routable addresses through an interface connecting the processor to a routable network.

[0027] As described elsewhere herein, embodiments of the present invention can automatically determine unspecified serial protocol frames, thereby enabling implementation and operation without foreknowledge of the protocol frames. In some instances, the determination is based on statistically significant deviations from a baseline time gap in the signals of the serial communications and/or statistically significant byte frequency patterns.

[0028] As used herein, a baseline time gap refers to the mean value of all previously processed signal time gaps and the associated standard deviation range. Statistically significant deviations from the baseline time gap can be determined by time gaps that fall outside a standard deviation range from the mean.

[0029] As used herein, byte frequency can refer to frequencies of occurrence for patterns of 2 or more byte sequences that occur in the serial traffic. Statistically significant byte frequency patterns can refer to byte frequencies that have a higher frequency percentage of occurrence relative to other byte frequencies. They can be determined by continuously calculating the frequencies of occurence for patterns in the data. Those byte frequencies with the highest frequency of occurrence can be designated as statistically significant according to predetermined criteria.

[0030] While a number of embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that many changes and modifications may be made without departing from the invention in its broader aspects. The appended claims, therefore, are intended to cover all such changes and modifications as they fall within the true spirit and scope of the invention.

We claim:

1. An apparatus to passively tap serial communications having serial protocol frames that are unspecified to the apparatus, the apparatus characterized by:

Passive, serial-communications, interception circuitry comprising at least one serial communications pass-through and a processor, each serial communications pass-through connected to the processor and interfaced to a serial communication cable through which the serial communications are transmitted;

The processor executing programming to determine serial protocol frames according to characteristics of the serial communications, to wrap the serial protocol frames in a routable protocol, thereby forming a routable packet, and to transmit the routable packets to one or more routable addresses through an interface connecting the processor to a routable network.

2. The apparatus of claim **1**, wherein the pass-through comprises a pair of serial ports directly connected to the serial communication cable and wherein the passive, serial-communications, interception circuitry has an impedance greater than that of the serial communication cable.

3. The apparatus of claim **1**, wherein the pass-through comprises an inductive coupling.

4. The apparatus of claim **1**, wherein the pass-through comprises a capacitive coupling

5. The apparatus of claim **1**, wherein the characteristics of serial communications comprise timing-based signals, and the processing device executes further programming to associate timing gaps between the timing-based signals with frame edges that define the serial protocol frames.

6. The apparatus of claim **1**, wherein the characteristics of serial communications comprise frame synchronization delimiters and length fields and the processing device executes further programming to define the beginning and the length of serial protocol frames according to the frame synchronization delimiters and length fields, respectively.

7. The apparatus of claim **1**, wherein the characteristics of serial communications comprise frame synchronization delimiters and frame end delimiters and the processing device executes further programming to define the beginning and the end of serial protocol frames according to the frame synchronization delimiters and frame end delimiters, respectively.

8. The apparatus of claim **1**, wherein the characteristics of serial communications comprise time variance between signals and the processing device executes further programming to identify a baseline time gap in the signals and to define statistically significant deviations from the baseline time gap as the beginnings and the ends of serial protocol frames.

9. The apparatus of claim **1**, wherein the characteristics of serial communications comprise byte frequency and the processing device executes further programming to identify statistically significant occurrences of byte frequency patterns and to define the statistically significant occurrences with the beginnings and the ends of serial protocol frames.

10. The apparatus of claim **1**, wherein the characteristics of serial communications comprise byte frequency as well as time variance between signals and the processing device executes further programming to identify statistically significant occurrences of byte frequency patterns, to identify a baseline time gap in the signals, and to define statistically significant deviations from the baseline time gap combined with statistically significant occurrences of byte patterns as the beginnings and the ends of the serial protocol frames.

11. The apparatus of claim **1**, wherein the unspecified serial protocol frames are based on a process control serial protocol.

12. The apparatus of claim **1**, further comprising storage circuitry storing the programming, wherein the pass-through, the processor, the storage circuitry, and the interface are assembled as an embedded system.

13. A method to passively tap serial communications, which have serial protocol frames that are unspecified, transmitted through a serial communication cable between a source and a receiver, the method executed by a processor and characterized by the steps of:

Passively intercepting the serial communications through a serial communications pass-through connected to the processor and to the serial communication cable;

Determining serial protocol frames according to characteristics of the serial communications;

Forming routable packets by wrapping the serial protocol frames in a routable protocol; and

Transmitting the routable packets to one or more routable addresses through an interface connecting the processor to a routable network.

14. The method of claim **13**, wherein the characteristics of serial communications comprise timing-based signals, and said determining comprises associating timing gaps between the timing-based signals with frame edges that define the serial protocol frames.

15. The method of claim **13**, wherein the characteristics of serial communications comprise frame synchronization delimiters and length fields and said determining comprises defining the beginning and the length of serial protocol frames according to the frame synchronization delimiters and length fields, respectively.

16. The method of claim **13**, wherein the characteristics of serial communications comprise frame synchronization delimiters and frame end delimiters and said determining comprises defining the beginning and the end of serial protocol frames according to the frame synchronization delimiters and frame end delimiters, respectively.

17. The method of claim **13**, wherein the characteristics of serial communications comprise time variance between signals and said determining comprises to identifying a baseline time gap in the signals and defining statistically significant deviations from the baseline time gap as the beginnings and the ends of serial protocol frames.

18. The method of claim **13**, wherein the characteristics of serial communications comprise byte frequency and said determining comprises identifying statistically significant

occurrences of byte frequency patterns and defining the occurrences of byte frequency patterns with the beginnings and the ends of serial protocol frames.

19. The method of claim **13**, wherein the characteristics of serial communications comprise byte frequency as well as time variance between signals and said determining comprises identifying statistically significant occurrences of byte frequency patterns, identifying a baseline time gap in the signals, and defining statistically significant deviations from the baseline time gap combined with statistically significant occurrences of byte patterns as the beginnings and the ends of the serial protocol frames.

20. The method of claim **13**, wherein the unspecified serial protocol frames are based on a process control serial protocol.

* * * * *