

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

NETWORK INTEGRITY SYSTEMS, INC.,

 Plaintiff,

 v.

 CYBERSECURE IPS LLC,

 Defendant.

Case No.: 8:25-cv-01974-TDC

**DEFENDANT CYBERSECURE IPS LLC'S ANSWER AND COUNTERCLAIMS TO
PLAINTFF NETWORK INTEGRITY SYSTEMS, INC.'S COMPLAINT**

Defendant Cybersecure IPS LLC (“CS”), by and through its undersigned counsel, hereby responds to Plaintiff Network Integrity Systems, Inc.’s (“NIS”) Complaint.

NATURE OF THE SUIT

1. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code, involving infringement of U.S. Patent No. 7,706,641 (“the ‘641 patent” or “patent-in-suit”, attached as **Exhibit 1**, in reference to the patent claim chart, attached as **Exhibit 2**, incorporated herein by reference).

ANSWER: Admitted that Plaintiff's claims purport to arise under the Patent Laws of the United States pertaining to the patent-in-suit, and that Exhibit 1 appears to be a copy of U.S. Patent No. 7,706,641. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable.

PARTIES JURISDICTION AND VENUE

2. NIS is a North Carolina corporation with a principal place of business at 1937 Tate Boulevard SE, Hickory, North Carolina 28602.

ANSWER: CS lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in this paragraph, and therefor denies them.

3. CS is a Maryland limited liability company headquartered in Herndon, Virginia.¹

ANSWER: CS admits that it is a Maryland limited liability company, but denies that it is headquartered in Herndon, Virginia. CS is headquartered in Maryland.

4. This Court has jurisdiction over this matter pursuant to 28 U.S.C. §§ 1331 and 1338(a).

ANSWER: This paragraph contains legal conclusions to which no response is required. To the extent a response is required, CS denies it has committed acts of infringement. CS admits that NIS makes allegations of patent infringement under the patent laws of the United States and that this Court has subject matter jurisdiction over patent infringement actions. CS lacks knowledge or information sufficient to form a belief as to the truth of whether NIS has standing to bring this action and therefore denies that the Court has subject matter jurisdiction over this action.

5. Personal jurisdiction exists over CS because it has its headquarters in Virginia where it also conducts regular business and engaged in infringement.

ANSWER: This paragraph contains legal conclusions to which no response is required. To the extent a response is required, CS denies it has committed acts of infringement and denies that it is headquartered in Virginia. For purposes of this action, CS does not contest jurisdiction in Maryland.

6. Venue is proper under 28 U.S.C. § 1400(b) in this Division and District where CS has committed acts of infringement and has a regular and established place of business.

¹ <https://www.linkedin.com/company/cybersecure-ips/about/>.

ANSWER: This paragraph contains legal conclusions to which no response is required. To the extent a response is required, CS denies it has committed acts of infringement and denies that it is headquartered in Virginia. For purposes of this action, CS does not contest venue in the District of Maryland.

FACTUAL BACKGROUND

7. NIS owns patents in the field of optical fiber security and is a cyber-security business and leading provider of optical sensing technology for cyber and physical security applications specializing in optical fiber monitoring to enhance network infrastructure security across various sectors.

ANSWER: Admitted that NIS is listed as the assignee on the face of the '641 patent which is titled "Monitoring Individual Fibers of an Optical Cable for Intrusion" (Dkt. 1-2) and that NIS is cyber-security business. CS lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in this paragraph, and therefor denies them.

8. CS is also a cyber-security business that specializes in the design and development of prepackaged computer software and fiber-optic-based solutions for network infrastructure security.

ANSWER: Admitted that CS is in the cyber-security industry. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

9. The parties have a long history of working together. Effective October 1, 2015, the parties entered into an Exclusive Strategic Relationship Agreement ("ESR Agreement") related to integration and joint sale of technology solutions to customers.

ANSWER: Admitted that the parties have worked together. Admitted that there was an Exclusive Strategic Relationship Agreement and the document speaks for itself. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

10. Effective June 23, 2023, the parties terminated the ESR Agreement and entered into a Memorandum of Understanding (“MOU”) to continue working together to service customers after the termination of the ESR Agreement. This Complaint is limited to CS’s infringing activity after the termination of the ESR Agreement on June 23, 2023.

ANSWER: Admitted that the ESR Agreement was terminated on or around June 23, 2023, and that a memorandum of understanding was entered. Admitted that the Complaint alleges infringement limited to activity after June 23, 2023. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

11. Effective September 5, 2024, the parties entered into a “Settlement Agreement” (the “Settlement Agreement”) whereby they resolved various MOU disputes, including claims by NIS that CS improperly hired current and former NIS employees who were subject to non- competition and/or non-solicitation clauses in their employment contracts with NIS, and that CS disclosed and/or misused confidential NIS information.

ANSWER: Admitted that the parties entered a Settlement Agreement and the document speaks for itself. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

12. The ‘641 patent is entitled “MONITORING INDIVIDUAL FIBERS OF AN OPTICAL CABLE FOR INTRUSION” and was duly and legally issued by the United States Patent and Trademark Office on April 27, 2010.

ANSWER: Admitted that NIS is listed as the assignee on the face of the ‘641 patent which is titled “Monitoring Individual Fibers of an Optical Cable for Intrusion” which was issued April

27, 2010. (Dkt. 1-2.) To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

13. The '641 patent includes method claims related to detecting movement of optical fibers of an optical fiber cable and generating an alarm indicating the movement.

ANSWER: Admitted that the '641 patent includes method claims, and the document speaks for itself. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

14. The '641 patent is valid and enforceable.

ANSWER: Denied.

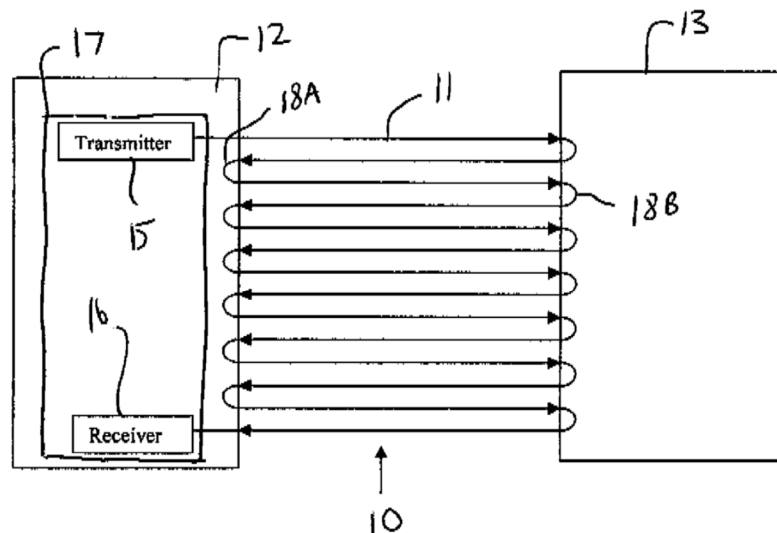
15. NIS is the exclusive owner of all right, title, and interest in the '641 patent. NIS practices the technology disclosed in the patents and has the right to bring this action to recover damages for any current or past infringement of these patents. CS does not have a license to practice the inventions claimed in the '641 patent.

ANSWER: Admitted that NIS is listed as the assignee on the face of the '641 patent. (Dkt. 1-2.) To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

16. The '641 patent is directed to a system and method for detecting movement of optical fibers for the purpose of intrusion detection. The claims of the '641 patent are method claims that include method steps such as injecting light into fibers to be monitored and receiving light signals that have been transmitted along the fibers being monitored. At least claims 1 and 12 of the '641 patent read on a point-to-multipoint network layout where the number of fibers being monitored is greater than the number of light sources and greater than the number of sensor arrangements that detect the light being transmitted through the monitored fibers.

ANSWER: Admitted that the '641 patent includes method claims, and the document speaks for itself. Admitted that the '641 patent includes claims that include steps such as “injecting light from the at least one source into one end of each of the fibers to be monitored” (Dkt. 1-2, claim 1) and “providing a plurality of optical fiber cables arranged in a hub-and-spoke arrangement where each optical fiber cable extends from a main unit at a central location to one of a plurality of remote units.” (Dkt. 1-2, claim 12). To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

17. Fig. 1 of the '641 patent (set forth below) depicts an exemplary point-to-multipoint network layout.



ANSWER: Admitted that the image provided in this paragraph appears to be a copy of Figure 1 from the '641 patent. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

18. NIS manufactures and sells two products that are relevant to the '641 patent. The “Interceptor” and “Vanguard,” which are both interrogator type devices that provide light to optical fibers being monitored and receive light signals from those fibers. The received light signals are

analyzed for abnormalities that indicate whether there is an intrusion into the cable carrying the fiber or the fiber itself. The analysis of the light signals may be performed by software in the interrogator device or by software on a separate computer providing a user interface, or both. Both the Interceptor and Vanguard devices are capable of protecting up to 8-separate zones or cable paths distributed throughout the building by monitoring strands of fibers within optical cables making up the network infrastructure.

ANSWER: Admitted that NIS has sold the “Interceptor” and “Vanguard” products. CS lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in this paragraph, and therefor denies them.

19. A system operating with a NIS Interceptor or Vanguard device detects and reports tampering or intrusion attempts for the purposes of data theft (tapping) or denial of service attacks. The Interceptor and Vanguard devices are designed to be used in a detection system and method that utilizes a point-to-multipoint network layout.

ANSWER: Admitted that NIS has sold the Interceptor and Vanguard devices advertised for detecting and reporting tampering or intrusion attempts. CS lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in this paragraph, and therefor denies them.

20. On information or belief, CS has had knowledge of the ‘641 patent at least since the parties entered into the ESR Agreement in 2015. CS personnel have frequently visited NIS facilities where a plaque showing the cover page of the ‘641 patent is displayed. In addition, CS personnel attended training at NIS facilities where the NIS innovations (e.g., network intrusion monitoring using point-to-multipoint network layout) covered by the ‘641 patent were described as “patented.” NIS and CS created and distributed co-branded marketing materials that referenced

NIS’ “patented hub and spoke technology.” Two examples of these marketing materials are attached as **Exhibit 3**. In addition, on information and belief, CS conducted a review of NIS’s patent portfolio (including the ‘641 patent) in 2023 when the ESR Agreement was terminated.

ANSWER: Admitted that Exhibit 3 appears to be copies of marketing materials. Admitted that CS employees have visited NIS facilities. Admitted that CS has reviewed NIS patents. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

21. Until the parties severed their relationship in 2024, CS partnered with NIS to offer both CS and NIS products to their joint customers. These joint customers included both data center customers who purchased and installed numerous Vanguard devices and practiced the claims of the ‘641 patent, and customers who operated Protective Distribution Systems (PDS) and purchased and installed numerous Interceptor devices. One of the parties’ data center customers (the “Primary Customer”) was responsible for the vast majority of the parties’ data center related business.

ANSWER: Admitted that during the parties’ working relationship, CS partnered with NIS and offered products, including the Interceptor and Vanguard products, to customers jointly, including data center customers and customers who operated PDS. CS lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in this paragraph, and therefor denies them.

22. During the approximately nine years that the parties co-marketed products, CS did not have a product that competed with the NIS Interceptor and Vanguard devices. CS is now offering for sale and selling a product that competes with the NIS Interceptor and Vanguard devices. CS has incorporated the functionality of the Interceptor and Vanguard devices into a newly marketed device named “Opti-Guard.” CS marketing materials for the Opti-Guard device are

attached as **Exhibits 4 and 5**. CS touts its Opti-Guard device to customers as a device that can “replace the [NIS] Interceptor.” Ex. 5 at p. 2.

ANSWER: Admitted that Exhibits 4 and 5 appear to be copies of CS’s marketing materials, and the documents speak for themselves. Admitted that CS did not have a product that competed with the Interceptor and Vanguard devices when the parties co-marketed products. Admitted that Opti-Guard is a product developed by CS. Denied that CS incorporated the functionality of the Interceptor and Vanguard devices into the Opti-Guard product. CS lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in this paragraph, and therefor denies them.

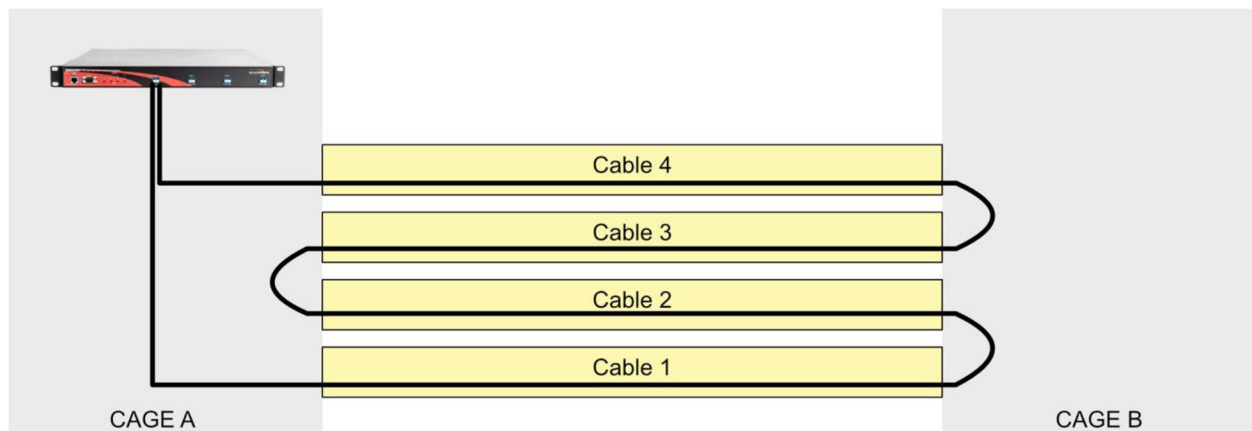
23. As described further below, CS makes, uses, sells, and/or offers for sale products and services that infringe the ‘641 patent. These products and services include intrusion systems and methods that include both software and hardware devices. In particular, CS makes, uses, sells, and/or offers for sale at least the following products and services that infringe the ‘641 patent (“Accused Products and Services”):

- a. Detection System and Method used in Data Centers;
- b. Detection System and Method used in Protected Distribution Systems (PDS); and
- c. Detection System and Method used in Manhole, Lockbox, and other Fiber Bragg Grating (FBG) Intrusion Monitoring.

ANSWER: Denied.

24. Until its relationship with NIS ended in 2024, CS partnered with NIS to pair its software with the NIS Vanguard device for use in data centers for monitoring movement of optical fibers. CS now offers an alternative to the NIS Vanguard device, and offers for sale, sells, and has sold its software and hardware for use in a system and method for monitoring intrusion of OSP/ISP

Pathways and Conduits for various data centers having a point-to-multipoint network layout. An exemplary layout of a commercial point-to-multipoint network layout is set forth below:



ANSWER: Admitted that the parties previously worked together in selling products and services, including software and the Vanguard device. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. CS lacks knowledge or information sufficient to form a belief as to the truth of the allegations regarding the “exemplary layout” and various data centers having a “point-to-multipoint” network layout, and therefor denies them. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

25. Use of these CS products in a system and method for monitoring intrusion of OSP/ISP Pathways and Conduits for use in an intrusion detection system with a point-to-multipoint network layout infringes at least claims 1 and 12 of the ‘641 patent, either literally or under the doctrine of equivalents, because such a detection system including CS products performs all of the steps required in these claims, as set forth in detail in Exhibit 2.

ANSWER: Denied.

26. In particular, CS has offered for sale and sold its products for use in a system and method for monitoring intrusion of OSP/ISP Pathways and Conduits for use in data centers owned

by the Primary Customer that employ an intrusion detection system with point-to-multipoint network layout. The CS products and services for sale and sold for use in data centers are described on the CS website. (“Realize True Data Center Security with CyberSecure IPS”, attached as **Exhibit 6.**)

ANSWER: Admitted that Exhibit 6 appears to be a copy of a screen capture of CS’s website, and the website speaks for itself. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. CS lacks knowledge or information sufficient to form a belief as to the truth of the allegations regarding the “point-to-multipoint” network layout, and therefor denies them. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

27. For certain Primary Customer data centers, CS has offered for sale and sold its products to replace existing NIS Vanguard device already in use in the point-to-multipoint network layouts in the Primary Customer data centers. In particular, NIS began providing its Vanguard devices to the Primary Customer in 2017 for use in data centers that include a point-to-multipoint network layout and are located in this Division and District. The Primary Customer has a life cycle replacement policy that requires it to replace electronic devices at least every seven years. CS has offered for sale and sold its OptiGuard device to replace Vanguard devices located in this Division and District, in response to the Primary Customer acting according to its life cycle replacement policy. The CS system and method that includes the OptiGuard and is being offered for sale and sold for use in the Primary Customer data centers with a point-to-multipoint network layout infringes at least claims 1 and 12 of the ‘641 patent.

ANSWER: Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. CS lacks knowledge or information sufficient to form

a belief as to the truth of the allegations regarding the “point-to-multipoint” network layout and the alleged life cycle replacement policy, and therefor denies them. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

28. CS, with knowledge of the ‘641 patent and knowledge that the CS intrusion detection system and method used in the point-to-multipoint network layout at Primary Customer data centers infringes the ‘641 patent, provides assistance and instruction in connection with the installation and use of the CS intrusion detection system at the Primary Customer data centers and the knowhow to use the CS intrusion detection system in an infringing manner.

ANSWER: Denied.

29. CS, with knowledge of the ‘641 patent and knowledge that the CS intrusion detection system and method used in the point-to-multipoint network layout at Primary Customer data centers infringes the ‘641 patent, directs its salespeople and technical personnel to conduct troubleshooting and testing on the CS intrusion detection system used in the point-to-multipoint network layout at Primary Customer data centers.

ANSWER: Denied.

30. The infringing CS intrusion detection system and method is designed for use with the point-to-multipoint network layout at Primary Customer data centers in a manner that infringes the ‘641 patent.

ANSWER: Denied.

31. Until its relationship with NIS ended in 2024, CS partnered with NIS to pair its software with the NIS Interceptor device for use with a PDS for monitoring movement of optical fibers. CS now offers an alternative to the NIS Interceptor device – the Opti-Guard device -- and

offers for sale, sells, and has sold its own products for use in a system and method for monitoring intrusion of optical fibers in a PDS.

ANSWER: Admitted that the parties previously worked together in selling products and services, including software and the Interceptor device. Admitted that CS sells the Opti-Guard device and that CS sells products for use in a PDS. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

32. The CS products and services for sale for use with a PDS are described on the CS website. (“Alarmed Carrier PDS Solutions For Military and Government,” attached as **Exhibit 7**.) CS has offered for sale and sold its products for use in a system and method for monitoring intrusion of the PDS used in a secure government facility located in the District of Columbia, Maryland and Virginia region (the “DMV Facility”).

ANSWER: Admitted that Exhibit 7 appears to be a copy of a screen capture of CS’s website, and the website speaks for itself. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

33. The DMV Facility is well known to CS because CS knew it was competing with NIS to provide products and services to monitor PDS intrusion at the DMV Facility. CS and NIS were working with the same integration company that was offering CS and NIS products as alternative solutions to the DMV Facility. The cables used at the DMV Facility include air blown optical fibers which, although not unique, distinguish the DMV Facility from other government facilities that employ a PDS. The CS products and services offered for sale and sold for use at the DMV Facility include an intrusion detection system for a PDS with a point-to-multipoint network

layout. Use of the CS products in a system and method for monitoring intrusion of the PDS used at the DMV Facility infringes at least claims 1 and 12 of the '641 patent, either literally or under the doctrine of equivalents, because such an intrusion detection system including CS products performs all the steps required in these claims, as set forth in detail in Exhibit 2.

ANSWER: Admitted that CS is aware of the DMV Facility. CS lacks knowledge or information sufficient to form a belief as to the truth of the allegations regarding whether the DMV Facility is distinguishable from other unidentified government facilities that employ a PDS and the allegations regarding a "point-to-multipoint" network layout, and therefore denies them. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

34. CS, with knowledge of the '641 patent and knowledge that the CS intrusion detection system used in the PDS with a point-to-multipoint network layout at the DMV Facility infringes the '641 patent, provides assistance and instruction in connection with the installation and use of the CS intrusion detection system at the DMV Facility and the knowhow to use the CS intrusion detection system in an infringing manner.

ANSWER: Denied.

35. CS, with knowledge of the '641 patent and knowledge that the CS intrusion detection system used in the PDS with a point-to-multipoint network layout at DMV Facility infringes the '641 patent, directs its salespeople and technical personnel to conduct troubleshooting and testing on the CS intrusion detection system used at the DMV Facility.

ANSWER: Denied.

36. When deployed for use with the PDS with a point-to-multipoint network layout at the DMV Facility, the CS intrusion detection system and method is specifically designed in a manner that infringes the '641 patent.

ANSWER: Denied.

37. In addition to those infringing detection systems and methods discussed above that are used with networks arranged in a point-to-multipoint layout, CS also manufactures, distributes, offers to sell and sells its "Controller," "Opti-Guard," and "Cyber Sensor" products (<https://www.cybersecureips.com/our-products/>) for use in a system and method for monitoring intrusion of manholes, lockboxes, and other purposes.

ANSWER: Admitted that the "Controller," "Opti-Guard," and "Cyber Sensor" products are listed at the linked website, and that webpage speaks for itself. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

38. Use of the CS Controller, Opti-Guard, and/or Cyber Sensor Products for manhole, lockbox, and other FBG monitoring infringes at least claim 8 of the '641 patent, either literally or under the doctrine of equivalents, because systems including these CS products perform all the steps required in the claim, as set forth in detail in Exhibit 2. CS has published the following two documents that provide a detailed description of the use of the CS Controller and Cyber Sensor for manhole and lockbox monitoring:

- a. Cyber Sensor Installation Guide (attached as **Exhibit 8**); and
- b. CyberSecure CSS Cyber Sensor Solution (attached as **Exhibit 9**).

As shown in detail in the claim chart attached as Exhibit 2, both these documents provide support for NIS' infringement claims.

ANSWER: Admitted that Exhibit 8 appears to be a copy of a Cyber Sensor Installation Guide, and Exhibit 9 appears to be a copy of a CyberSecure CSS Cyber Sensor Solution document, and these documents speak for themselves. Denied that there has been any infringement by CS of the patent-in-suit, or that the patent-in-suit is valid and enforceable. To the extent any remaining allegations in this paragraph are not expressly admitted herein, they are denied.

39. CS, with knowledge of the '641 patent and knowledge that manhole, lockbox, and other FBG monitoring systems that include the CS Controller, Opti-Guard, and/or Cyber Sensor Products infringe the '641 patent, provides assistance and instruction to customers in connection with the installation and use of these CS products and the knowhow to use these CS products in an infringing manner.

ANSWER: Denied.

40. CS, with knowledge of the '641 patent and knowledge that FBG monitoring systems that include the CS Controller, Opti-Guard, and/or Cyber Sensor Products infringe the '641 patent, directs its salespeople and technical personnel to conduct troubleshooting and testing on monitoring systems that employ these CS products.

ANSWER: Denied.

41. On information and belief, the CS Controller, Opti-Guard, and/or Cyber Sensor Products, when employed in FBG monitoring systems, are specifically designed for use in a manner that infringes the '641 patent, either literally or under the doctrine of equivalents, and these products have no substantially non-infringing use.

ANSWER: Denied.

42. On information and belief, CS offers products and services that infringe the claims of the '641 patent and other NIS patents, and NIS reserves the right to pursue additional infringement in this lawsuit. These products and services include, at least, other detection systems being offered for sale and/or sold to customers for use in fiber optic network layouts arranged in a point-to-multipoint configuration.

ANSWER: Denied.

COUNT I

([Alleged] Direct Infringement of the '641 Patent)

43. NIS adopts and incorporates by reference all the foregoing allegations as if fully set forth herein.

ANSWER: CS adopts and incorporates by reference all the foregoing answers as if fully set forth herein.

44. CS has directly infringed and continues to directly infringe under 35 U.S.C. § 271(a) one or more claims of the '641 patent either literally and/or under the doctrine of equivalents, by making, using, selling, and/or offering for sale in the United States the Accused Products and Services that infringe one or more claims of the '641 patent.

ANSWER: Denied.

45. CS is directly infringing the claims of the '641 patent by conducting the steps of the methods recited in the claims of the '641 patent at least when CS salespeople and technical representatives troubleshoot and test the CS systems and methods both during and after installation at end customer facilities such as the Primary Customer data centers and DMV Facility.

ANSWER: Denied.

46. On information and belief, CS has been aware of the '641 patent at least since the date that the parties entered into the ESR Agreement.

ANSWER: Denied.

COUNT II

([Alleged] Inducing of Infringement of the '641 Patent)

47. NIS adopts and incorporates by reference all the foregoing allegations as if fully set forth herein.

ANSWER: CS adopts and incorporates by reference all the foregoing answers as if fully set forth herein.

48. CS has induced infringement and continues to induce infringement under 35 U.S.C. § 271(b).

ANSWER: Denied.

49. CS offers for sale, sells, and has sold the Accused Products and Services to entities in the networking sector including, but not limited to, the DMV Facility and the Primary Customer data centers.

ANSWER: Denied.

50. CS's customers have directly infringed and continue to directly infringe, under 35 U.S.C. § 271(a), one or more claims of the '641 patent, either literally and/or under the doctrine of equivalents, by using the Accused Products and Services in the United States that infringe one or more claims of the '641 patent, as described in detail above.

ANSWER: Denied.

51. CS has actively, knowingly, and intentionally induced, and continues to actively, knowingly, and intentionally induce, infringement of the '641 patent, by offering to sell, selling and/or otherwise supplying the Accused Products and Services, with the knowledge and intent that

third parties will use the Accused Products and Services in the United States, for their intended purpose to infringe the '641 patent, and with the knowledge and intent to encourage and facilitate infringement through the dissemination of the Accused Products and Services and/or the creation and dissemination of documentation and technical information to customers and prospective customers related to the Accused Products and Services.

ANSWER: Denied.

52. CS, through its sales people and technical field representatives, over whom CS exerts control and direction, provides assistance and instruction in connection with installation and use of the Accused Product and Services at facilities and the knowhow to use the Accused Product and Services in an infringing manner, at all times having knowledge of the '641 patent and with the intent that personnel at the facilities operate the Accused Product and Services so that there is infringement of the '641 patent.

ANSWER: Denied.

53. On information and belief, CS, through its sales people and technical field representatives, troubleshoot operation of the Accused Product and Services at customer facilities during and after installation of the Accused Product and Services with full knowledge of the '641 patent and that the Accused Product and Services operate in a manner that infringes the '641 patent and with the intent that the customers operate the Accused Product and Services in a manner that infringes the '641 patent.

ANSWER: Denied.

54. On information and belief, CS has been aware of the '641 patent at least since the date that the parties entered into the ESR Agreement.

ANSWER: Denied.

COUNT III

([Alleged] Contributory Infringement of the '641 Patent)

55. NIS adopts and incorporates by reference all the foregoing allegations as if fully set forth herein.

ANSWER: CS adopts and incorporates by reference all the foregoing answers as if fully set forth herein.

56. CS offers for sale, sells, and has sold the Accused Products and Services to entities in the networking sector including, but not limited to, the DMV Facility and the Primary Customer data centers.

ANSWER: Denied.

57. CS's customers have directly infringed and continue to directly infringe, under 35 U.S.C. § 271(a), one or more claims of the '641 patent, either literally and/or under the doctrine of equivalents, by using the Accused Products and Services in the United States that infringe one or more claims of the '641 patent, as described in detail above.

ANSWER: Denied.

58. CS has contributed and continues to contribute to the infringement by third parties, including its customers, of one or more claims of the '641 patent under 35 U.S.C. § 271(c), by selling and/or offering for sale in the United States the Accused Products and Services knowing that those products and services constitute a material part of the inventions of the '641 patent, knowing that those products and services are especially made or adapted to infringe the '641 patent, and knowing that when sold for use with a point-to-multipoint network layout those products are not staple articles of commerce suitable for substantial non-infringing use.

ANSWER: Denied.

59. CS, through its sales people and technical field representatives, over whom CS exerts control and direction, provides assistance and instruction in connection with installation and use of the Accused Product and Services at facilities and the knowhow to use the Accused Product and Services in an infringing manner at all times having knowledge of the '641 patent and with the intent that personnel at the facilities operate the Accused Product and Services so that there is infringement of the '641 patent.

ANSWER: Denied.

60. On information and belief, CS, through its sales people and technical field representatives, troubleshoot operation of the Accused Product and Services at customer facilities during and after installation of the Accused Product and Services with full knowledge of the '641 patent and that the Accused Product and Services operate in a manner that infringes the '641 patent and with the intent that the customers operate the Accused Product and Services in a manner that infringes the '641 patent.

ANSWER: Denied.

61. The Accused Products and Services are designed in a manner that infringe one or more claims of the '641 patent, and the Accused Products and Services when sold for use with a point-to-multipoint network layout are not staple articles of commerce suitable for substantial non-infringing use.

ANSWER: Denied.

62. On information and belief, CS has been aware of the '641 patent at least since the date that the parties entered into the ESR Agreement.

ANSWER: Denied.

CS [ALLEGEDLY] WILLFULLY INFRINGES THE '641 PATENT

63. NIS adopts and incorporates by reference all the foregoing allegations as if fully set forth herein.

ANSWER: CS adopts and incorporates by reference all the foregoing answers as if fully set forth herein.

64. On information and belief, CS has been aware of the '641 patent at least since the date that the parties entered into the ESR Agreement in 2015. Despite this knowledge, and an objectively high likelihood that its actions constitute direct and other infringement of the '641 patent, CS has engaged in infringement of the '641 patent.

ANSWER: Denied.

65. CS has sought to replace NIS products with its own products thereby ensuring that the resulting CS optical fiber intrusion monitoring system and method would infringe the '641 patent.

ANSWER: Denied.

66. The infringing conduct by CS of the '641 patent renders this case exceptional within the meaning of 35 U.S.C. § 285.

ANSWER: Denied.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Network Integrity Systems, Inc. respectfully requests that this Court enter judgment against Defendant CyberSecure IPS LLC:

- A. That Defendant has directly infringed the patent-in-suit;
- B. That Defendant has induced infringement of the patent-in-suit;
- C. That Defendant has contributed to infringement of the patent-in-suit;

- D. That Plaintiff be awarded all damages adequate to compensate it for Defendant's infringement of the patent-in-suit, such damages to be determined by a jury with pre-judgment and post-judgment interest;
- E. That Defendant's infringement was willful and that such damages be trebled pursuant to 35 U.S.C. § 284;
- F. For an order permanently enjoining Defendant and its officers, agents, servants and employees, privies, and all persons in concert or participation with it, from further infringement of the patent-in-suit;
- G. That this case be declared an exceptional case within the meaning of 35 U.S.C. § 285 and that Plaintiff be awarded its attorney's fees, costs and expenses incurred relating to this action; and
- H. That Plaintiff be awarded such other and further relief as the Court deems just and proper.

ANSWER: Denied that NIS is entitled to any relief.

AFFIRMATIVE AND OTHER DEFENSES

Without assuming any burden that it would not otherwise bear and reserving the right to assert additional defenses, CS, without waiver, limitation, or prejudice, hereby asserts the following defenses to NIS's Complaint.

First Defense: Failure to State a Claim

Every claim asserted in the Complaint fails to state a claim upon which relief can be granted

Second Defense: Non-Infringement

CS does not infringe any claim of the asserted patent-in-suit, either literally or under the doctrine of equivalents. CS does not infringe either directly or indirectly.

Third Defense: Invalidity

The patent-in-suit is invalid under one or more of 35 U.S.C. §§ 101, 102, 103, 112, 115, 116, 132, and/or under the doctrine of obviousness-type double patenting.

Fourth Defense: Equitable Defenses and Unenforceability

Plaintiff's claims are barred, in whole or in part, by one or more of the doctrine of waiver, equitable estoppel, unclean hands and/or other applicable equitable defenses.

Fifth Defense: No Ensnarement

Plaintiff's claims are barred, in whole or in part, by the doctrine of ensnarement. Plaintiff is precluded from asserting infringement under the doctrine of equivalents if it will encompass or ensnare the prior art.

Sixth Defense: License and Exhaustion

Plaintiff's claims are barred, in whole or in part, by defenses of license (either express or implied) and/or patent exhaustion.

Seventh Defense: Failure to State a Claim for Willful Infringement

Plaintiff's claims, and each and every claim stated therein, fails to state a claim for willful infringement upon which relief can be granted.

Eighth Defense: Limitation on Damages

Plaintiff's claims for damages are limited (including lack of any pre-suit damages) as a consequence of failing to comply with the requirements of 35 U.S.C. §§ 286, 287 (including but not limited to failure to mark and/or provide pre-suit notice of infringement), and/or 288 (asserted Patents-in-Suit are invalid).

Ninth Defense: Limitation on Damages

Any recovery of damages by Plaintiff is limited in whole or in part by the failure to mitigate damages.

Tenth Defense: No Injunctive Relief

Plaintiff is not entitled to injunctive relief because any alleged injury to Plaintiff is not immediate or irreparable, and Plaintiff has an adequate remedy at law.

Reservation of Defenses

CS reserves the right to assert other defenses, including inequitable conduct, based upon evidence adduced in discovery.

COUNTERCLAIMS

These are counterclaims by CyberSecure IPS LLC (“CS”) for declaratory judgment of invalidity and noninfringement of U.S. Patent No. 7,706,641 (“the ’641 patent”) (Dkt. 1-2), as well as patent infringement against Network Integrity Systems, Inc. (“NIS”).

NATURE OF THE ACTION

1. CS’s counterclaims for declaratory judgment of invalidity and noninfringement arise under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.* CS’s counterclaims for patent infringement arise under the Patent Laws of the United States, 35 U.S.C. § 1, *et. seq.*, resulting from NIS’s infringement of at least four patents through its unauthorized manufacture, use, offers to sell, and sale of products in the United States, and

THE PARTIES

2. CS is a corporation organized and existing under the laws of the State of Maryland with a principal place of business located at 3 Bethesda Metro Center Suite 700, Bethesda, MD 20814.

3. Network Integrity Systems, Inc. alleges it is corporation organized and existing under the laws of North Carolina with its principal place of business at 1937 Tate Blvd SE, Hickory, NC 28602-1430.

JURISDICTION AND VENUE

4. This action arises under the patent laws of the United States, 35 U.S.C. § 1, *et seq.* Accordingly, this Court has original and subject-matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1338(a), 2201, and 2202.

5. This Court has personal jurisdiction over NIS because the parties have stipulated to litigate in this District. (Dkt. 12.)

6. Venue is proper in this District pursuant to 28 U.S. Code §§ 1391(b), 1391(c), and 1400(b) because the parties have stipulated to litigate in this District. (Dkt. 12.)

THE PATENTS-IN-SUIT

NIS Patent

7. The '641 patent is titled "Monitoring Individual Fibers of an Optical Cable for Intrusion" and was issued on April 27, 2010. The '641 patent names NIS as the assignee on its face. (Dkt. 1-2.)

CS Patents

8. On November 29, 2022, U.S. Patent No. 11,515,940 ("the '940 Patent") titled "Test device for verifying operation of an optical fiber monitoring system" was duly and legally issued by the United States Patent and Trademark Office. A copy of the '940 Patent is attached as **Exhibit 1**. The '940 Patent is presumed valid pursuant to 35 U.S.C. § 282.

9. On July 12, 2022, U.S. Patent No. 11,388,181 ("the '181 Patent") is titled "Cable assembly disturbance detection method" was duly and legally issued by the United States Patent and Trademark Office. A copy of the '181 Patent is attached as **Exhibit 2**. The '181 Patent is presumed valid pursuant to 35 U.S.C. § 282.

10. On September 27, 2016, U.S. Patent No. 9,455,999 ("the '999 Patent") titled "Method and system for protective distribution system (PDS) and infrastructure protection and management" was duly and legally issued by the United States Patent and Trademark Office. A copy of the '999 Patent is attached as **Exhibit 3**. The '999 Patent is presumed valid pursuant to 35 U.S.C. § 282.

11. On June 21, 2022, U.S. Patent No. 11,367,342 ("the '342 Patent") was duly and legally issued by the United States Patent and Trademark Office. A copy of the '342 Patent is attached as **Exhibit 4**. The '342 Patent is presumed valid pursuant to 35 U.S.C. § 282.

12. Collectively, the '940 Patent, '181 Patent, '999 Patent, and '342 Patent are the "Patents-in-Suit" or "Asserted Patents."

BACKGROUND

13. CS created the first-of-its-kind critical infrastructure end-to-end solution that protects data centers from physical threats and cyber-attacks. CS protects its innovative and valuable solutions via patent protection.

14. CS and NIS both operate in the field of data center network security technology and infrastructure. Originally, NIS prosecuted the '940 Patent, as well as other patents covering similar technology. Then, on May 5, 2023, NIS assigned the '940 Patent, as well as the other related patents, to CS. A copy of the assignment agreement is attached as **Exhibit 5**.

15. The '181 Patent, '999 Patent, and '342 Patent were prosecuted by and assigned to CS.

16. On January 24, 2025, CS, through counsel, sent a cease and desist letter to NIS to demand immediate termination of infringing activities related to the Asserted Patents. A copy of the January 24, 2025 cease and desist letter is attached as **Exhibit 6**.

17. On February 24, 2025, NIS responded through counsel, declining to cease its infringing activities. A copy of the February 24, 2025 NIS responding correspondence is attached as **Exhibit 7**.

COUNTERCLAIM I – DECLARATORY JUDGMENT OF INVALIDITY OF U.S. PATENT NO. 7,706,641

18. CS repeats and realleges the allegations in each of the preceding paragraphs as if fully set forth herein.

19. All of the claims of the '641 patent are invalid for failure to meet one or more of the requirements of §§ 101, 102, 103, and/or 112 of Title 35 of the United States Code.

20. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, Defendant is entitled to a declaratory judgment of invalidity of the '641 patent.

COUNTERCLAIM II – DECLARATORY JUDGMENT OF NONINFRINGEMENT OF U.S. PATENT NO. 7,706,641

21. CS repeats and realleges the allegations in each of the preceding paragraphs as if fully set forth herein.

22. CS has not infringed, either directly or indirectly, any valid and enforceable claim of the '641 patent.

23. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, Defendant is entitled to a declaratory judgment of noninfringement of the '641 patent.

COUNTERCLAIM III – PATENT INFRINGEMENT OF U.S. PATENT NO. 11,515,940

24. CS repeats and realleges the allegations in each of the preceding paragraphs as if fully set forth herein.

25. CS is the assignee of all right, title, and interest in the '940 Patent.

26. The '940 Patent is directed to improved methods “for periodically, or on demand, checking and verifying proper operation of a monitoring system of an optical fiber.” **Exhibit 1**, at 1:5-7.

27. The U.S. Patent Office considered the claims of the '940 Patent against the background of prior technology to determine if the claims of the '940 Patent identified a patentable advance over prior art systems before issuing the patent. The face of the '940 Patent identifies some of the prior art considered in allowing the various claims of the '940 Patent, including for example U.S. Patent No. 5,384,635 entitled “Remote sensing in optical fiber networks by synchronously detecting backscattered optical signals.”

28. A person of ordinary skill in the art would understand that the separate claims in the '940 Patent did not pre-empt any field, but are improvements in methods and systems for checking and verifying proper operation of a monitoring system of an optical fiber. A person of ordinary skill in the art would also recognize that the claims of the '940 Patent do not relate to implementation of a business method on a general purpose computer, but are specific improvements to checking and verifying proper operation of a monitoring system of an optical fiber.

29. NIS was on notice of the '940 Patent from the moment it issued, because NIS prosecuted the patent. *See Exhibit 5*. NIS further had notice of the '940 Patent and its infringing activities as of the January 24, 2025 cease and desist letter from CS. *See Exhibit 6*. Alternatively, at minimum, the filing of this Complaint constitutes notice and actual knowledge in accordance with 35 U.S.C. § 287.

30. Without permission or authorization from CS, in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, NIS has been, and still is, infringing one or more claims of the '940 Patent by using at least the products identified in the chart incorporated into this Claim below (“the '940 Patent Exemplary Products”).

31. For example, and not by way of limitation, the '940 Patent Exemplary Products practice at least claim 9 of the '940 Patent. A claim chart comparing claim 9 to the '940 Patent Exemplary Products is attached as **Exhibit 8**. CS reserves the right to modify its infringement theories as discovery progress in the case; it shall not be estopped for infringement contention or claim construction purposes by the information contained herein.

32. Without permission or authorization from CS, in violation of 35 U.S.C. § 271(b), NIS is inducing the direct infringement of at least claim 9 of the '940 Patent by aiding, abetting,

and encouraging its customers' use of the '940 Patent Exemplary Products with knowledge of the infringement of the '940 Patent and with the intent to cause such infringement.

33. For example, NIS provides product literature and maintains a website advertising the infringing use of the '940 Patent Exemplary Products. *See Exhibit 8* (citing relevant portions of NIS's website and marketing material).

34. NIS's infringement of the '940 Patent has been, and continues to be, willful and deliberate.

35. As a result of NIS's infringement, CS has suffered and will continue to suffer damages in an amount to be proven at trial and irreparable harm.

36. The conduct of NIS presents an exceptional case such that CS is entitled to an award of its reasonable attorneys' fees, as provided by 35 U.S.C. § 285.

COUNTERCLAIM IV – PATENT INFRINGEMENT OF U.S. PATENT NO. 11,388,181

37. CS repeats and realleges the allegations in each of the preceding paragraphs as if fully set forth herein.

38. CS is the assignee of all right, title, and interest in the '181 Patent.

39. The '181 Patent is directed to improved methods for “detection of a disturbance on an information transmission line, including, for example, disturbance location identification, disturbance type identification, disturbance-triggered sensory indicators, disturbance detection handling, or cable assemblies with respect to a physical transmission line,” including implementing machine learning techniques. **Exhibit 2**, at 1:23-28; 25:10-40.

40. The U.S. Patent Office considered the claims of the '181 Patent against the background of prior technology to determine if the claims of the '181 Patent identified a patentable advance over prior art systems before issuing the patent. Among other things, the U.S. Patent Office searched multiple sets of prior art in classifications including, but not limited to, H04L

63/1416 (2013.01); G08B 13/186 (2013.01); H04L 41/22 (2013.01); H04L 63/1425; H04L 63/1408; H04L 63/1433; H04L 41/22; H04L 43/0864 (2013.01); H04L 43/16 (2013.01); H04L 63/1425 (2013.01); H04L 41/0213 (2013.01); H04L 63/1408 (2013.01); H04L 63/1433 (2013.01); and H04L 67/12 (2013.01). The face of the '181 Patent identifies some of the prior art from the classifications and other prior art considered in allowing the various claims of the '181 Patent, including for example U.S. Patent No. 7,092,586 entitled "Intrusion detection system for use on an optical fiber using a translator of transmitted data for optimum monitoring conditions."

41. A person of ordinary skill in the art would understand that the separate claims in the '181 Patent did not pre-empt any field, but are improvements in methods for detection of a disturbance on an information transmission line. A person of ordinary skill in the art would also recognize that the claims of the '181 Patent do not relate to implementation of a business method on a general purpose computer, but are specific improvements to detection of a disturbance on an information transmission line, including via machine learning techniques.

42. NIS at least had notice of the '181 Patent and its infringing activities as of the January 24, 2025 cease and desist letter from CS. *See Exhibit 6*. Alternatively, at minimum, the filing of this Complaint constitutes notice and actual knowledge in accordance with 35 U.S.C. § 287.

43. Without permission or authorization from CS, in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, NIS has been, and still is, infringing one or more claims of the '181 Patent by, without authority, at least making, using, selling, and/or offering to sell at least the products identified in the chart incorporated into this Claim below ("the '181 Patent Exemplary Products").

44. For example, and not by way of limitation, the '181 Patent Exemplary Products practice at least claim 14 of the '181 Patent. A claim chart comparing claim 14 to the '181 Patent Exemplary Products is attached as **Exhibit 9**. CS reserves the right to modify its infringement theories as discovery progress in the case; it shall not be estopped for infringement contention or claim construction purposes by the information contained herein.

45. Without permission or authorization from CS, in violation of 35 U.S.C. § 271(b), NIS is inducing the direct infringement of at least claim 14 of the '181 Patent by aiding, abetting, and encouraging its customers' use of the '181 Patent Exemplary Products with knowledge of the infringement of the '181 Patent and with the intent to cause such infringement.

46. For example, NIS provides product literature and maintains a website advertising the infringing use of the '181 Patent Exemplary Products. *See Exhibit 9* (citing relevant portions of NIS's website and marketing material).

47. NIS's infringement of the '181 Patent has been, and continues to be, willful and deliberate.

48. As a result of NIS's infringement, CS has suffered and will continue to suffer damages in an amount to be proven at trial and irreparable harm.

49. The conduct of NIS presents an exceptional case such that CS is entitled to an award of its reasonable attorneys' fees, as provided by 35 U.S.C. § 285.

COUNTERCLAIM V – PATENT INFRINGEMENT OF U.S. PATENT NO. 9,455,999

50. CS repeats and realleges the allegations in each of the preceding paragraphs as if fully set forth herein.

51. CS is the assignee of all right, title, and interest in the '999 Patent.

52. The '999 Patent is directed to improved systems and methods for “managing a protective distribution system.” **Exhibit 3**, at 1:18-20.

53. The U.S. Patent Office considered the claims of the '999 Patent against the background of prior technology to determine if the claims of the '999 Patent identified a patentable advance over prior art systems before issuing the patent. Among other things, the U.S. Patent Office searched multiple sets of prior art in classifications including, but not limited to, H04L 63/1416 (2013.01); H04L 63/1408 (2013.01); H04L 63/1425 (2013.01); H04L 63/1433 (2013.01). The face of the '999 Patent identifies some of the prior art from the classifications and other prior art considered in allowing the various claims of the '999 Patent, including for example U.S. Patent Publ. No. US 2014/0091929A1 entitled "Systems and Methods for Secure Alarmed Armored Protective Distribution Systems and Management."

54. A person of ordinary skill in the art would understand that the separate claims in the '999 Patent did not pre-empt any field, but are improvements in systems and methods for detection of managing a protective distribution system. A person of ordinary skill in the art would also recognize that the claims of the '999 Patent do not relate to implementation of a business method on a general purpose computer, but are specific improvements to managing a protective distribution system.

55. Upon information and belief, NIS was on notice of the '999 Patent shortly after issuance because NIS monitors CS's patent portfolio.

56. NIS at least had notice of the '999 Patent and its infringing activities as of the January 24, 2025 cease and desist letter from CS. *See Exhibit 6*. Alternatively, at minimum, the filing of this Complaint constitutes notice and actual knowledge in accordance with 35 U.S.C. § 287.

57. Without permission or authorization from CS, in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, NIS has been, and still is, infringing one or more

claims of the '999 Patent by, without authority, at least making, using, selling, and/or offering to sell at least the products identified in the chart incorporated into this Claim below (“the '999 Patent Exemplary Products”).

58. For example, and not by way of limitation, the '999 Patent Exemplary Products practice at least claim 1 of the '999 Patent. A claim chart comparing claim 1 to the '999 Patent Exemplary Products is attached as **Exhibit 10**. CS reserves the right to modify its infringement theories as discovery progress in the case; it shall not be estopped for infringement contention or claim construction purposes by the information contained herein.

59. Without permission or authorization from CS, in violation of 35 U.S.C. § 271(b), NIS is inducing the direct infringement of at least claim 1 of the '999 Patent by aiding, abetting, and encouraging its customers' use of the '999 Patent Exemplary Products with knowledge of the infringement of the '999 Patent and with the intent to cause such infringement.

60. For example, NIS provides product literature and maintains a website advertising the infringing use of the '999 Patent Exemplary Products. *See Exhibit 10* (citing relevant portions of NIS's website and marketing material).

61. NIS's infringement of the '999 Patent has been, and continues to be, willful and deliberate.

62. As a result of NIS's infringement, CS has suffered and will continue to suffer damages in an amount to be proven at trial and irreparable harm.

63. The conduct of NIS presents an exceptional case such that CS is entitled to an award of its reasonable attorneys' fees, as provided by 35 U.S.C. § 285.

COUNTERCLAIM VI – PATENT INFRINGEMENT OF U.S. PATENT NO. 11,367,342

64. CS repeats and realleges the allegations in each of the preceding paragraphs as if fully set forth herein.

65. CS is the assignee of all right, title, and interest in the '342 Patent.

66. CS has complied with the marking requirements of 35 U.S.C. § 287.

67. The '342 Patent is directed to improved systems and methods for “facilitating real-time playback modification for activity event playback.” **Exhibit 4**, at 1:17-18.

68. The U.S. Patent Office considered the claims of the '342 Patent against the background of prior technology to determine if the claims of the '342 Patent identified a patentable advance over prior art systems before issuing the patent. Among other things, the U.S. Patent Office searched multiple sets of prior art in classifications including, but not limited to, GOSB 29/185; G08B 21/182; G08B 13/186; G08B 29/24; GOIV 8/14; G06K 9/6277; G06K 9/6288; G06K 9/6271; HO4L 67/12; G06V 10/82; G06V 20/52. The face of the '342 Patent identifies some of the prior art from the classifications and other prior art considered in allowing the various claims of the '342 Patent, including for example U.S. Patent No. 10,516,689 entitled “Distributed data surveillance in a community capture environment.”

69. A person of ordinary skill in the art would understand that the separate claims in the '342 Patent did not pre-empt any field, but are improvements in systems and methods for facilitating real-time playback modification for activity event playback. A person of ordinary skill in the art would also recognize that the claims of the '342 Patent do not relate to implementation of a business method on a general purpose computer, but are specific improvements to facilitating real-time playback modification for activity event playback.

70. Upon information and belief, NIS was on notice of the '342 Patent shortly after issuance because NIS monitors CS's patent portfolio.

71. NIS at least had notice of the '342 Patent and its infringing activities as of the January 24, 2025 cease and desist letter from CS. *See Exhibit 6*. Alternatively, at minimum, the

filing of this Complaint constitutes notice and actual knowledge in accordance with 35 U.S.C. § 287.

72. Without permission or authorization from CS, in violation of 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, NIS has been, and still is, infringing one or more claims of the '342 Patent by, without authority, at least making, using, selling, and/or offering to sell at least the products identified in the chart incorporated into this Claim below ("the '342 Patent Exemplary Products").

73. For example, and not by way of limitation, the '342 Patent Exemplary Products practice each and every element of at least claim 17 of the '342 Patent. A claim chart comparing claim 17 with the '342 Patent Exemplary Products is attached as **Exhibit 11**. CS reserves the right to modify its infringement theories as discovery progress in the case; it shall not be estopped for infringement contention or claim construction purposes by the information contained herein.

74. Without permission or authorization from CS, in violation of 35 U.S.C. § 271(b), NIS is inducing the direct infringement of at least claim 14 of the '342 Patent by aiding, abetting, and encouraging its customers' use of the '342 Patent Exemplary Products with knowledge of the infringement of the '342 Patent and with the intent to cause such infringement.

75. For example, NIS provides product literature and maintains a website advertising the infringing use of the '342 Patent Exemplary Products. *See Exhibit 11* (citing relevant portions of NIS's website and marketing material).

76. NIS's infringement of the '342 Patent has been, and continues to be, willful and deliberate.

77. As a result of NIS's infringement, CS has suffered and will continue to suffer damages in an amount to be proven at trial and irreparable harm.

78. The conduct of NIS presents an exceptional case such that CS is entitled to an award of its reasonable attorneys' fees, as provided by 35 U.S.C. § 285.

PRAYER FOR RELIEF

WHEREFORE, CS respectfully requests that this Court enter judgment against NIS as follows:

- A. Dismiss NIS's Complaint with prejudice and find that NIS takes nothing by its claims against CS;
- B. Enter judgment in favor of CS, and against NIS, on the Complaint;
- C. For judgment in CS's favor on each Counterclaim asserted herein;
- D. Declare that the claims of the '641 patent are invalid;
- E. Declare that CS does not and has not infringed any claim of the '641 patent;
- F. For judgment that NIS has infringed the CS Patents-in-Suit;
- G. For judgment that NIS's patent infringement has been willful;
- H. For judgment that NIS's conduct is "exceptional" under 35 U.S.C. § 284;
- I. Awarding all damages sustained by CS as a result of NIS's acts of patent infringement, including supplemental damages for any continuing post-verdict infringement up until entry of the final judgment with an accounting as needed;
- J. For a permanent injunction enjoining NIS from infringing the claims of the CS Patents-in-Suit;
- K. Awarding CS its attorneys' fees pursuant to 35 U.S.C. § 285 or as otherwise permitted by law, together with the costs and disbursements of this action;
- L. Awarding all pre-judgment interest and post-judgment interest; and
- M. Awarding such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

CS demands a trial by jury of all issues so triable.

Dated: July 21, 2025

By: /s/ Jarren N. Ginsburg

Jarren N. Ginsburg (D.Md. Bar No 19688)
FOLEY & LARDNER LLP
Washington Harbour, 3000 K Street N.W.
Suite 600, Washington, DC 20007-5101
Telephone: (202) 672-5300
Facsimile: (202) 672-5399
Email: JGinsburg@foley.com

Kimberly K. Dodd (admission pending)
FOLEY & LARDNER LLP
777 East Wisconsin Avenue
Milwaukee, WI 53202-5306
Telephone: (414) 271-2400
Facsimile: (414) 297-4900
Email: kdodd@foley.com

Jack T. Carroll (*pro hac vice* forthcoming)
FOLEY & LARDNER LLP
150 E Gilman St, Suite 5000,
Madison, WI 53703
Telephone: (608) 257-5035
Facsimile: (608) 258-4258
Email: jcarroll@foley.com

Attorneys for Cybersecure IPS, LLC

Exhibit 1

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

(10) **Patent No.:** **US 11,515,940 B2**
(45) **Date of Patent:** **Nov. 29, 2022**

(54) **TEST DEVICE FOR VERIFYING
OPERATION OF AN OPTICAL FIBER
MONITORING SYSTEM**

(71) Applicant: **Network Integrity Systems, Inc.,**
Hickory, NC (US)

(72) Inventors: **Cary R. Murphy**, Hickory, NC (US);
Dave Eric Cunningham, Conover, NC
(US); **Mark K Bridges**, Hickory, NC
(US); **Daniel M. Goertzen**, Winnipeg
(CA); **Matthew R. Friede**, Greenville,
SC (US); **Andrew V. Pasterczyk, Jr.**,
Virginia Beach, VA (US); **Darrell J.**
Magee, III, Yorktown, VA (US)

(73) Assignee: **Network Integrity Systems, Inc.,**
Hickory, NC (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 0 days.

(21) Appl. No.: **17/018,535**

(22) Filed: **Sep. 11, 2020**

(65) **Prior Publication Data**

US 2022/0085879 A1 Mar. 17, 2022

(51) **Int. Cl.**
H04B 17/00 (2015.01)
H04B 10/079 (2013.01)

(52) **U.S. Cl.**
CPC **H04B 10/0795** (2013.01)

(58) **Field of Classification Search**
CPC H04B 10/0795
USPC 398/28
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,384,635 A * 1/1995 Cohen G01S 7/499
356/73.1
5,703,682 A * 12/1997 Eslambolchi H04B 10/079
356/73.1
7,142,737 B1 11/2006 Murphy
7,706,641 B2 4/2010 Murphy
9,621,262 B1 4/2017 Timmins
2005/0254038 A1 * 11/2005 Harres G01M 11/083
356/73.1
2007/0086694 A1 4/2007 Murphy
(Continued)

FOREIGN PATENT DOCUMENTS

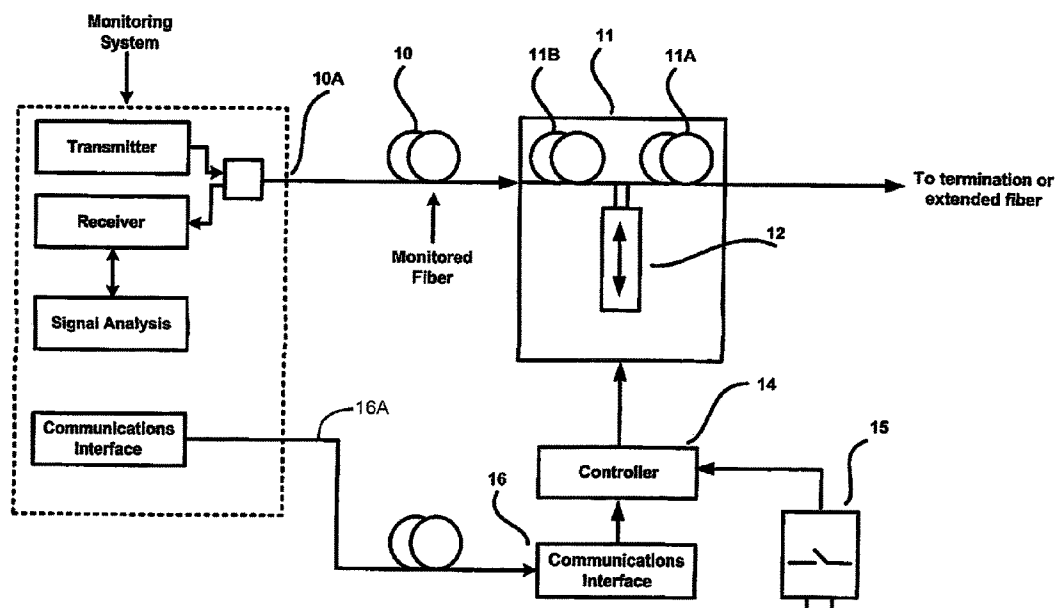
CN 103926061 7/2014
CN 104240455 12/2014
(Continued)

Primary Examiner — Mohammad R Sedighian
(74) *Attorney, Agent, or Firm* — Adrian D. Battison; Ade
& Company Inc.; Ryan W. Dupuis

(57) **ABSTRACT**

In an optical fiber monitoring system which detects physical disturbance or other parameters such as temperature or strain of a fiber where a monitor signal is transmitted along the optical fiber and analyzed to detect changes which are indicative of an event, a method is provided for periodically checking proper operation of the optical fiber monitoring system. A fiber disturbance actuator periodically causes a pattern of disturbances of a portion of the fiber at a predetermined location thereon where the disturbance is characteristic of the event to be monitored. The monitor signal is analyzed to detect the pattern of changes and in the event that expected changes are not detected, a warning is issued that the intrusion detection system is not properly operating.

26 Claims, 11 Drawing Sheets



US 11,515,940 B2

Page 2

(56)

References Cited

U.S. PATENT DOCUMENTS

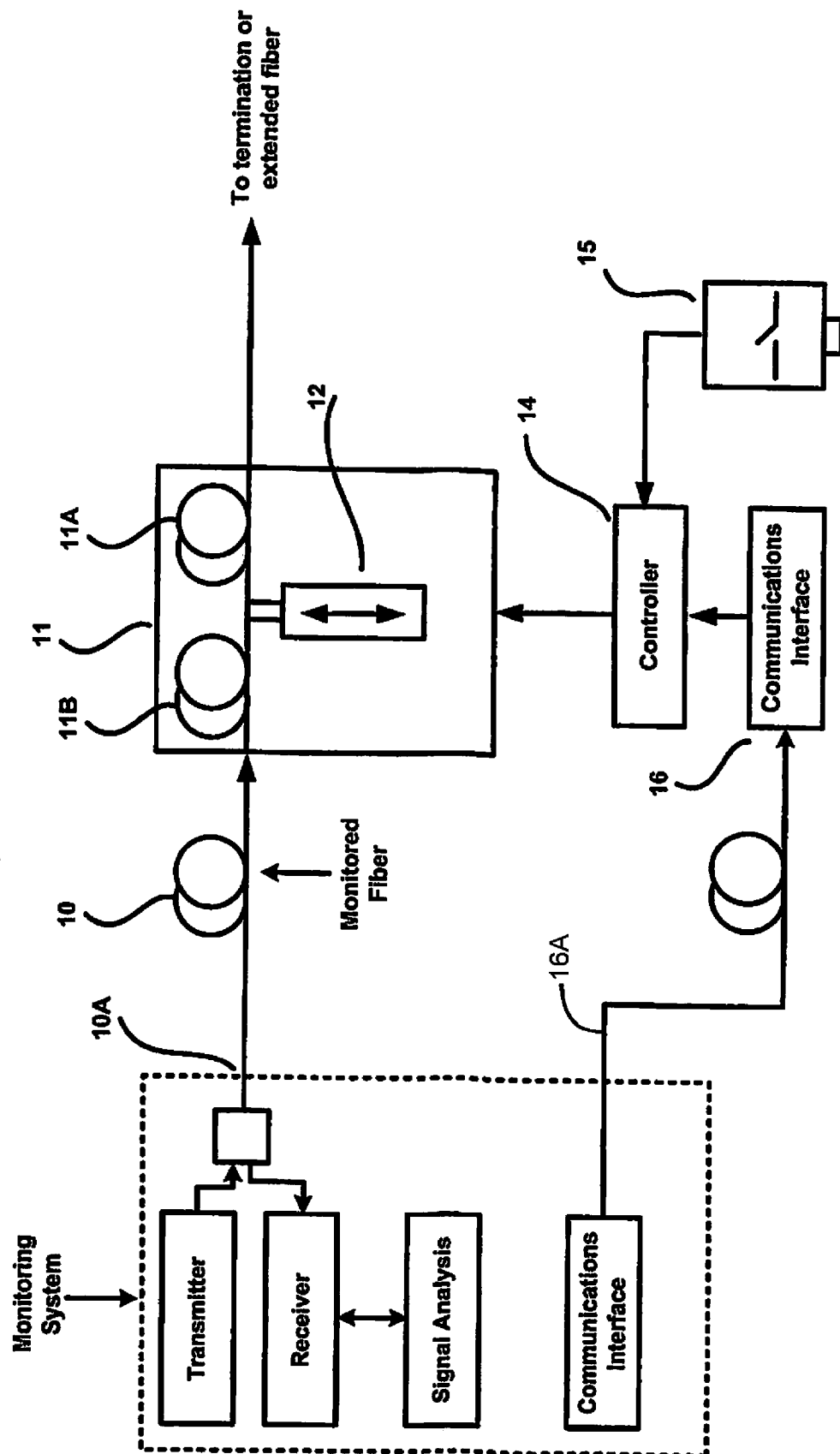
2010/0284000	A1 *	11/2010	Xu	G01D 5/35358
				356/301
2013/0188177	A1	7/2013	Lovely	
2014/0368809	A1	12/2014	Chen	
2016/0327436	A1 *	11/2016	Tur	G01K 11/32
2017/0067335	A1 *	3/2017	Weng	E21B 47/10
2018/0292240	A1 *	10/2018	Liu	G08B 13/186
2019/0074896	A1	3/2019	Murphy	
2021/0278314	A1 *	9/2021	Xia	G01M 11/088

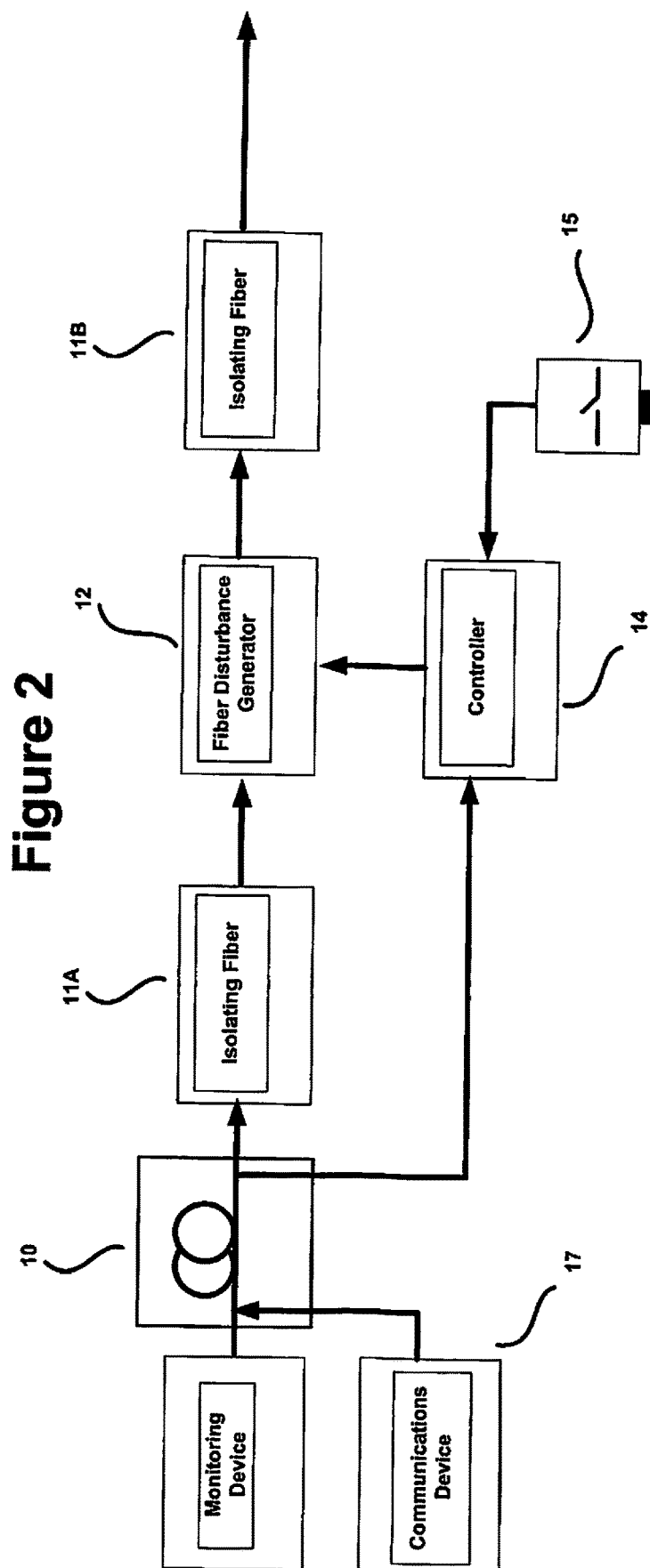
FOREIGN PATENT DOCUMENTS

GB	2317008	3/1998
JP	2007121090	5/2007
JP	2009014546	1/2009
JP	2018048917	3/2018
KR	20090087590	8/2009
KR	101574198	12/2015
WO	WO2005010562	2/2005
WO	WO2014035303	3/2014

* cited by examiner

Figure 1





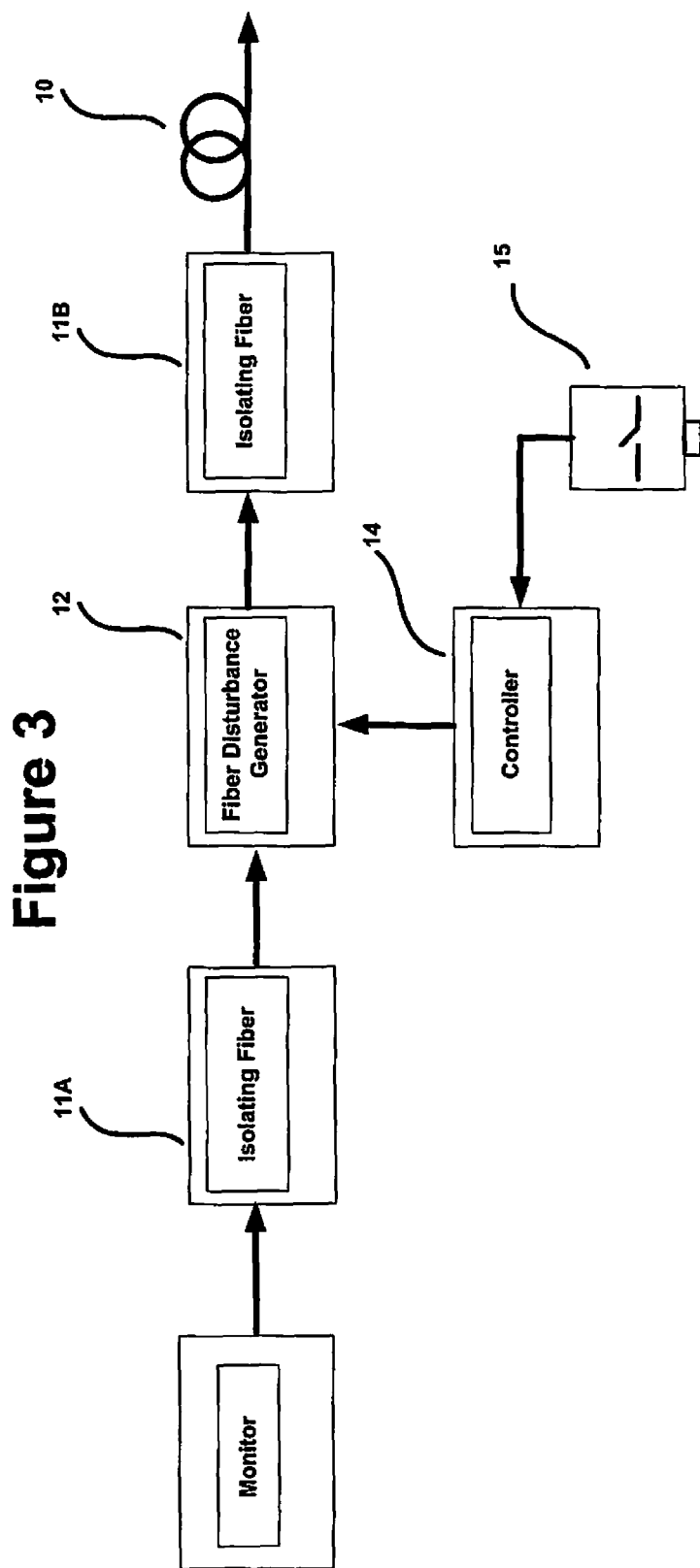
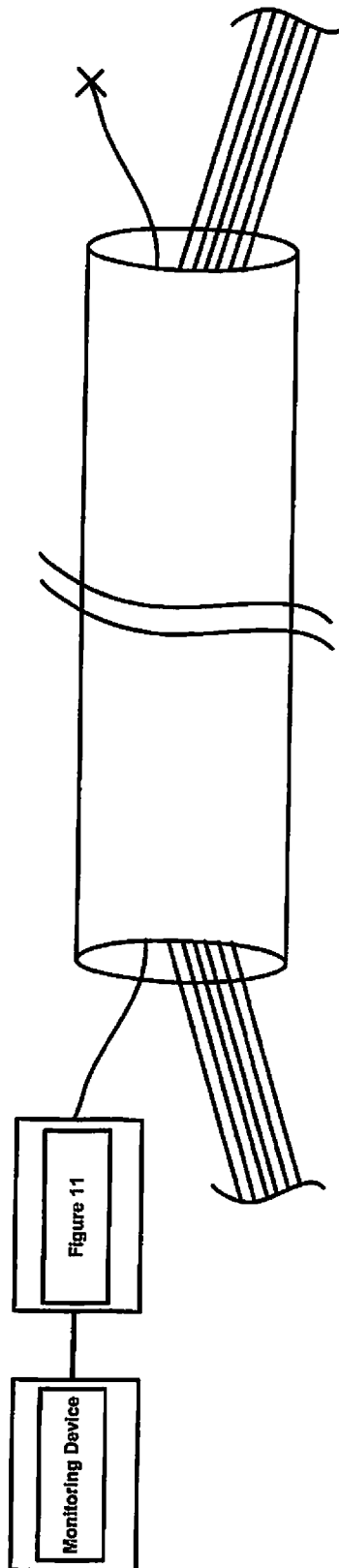


Figure 4



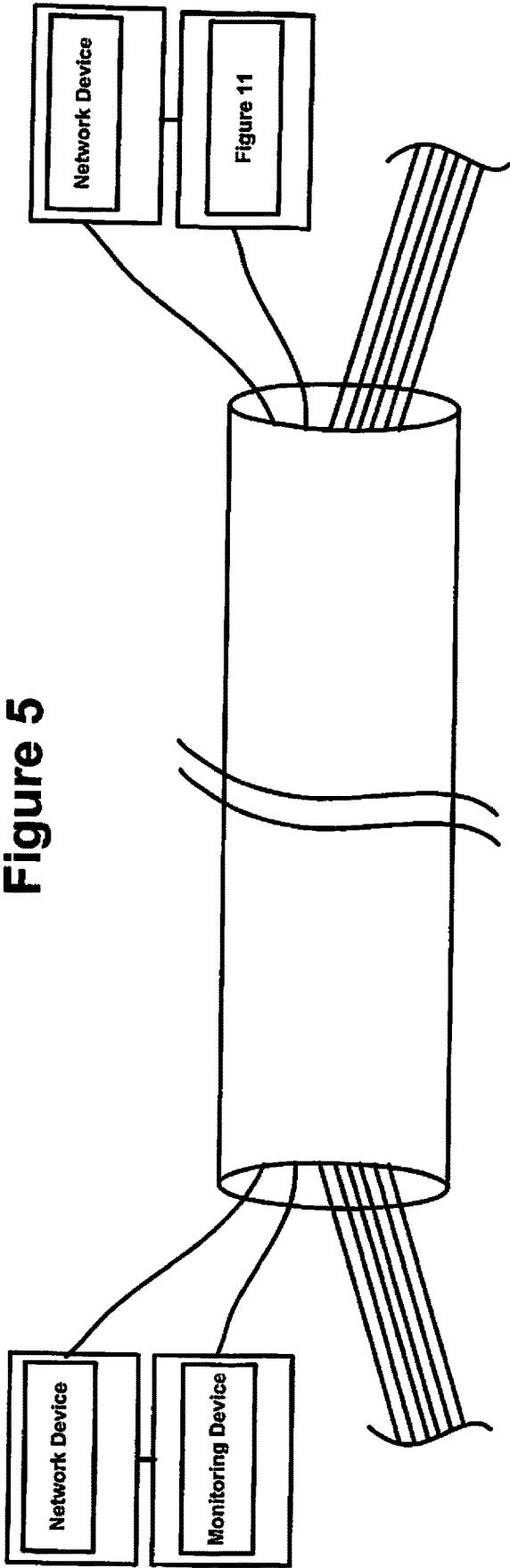


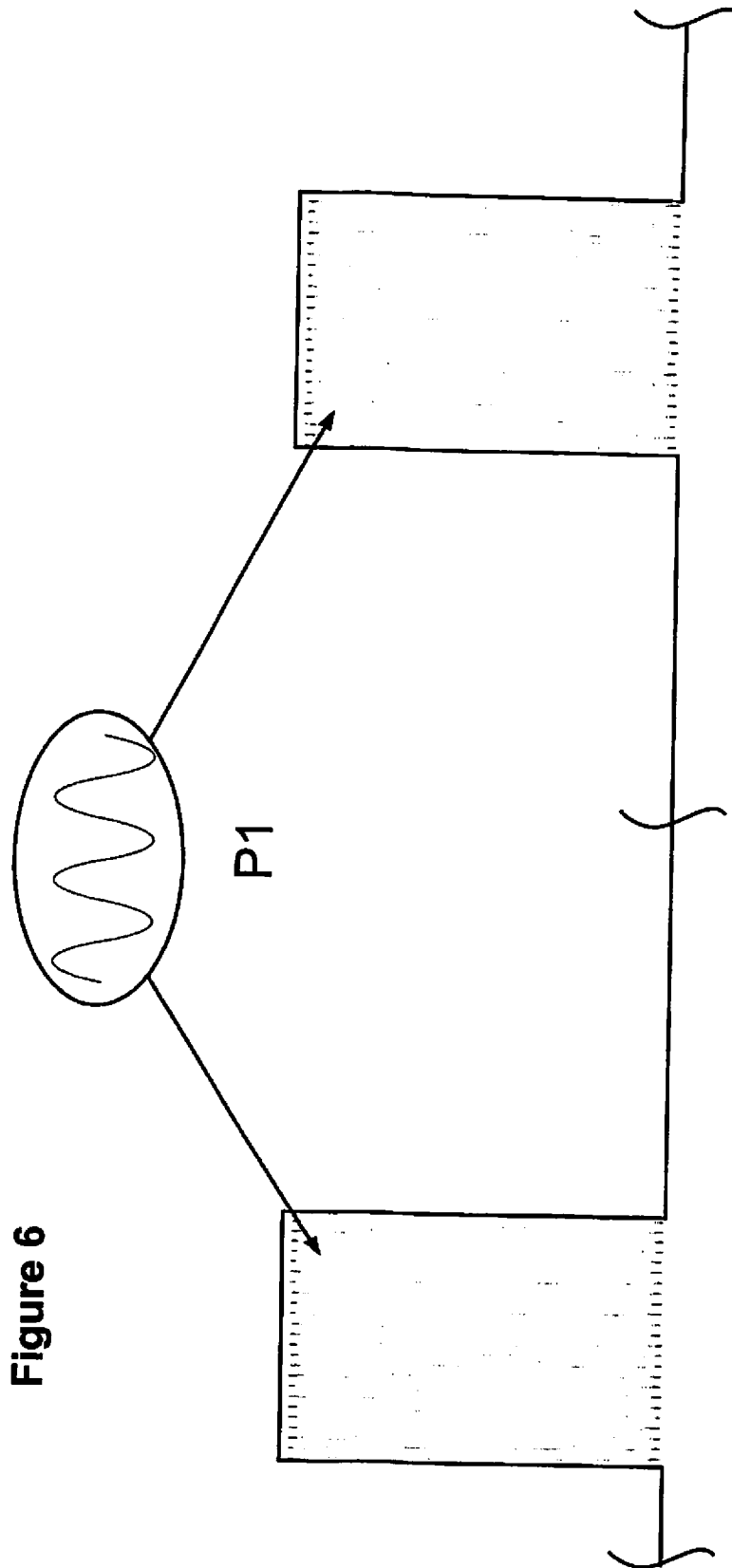
Figure 5

U.S. Patent

Nov. 29, 2022

Sheet 6 of 11

US 11,515,940 B2



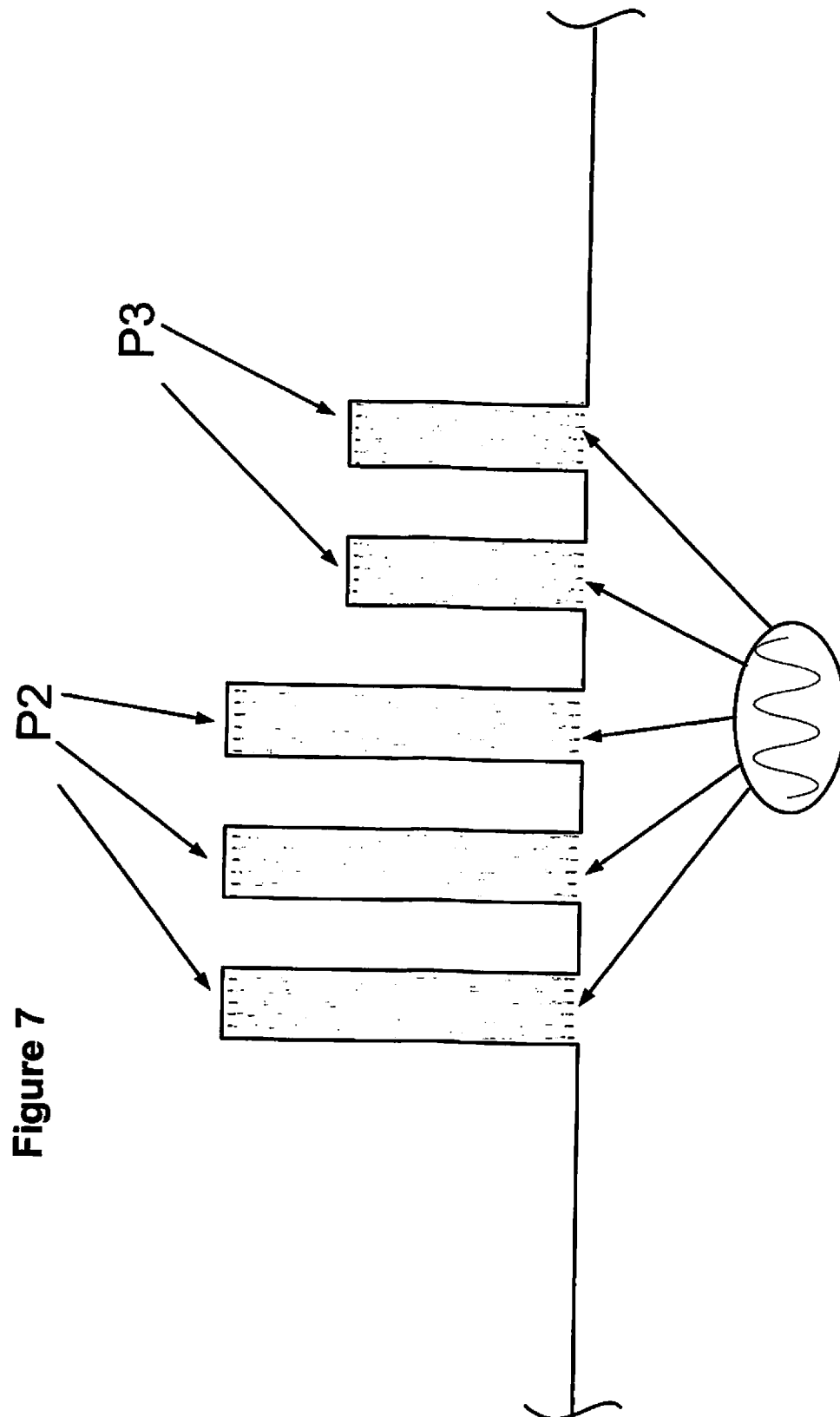
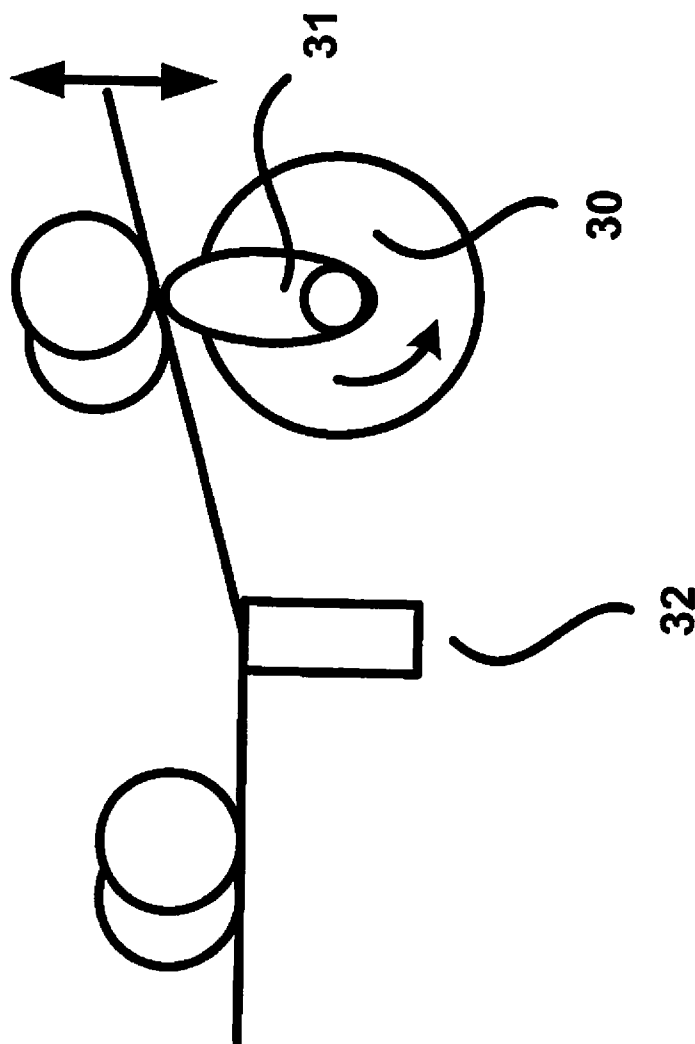


Figure 8



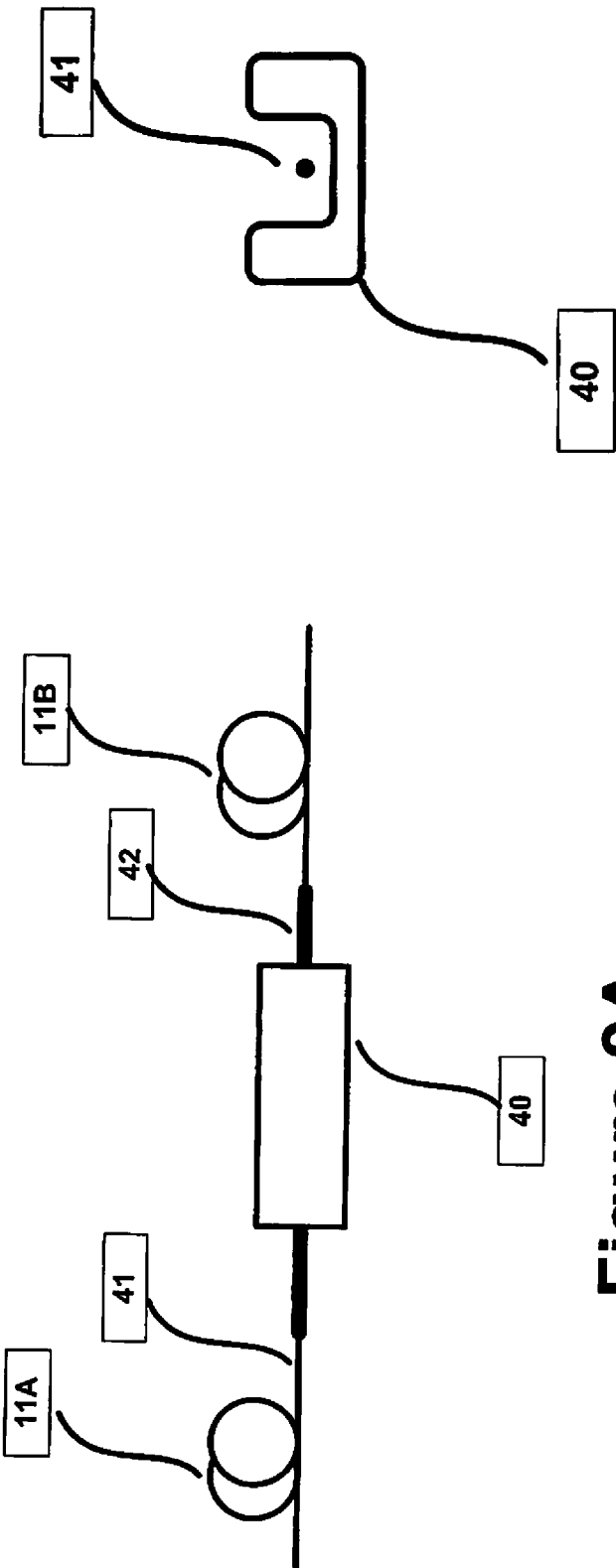


Figure 9A

Figure 9B

Figure 10

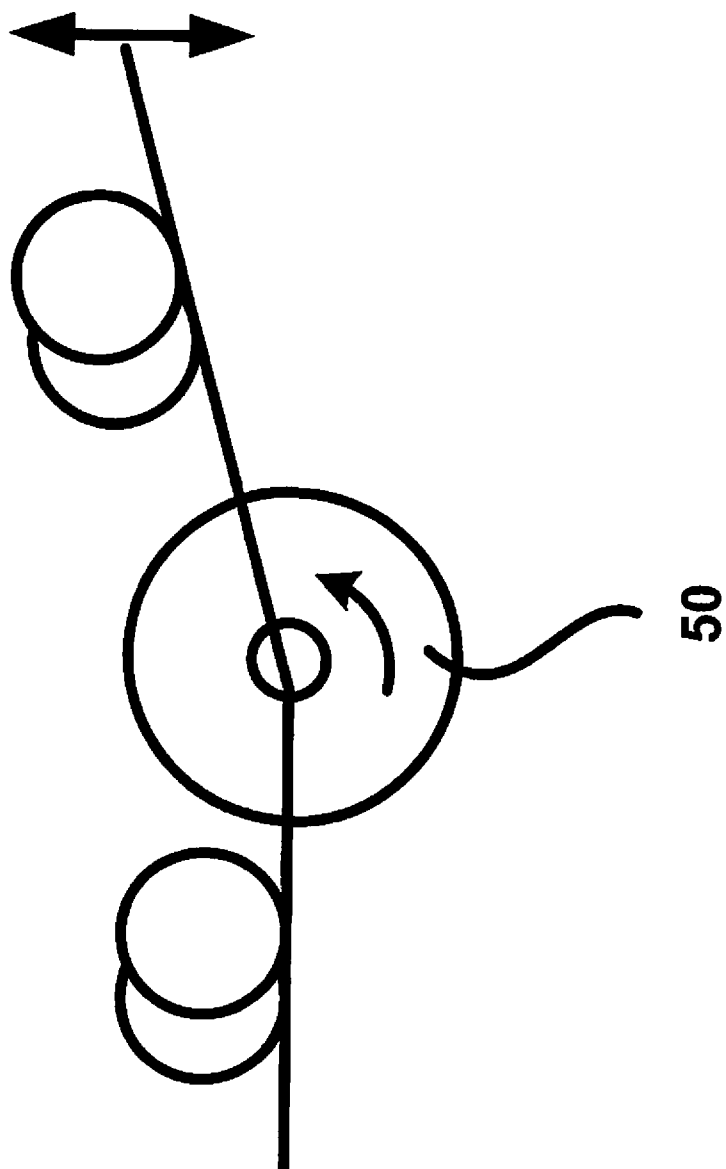
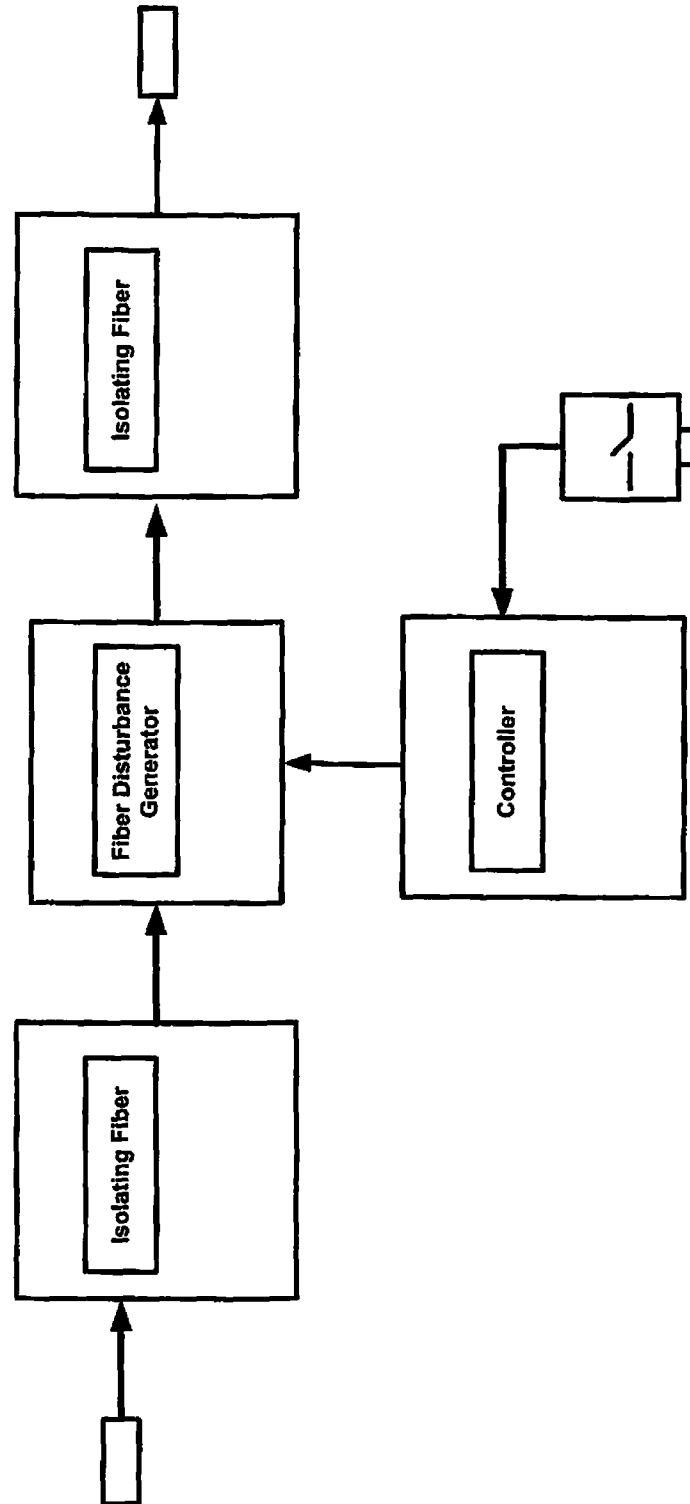


Figure 11



US 11,515,940 B2

1

TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM

This application relates to a test device for periodically, or on demand, checking and verifying proper operation of a monitoring system of an optical fiber.

BACKGROUND OF THE INVENTION

Optical fiber is used for many types of monitoring applications, including but not limited to perimeter security, network security, structural monitoring.

Typically the fiber concerned is monitored using a method which includes transmitting from a source of light at a transmit location a monitor signal along the optical fiber, receiving the monitor signal after transmission along the fiber, analyzing the monitor signal after transmission along the fiber to detect changes therein and generating an alarm in response to the detected changes.

In regard to communications networks, the monitor system is responsive to vibration, motion, or handling of the fiber which are indicative of an intrusion attempt on the fiber.

In addition, the invention herein can be used for fence and buried perimeter protection systems where a fiber is mounted on or at the item to be secured so that again the fiber is monitored for vibration or motion of the fiber caused by attempts to access or penetrate the item concerned.

Yet further, the invention herein can be used for other fibers used for monitoring forces on the fiber caused by strain or other forces that monitor bridge or building integrity. These can include stretching or compression of the fiber. In this case the monitor is not looking for transverse vibration or movement of the fiber from an intrusion attempt or other handling but is instead looking for changes in the character of the fiber caused by the application of the forces to the fiber. Such arrangement can be used in strain gauges, building and bridge monitoring systems and the like.

Additionally, the invention herein can be used to monitor temperature, strain, and pressure using sensors in wells and down-hole applications. Such methods require a looped fiber to accommodate the inability to place equipment in wells or down holes.

Additionally, the invention herein can be used to monitor fibers distributed throughout a so-called 'smart city' type application. In these instances, fibers are distributed to monitor traffic patterns, weather, electrical distribution, and seismic activity.

In all cases the change in the parameter to be measured causes a change in a characteristic in the fiber which can be measured using known techniques.

One method for monitoring a communications network cable is to use fibers that are internal to the protected cable. This so-called "intrinsic monitoring" is shown in U.S. Pat. No. 7,706,641 issued Apr. 27, 2010 to the present applicant, the disclosure of which is incorporated herein by reference.

The optical fibers can be monitored using a variety of detection techniques including:

Modal metric, where changes in a modal power distribution in a multimode fiber are detected as shown in U.S. Pat. No. 7,092,586 issued Aug. 15, 2006 to the present applicant, the disclosure of which is incorporated herein by reference.

Attenuation, where simply an attenuation in the monitoring signal received is measured.

2

Optical Time Domain Reflectometer (OTDR) where reflections or localized attenuations from components of the fiber are detected.

Distributed sensing (DAS/DSS/DTS):

DAS—Distributed Acoustic Sensing where vibrations and displacements cause localized shifts in the path length of the optical fiber. This is detected by a high precision optical Time Domain Reflectometer (OTDR). This OTDR is often referred to as a Phase-OTDR or ϕ -OTDR, and measures changes in the distance between points of Rayleigh backscatter.

DSS—Distributed Strain Sensing—where strain is measured along a fiber due to tensile or compressive displacements, compression, or cracks. Typically measured using Brillouin OTDR, transmitted light and scattered light are mixed as a heterodyne receiver. This Brillouin frequency shift is proportional to strain and temperature in the fiber.

DTS—Distributed Temperature Sensor—where temperature is measured along an optical fiber including by use of Raman OTDR. Light propagating down the fiber at two wavelengths cause Stokes and anti-Stokes light. The amplitude of light reflected back to the detector in a similar fashion to Rayleigh Backscattering in a traditional OTDR, is highly dependent on temperature. The ratio of Stokes and anti-Stokes light indicates temperature, while the round trip transit time indicates location. As with DSS, Brillouin OTDR can also be used to measure distributed temperature.

Polarization monitoring, where changes in a polarization in the signal in a single mode fiber are detected as shown in U.S. Pat. No. 7,142,737 issued Nov. 28, 2006 to the present applicant, the disclosure of which is incorporated herein by reference.

Active fiber monitoring, where monitoring signal and data signal pass on the same fibers as shown in U.S. Pat. No. 7,092,586 issued Aug. 15, 2006 to Vokey et al. and the present applicant, the disclosure of which is incorporated herein by reference.

Strain monitoring such as strain gauge where a Fiber Bragg Grating, strain gauge or DSS monitors a fiber or mechanical structure, disturbance will be stretching or compression

Interferometry such as the Mach-Zehnder interferometers used for network and perimeter monitoring. These may be zone based, or locating by use of bidirectional differential time of flight systems.

Each of these methods of monitoring exploit a specific attribute of the fiber—be it loss, rotation of state of polarization, Rayleigh scattering, or others.

In some cases a single fiber is monitored with typically the transmission at one end and the monitoring at the other or same end. However other arrangements can be used in the present invention including for example the loop type network shown for example in U.S. Pat. No. 7,142,737 issued Nov. 28, 2006 to the present applicant, the disclosure of which is incorporated herein by reference.

Often these systems are placed into service, but continued viability and availability should be verified. Accordingly an intelligent, automatic test is needed that does not interfere with or disrupt the actual performance of the monitoring fiber. The test should exercise the entire system, including perturbation detection, alarm generation, response to alarm, and alarm logging. Thus, it is desirable to create a controlled and characterized event on the monitor fiber structure itself to test the entire system and responses.

US 11,515,940 B2

3

One existing arrangement for this function is provided by the StopLight (trademark) available from CyberSecure IMS. This test is implemented by passing the monitoring fiber in a secure network through an optical shutter that simply shuts off transmission of the light to the fiber. At the appropriate time, scheduled, spontaneous, or random, the optical shutter opens the circuit, causing the monitoring equipment to register an alarm. This method is accepted in the industry, although a shortcoming is that the monitoring is "blind" during this short period of testing. This adds the vulnerability of an inside threat, cognizant of the blind period, which could act to switch the monitored fibers with a substitute fiber or fiber pair. The system owners would then operate under the belief that the system was secure, although in fact it is no longer monitored.

SUMMARY OF THE INVENTION

According to the present invention there is provided a method for verifying operation of an optical fiber monitoring system comprising:

- using a detection system to detect changes in an optical fiber caused by an event to be monitored by:
 - transmitting from a source of light at a transmit location a monitor signal along the optical fiber;
 - receiving the monitor signal after transmission along the fiber;
 - analyzing the monitor signal after transmission along the fiber to detect changes therein caused by the event to be monitored;
 - and generating an alarm in response to said detected changes which are indicative of an event;
- and periodically checking proper operation of the optical fiber monitoring system by:
 - providing a fiber disturbance actuator to cause disturbance of a portion of the fiber at a predetermined location thereon where the disturbance is characteristic of an event to be monitored;
 - periodically operating the fiber disturbance actuator;
 - analyzing the monitor signal to detect changes therein caused by said fiber disturbance actuator;
 - and in the event that expected changes in response to said fiber disturbance actuator are not detected, actuating a warning that the intrusion detection system is not properly operating.

The fiber concerned can be used for transmission of data as a single transmission fiber or as part of a network. Alternatively, the fiber may be used for monitoring movement of or damage to the fiber as part of a perimeter or structure monitoring system where the signal is used to detect the movement or vibrations of the fiber as a part of an intrusion even into the area being monitored.

Preferably the fiber disturbance actuator generates a predetermined pattern of movements which can thus be recognized by a signature associated with the pattern.

Preferably the fiber disturbance actuator generates predetermined periodic displacements to the fiber typically at a predetermined frequency. These displacements can be formed in bursts of a series of spaced envelopes each containing predetermined periodic displacements to the fiber.

Preferably the fiber disturbance actuator generates a modulation frequency which is chosen to be out of band with ambient disturbances.

4

Preferably the fiber disturbance actuator generates a modulation frequency which provides a duty cycle defining the frequency bursts which is chosen to be dissimilar to natural occurrences.

Preferably the method includes analyzing the monitor signal and adjusting a magnitude of disturbance caused by the fiber disturbance actuator in response to the analysis. This will allow the amplitude of the perturbation to be adjusted to be appropriate to the magnitude of the monitor signal so that the amplitude must be high enough to be detected, but not so high as to interfere with the monitor signal processing. The adjustment can be controlled from any of several locations, including over a network from the monitor end of the fiber, or controlled locally such as a local network, manual adjustment, or serial connection.

The amplitude of the test perturbation can be monitored to detect fiber quality as insertion loss changes or the insertion of a fiber optic tap along the fiber.

The arrangement herein thus provides a system for applying a known disturbance or perturbation on a monitor fiber with the intention of being detected by the monitoring system.

This invention excites the fiber under very specific conditions in order to confirm that the fiber, cable, or structure is being monitored as expected.

In a preferred arrangement, the fiber being monitored includes or has connected as a part an input fiber length for isolation from the monitoring device of any connector reflections caused by connection of the fiber disturbance actuator. In many cases this includes also an exit fiber which again acts for isolation purposes. This isolation provided by the inlet and exit fiber portions is particularly important in the systems which rely on reflection techniques where any such reflections can be orders of magnitude greater than the signals to be detected.

This system including the inlet and exit isolation fiber portions is typically connected to a network and is instructed to commence a test. The internal fiber disturbance actuator is engaged in a pre-determined manner, the signal from which is then recognized by the monitoring device, which in turn registers the test as successful and proves that the fiber being monitored is connected and secure.

In a preferred embodiment, where the monitor equipment is of a type that determines location of the movement rather than simply the existence of the movement, the monitoring system acts to look for a specific location and for a specific signal signature. This will not only ensure the invention is still connected to the monitored fiber, and by applying detection to a very specific location on the fiber it ensures that a substitute fiber is not used to bypass the intended monitored cable.

This system satisfies a number of applications:

Under command from a communicating device such as a data network or serial port, the fiber disturbance actuator can be instructed to activate. When this activation is detected by the monitoring device, satisfaction of periodic health check of the monitoring system is satisfied. This test may be in satisfaction of a formal standard, or as good practice as defined by the user.

The fiber disturbance actuator may have a manual trigger such as a push button, causing a test to initiate. This test might occur immediately or after a predetermined or random time, adding confidence to the test.

The fiber disturbance actuator and the control system operating the actuator can in some cases be configured to initiate tests autonomously; where this might be scheduled or random in occurrence.

US 11,515,940 B2

5

The fiber disturbance actuator may be used as a health monitor of the security system. In this embodiment, the control system can initiate a test at a predetermined frequency, verifying the system is functional.

The arrangement can perform periodic connectivity test to confirm the intended fiber is being monitored.

As cited above in U.S. Pat. No. 7,706,641, fiber security products, such as the Interceptor (trademark) product from Network Integrity Systems perform a fiber monitoring function that is zone based. Rather than pinpoint a location, these devices utilize a loop of fiber, and monitor the entire continuous loop as one zone. The arrangement herein is applicable for zone use as well. The fiber disturbance function of the fiber disturbance actuator acts similarly to a location determining product.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing a system of the present invention installed in a fiber to be monitored by inlet and exit isolation fibers.

FIG. 2 is a block diagram showing a system of the present invention installed as a far end connection in a data transmission fiber to be monitored using inlet and exit isolation fibers.

FIG. 3 is a block diagram showing a system of the present invention installed as a near end connection in a data transmission fiber to be monitored using inlet and exit isolation fibers.

FIG. 4 is a block diagram showing a system of the present invention installed as a near end implementation using a separate dedicated monitoring fiber in a data transmission cable.

FIG. 5 is a block diagram showing a system of the present invention installed as a far end implementation using a separate dedicated monitoring fiber in a data transmission cable.

FIGS. 6 and 7 show sample bursts of cyclical disturbances arranged in envelopes which provide a specified signature of period and frequency which allows the monitoring device to identify the applied movements from the fiber disturbance actuator.

FIG. 8 shows schematically one example of a fiber disturbance actuator using a motor for physically moving one part of the fiber relative to another.

FIGS. 9A and 9B show schematically in side and end view respectively one example of a fiber disturbance actuator using an electromagnetic field to physically move a fiber portion which is coated with a material responsive to the field.

FIG. 10 shows schematically one example of a fiber disturbance actuator which uses a motor to bend one portion of the fiber relative to another.

FIG. 11 is a schematic illustration of the operating components which form the elements of the invention for attachment to the fiber to be monitored.

DETAILED DESCRIPTION

As shown in FIG. 1 there is provided a fiber 10 including connector 10A which provides an input from a monitoring device such as a fiber optic security system. An isolating fiber portion 11 including inlet and exit portions 11A, 11B is connected into the fiber 10 and acts to displace the main monitored section of the fiber from the monitoring device. A fiber disturbance generator 12 is mounted in the isolating fiber portion and is controlled by a controller 14. This causes

6

an input disturbance of a predetermined signature and magnitude, as discussed hereinafter, on the portion of the fiber 10 which is being monitored by the monitoring device.

The controller 14, which can be actuated by a switch 15 or by a communications interface 16, from the monitoring system acts for causing the fiber disturbance generator to generate the characteristic disturbance signature with the required magnitude of disturbance.

The communications interface acts to allow the monitor system to initiate a test. The mechanical switch can be used by a system operating person for generating an autonomous test.

In FIG. 3 an installation is provided of the fiber disturbance actuator system including the actuator and the isolation fiber portions at the near end of the fiber is shown. This consists of the system monitor, such as a Distributed Acoustic Sensor interrogator as discussed above. This detects the characteristic disturbance signature introduced by the fiber disturbance generator. As this type of monitoring system is very sensitive to reflections, the isolating fiber isolates the fiber disturbance generator from the reflections caused by the connection to the monitor. Also the isolation fiber portions act to allow recovery from any deadzone effect of the monitor. For example, any monitor utilizing optical time domain reflectometry (OTDR) exhibits a "deadzone" at the front panel, causing it to be blind to events immediately after the connection. The internal isolating fiber eliminates that issue since in effect the dead zone is moved into the isolation fiber area.

The output isolating fiber portion 11B, like the input isolating fiber portion 11A, allows for isolation from the front connector. It also allows the system to be connected bidirectionally. The output of this output fiber portion is connected to the fiber 10 to be protected. The controller section causes the fiber disturbance generator 12 to generate the required signature and amplitude for detection.

The optional external switch 15 can be activated to cause the controller to cause a test to be performed under control of the system operating personnel, that is, without prior instruction from other equipment in the control system.

FIG. 2 shows a version of the invention which is similar to the FIG. 3 with the differentiation that it is intended to be installed at the far end of the fiber, or at any location remote from the near end where power is available. The addition of a communication device 17 connected to a communication medium such as the shown fiber is used to send instructions such as a request for test to the controller and a feedback from the monitor system concerning the amplitude of the disturbances. This has the added benefit of testing the far end of the cable or at a location remote from the near end, which enhances assurance of security.

FIG. 4 illustrates the monitor fiber which intrinsically protects all the fibers in the cable by utilizing a spare fiber in the cable.

FIG. 5 illustrates an embodiment that utilizes a pair of available fibers in a cable: one for monitoring and one for communications between the monitoring device and the near end equipment. This is a preferred embodiment where a system can be installed on spare fibers in a cable adding connectivity assurance as well as health tests and periodic testing to the cable monitor.

FIGS. 6 and 7 show typical patterns P1, P2 and P3 of fiber displacement where the fiber disturbance actuator generates a series of spaced envelopes of signal bursts each containing predetermined periodic displacements to the fiber. In FIG. 7, the frequency of the bursts in the pattern P2 is increased relative to that of FIG. 6 and the period of the bursts is

US 11,515,940 B2

7

decreased. It will be appreciated that various patterns can be generated to create a signature pattern to be detected by the monitoring system. Preferably the frequency of the pulses is chosen to be out of band with ambient disturbances. Preferably the modulation frequency provides a duty cycle defining the frequency bursts which is chosen to be dissimilar to natural occurrences which can be expected from machine learning so that the signature pattern can be readily determined during the test process. This can include repetitive duty cycle such as 50:50. The duty cycle defining the frequency bursts may be a complex keyed code for security. This can be changed periodically, randomly, on a scheduled basis, or triggered by a coded or uncoded message or by detectable amplitude changes to the envelope as shown in pattern P3.

In FIG. 7 the last pulses in pattern P3 are shown at reduced amplitude which is determined by analysis of the received monitoring signals so that the amplitude matches a requirement to provide signals which are large enough to be identified and not so large that they interfere with the normal monitoring process by having changes which are beyond those which are expected and are measurable.

When used for near end applications, system can be implemented with only the first isolation fiber, which is provided between the monitoring device and actuator device.

When used for the far end application, system is implemented with both input and output fibers as a method for isolating the actuator signal from reflections.

The system with input and output fiber spools can be used either near end or far end, and is bidirectional in that it can be optically connected in either direction.

It will be appreciated that the type of disturbance used by the system actuator is selected to match the technology of the monitoring device; thus for example:

In a modal metric detection system, the actuator typically uses a disturbance device which acts to bend or physical move a portion of the fiber.

In an attenuation detection system, the actuator typically uses a disturbance device which acts to bend the fiber.

In an Optical Time Domain Reflectometer detection system, the actuator typically uses a disturbance device which acts to bend the fiber.

In a Distributed sensing (DAS/DSS/DTS) detection system, the actuator typically uses a disturbance device which acts to create changes in the monitor signal which can be detected by this type of monitoring system.

In a Distributed Acoustic Sensing (DAS) detection system, the actuator typically uses a disturbance device which acts to move the fiber in a shaking or vibrating action.

In a Strain monitoring system such as strain gauge detection system or a Distributed Strain Sensing system (DSS), the actuator 12 shown in FIG. 1 typically uses a disturbance device which acts to stretch or compress the fiber.

In a Distributed Temperature Sensing (DTS) detection system, the actuator 12 in FIG. 1 typically uses a disturbance device which acts to heat or cool the fiber.

In a Polarization detection system, the actuator typically uses a disturbance device which acts to bend or shake the fiber, or mechanically rotate the state of polarization such as by moving, shaking, or vibrating paddles which introduce birefringence by changing stress on the fiber by way of bending or rotating.

In an Interferometry detection system, the actuator typically uses a disturbance device which acts to bend or shake the fiber.

8

As an alternative an active area of actuator can contain a fiber Bragg grating, in which the actuator acts to heat, bend, or stretch the grating.

The communications interface may contain a dual wavelength/single fiber ethernet connection 16A. When used with a single fiber monitor, a two fiber solution will protect a cable. When installing optical cables, it is common practice to install cables with more fiber than is needed for the immediate or foreseeable future. As the bulk of the price of an installation is labor, and the price difference when upgrading the fiber count is incremental, unused (called "dark") fiber are often available. As networks most often utilize 2 fibers each, one for transmit and one for receive, and as fiber count in cables is typically an even number, often a multiple of 6 or 12, there are often pairs of optical fibers that are available for use. Single fiber monitoring systems, such as DAS, will utilize one fiber in a pair while leaving the other available for communication. Single fiber communications standards, such as Ethernet, provide full duplex communication over a single fiber by transmitting one wavelength, such as 1310 nm, in one direction, and another wavelength such as 1550 nm in the opposite direction. Combining the single fiber monitoring with the single fiber communication provides a complete instance of this invention on a pair of fibers. Single fiber communications solutions can also be achieved by techniques such as differing modulation frequencies, states of polarizations, time division multiplexing, and others.

Similarly, the communications might be realized by use of multiple fibers, such as two. Monitoring and communications functions can be performed over the same fiber pair(s) by use of wavelength division multiplexing, time division multiplexing, or other multiplexing schemes.

Zone based non-locating monitoring methods are often implemented over two fibers, or a fiber loop. Use of multiplexing methods such as wavelength division multiplexing, time division multiplexing, or other multiplexing schemes can be utilized to share the fibers between the monitoring and the communication systems.

CW detecting monitoring devices, such as zone type network or perimeter protection devices can detect the frequency with a frequency detecting method.

This method can be a hardware phase locked loop within the receiver circuitry of the monitoring equipment. In this embodiment, a disturbance of known frequency is generated while frequency detection equipment such as a phase locked loop is used for detection, which registers a successful test.

This method can be a software phase locked loop. Similar to the hardware phase locked loop within the receiver circuitry of the monitoring equipment, a detection algorithm is used within the signal processing software. In this embodiment, a disturbance of known frequency is generated while frequency detection algorithm emulating a phase locked loop is used for detection, which registers a successful test.

This method can be bandpass filters. Similar to the hardware phase locked loop within the receiver circuitry of the monitoring equipment, a hardware or software frequency filter can suppress all frequencies except that of the disturbance generator. In this embodiment, a disturbance of known frequency is generated while detection equipment detects the signal passed through the bandpass filter, which registers a successful test.

This method can be Fourier Transforms. The spectra of a received signal can be inspected for the presence of the disturbance frequency. In this embodiment, a disturbance of known frequency is generated while detection equipment

US 11,515,940 B2

9

detects the signal as a spectral spike of sufficient amplitude, which registers a successful test.

This method can be correlation, including Wavelet Transforms. The spectra of a received signal can be inspected for the presence of the disturbance frequency. In this embodiment, a disturbance consisting of a pulse, chirp, wavelet, or other finite signal of known composition is generated while detection equipment detects the signal and applies correlation or Wavelet Transform to detect the presence of the disturbance, which registers a successful test.

Zone based products may multiplex communication signal and monitor signal on the same fiber pair by using wavelength division multiplexers. Zone based systems may be configured for single mode or multimode fiber.

A system as described, but used for zone-based non-location determining systems, can omit the internal isolations fiber portions as reflections and dead zones are not of concern.

For vibration sensing monitoring sensors, the active device disturbing the fiber within the disturbance generator may be of several technologies, including but not limited to:

Electromagnetic actuators which cause displacement by energizing a coil or other electromagnetic device. This might include attaching a fiber to a moving portion of a voice coil

As Electromagnetic actuators which cause displacement by coating by depositing or other technique a sensitive material to the fiber and placing it within the field with no other moving parts.

The fiber disturbance device 12 shown in FIG. 1 can use a Piezo-electric actuator attached to the fiber and causing the vibration

The fiber disturbance device 12 shown in FIG. 1 can use a Haptic actuator such as the rotating motor type Mechanical such as rotating cam or sawtooth

The fiber disturbance device 12 shown in FIG. 1 can use an arrangement where the fiber is displaced by placing it between stators within an electrostatic field, and varying the field to displace the fiber Variable optical attenuator: perturbation is a variation in optical signal amplitude

Variable polarization controller: perturbation is variation in optical signal polarization

Variable optical mode mixing: use a mode mixer to change modal fill of optical signal in MMF fiber, causing a perceived perturbation in our products

In the described system, a fiber Bragg grating may be used within the disturbance generator. When perturbed, detectable wavelength shifts are detected.

In systems that determine distance or location, the detection signature should occur at a predetermined location, representative of the installation. This precise location thwarts attempts to spoof the system by bypassing with a separate fiber. This attempted spoofing might, at the fiber patch panel or other convenient locations, replace the connections to the monitored cable with a fiber. Requiring a precise fiber length and event location significantly eliminates that ability.

The disturbance repetition rate, frequency, or combination of these and other parameters may be arranged to be representative of a unique key.

The system may be placed at the beginning, end, or any location along the path of the fiber where electrical power is available.

10

The device is preferably arranged to produce a heartbeat at a configurable, identifiable frequency and cadence that the monitoring interrogator can reliably interpret as a unique event.

When operating in periodic mode the device can be configured with a cryptographic key to communicate time based one-time passwords (TOTP) during tests. This can be used to prove the identity of the test device to the sensing device. The password can be encoded by the content of the test signal. The password can be encoded by the timing of the test. In this way, devices operating in the above time based one-time password mode can be used not just for testing the sensing system, but for providing evidence that that sensing cable has not been bypassed. Devices operating in periodic mode only without network access may be battery powered.

The disturbance Generator will have an adjustable magnitude which will allow perturbation to be adjusted to be appropriate to the magnitude of the monitor signal. The amplitude must be high enough to be detected, but not so high as to interfere with signal processing. This may be controlled from any of several locations, including over a network from the monitor end of the fiber, or controlled locally such as a local network, manual adjustment, or serial connection.

FIG. 8 shows schematically one example of a fiber disturbance actuator using a motor 30 operating a rotating cam 31 for moving one part of the fiber relative to another part which is held fixed by an anchor 32.

FIGS. 9A and 9B show schematically one example of a fiber disturbance actuator using an electromagnetic field generator 40 to physically move a fiber portion 41 which is coated with a material 42 responsive to the field.

FIG. 10 shows schematically one example of a fiber disturbance actuator which uses a motor 50 to bend one portion of the fiber relative to another.

FIG. 11 shows schematically the components herein. Switch 18 represents a mechanical input device which, when actuated, initiates a test or a sequence that leads to the performance of a test. This can also represent other types of interfaces such as contact closures and/or other interfaces to allow the test device to send notifications when certain activities happen in and around the device; i.e. door closures or equipment cabinet openings. Signatures generated by the test device can communicate notifications of inputs at the test device, and report to the monitoring device.

The invention claimed is:

1. A method for verifying operation of an optical fiber monitoring system comprising:
 using a detection system to detect changes in an optical fiber caused by an event to be monitored by:
 transmitting from a source of light at a transmit location a monitor signal along the optical fiber;
 receiving the monitor signal after transmission along the optical fiber;
 analyzing the monitor signal after transmission along the optical fiber to detect changes therein caused by the event to be monitored;
 and generating an alarm in response to said detected changes which are indicative of the event;
 and repeatedly checking proper operation of the optical fiber monitoring system by:
 providing a fiber disturbance actuator to cause at least one disturbance of a portion of the optical fiber at a predetermined location thereon;
 repeatedly operating the fiber disturbance actuator;

US 11,515,940 B2

11

wherein the fiber disturbance actuator is arranged to produce said at least one disturbance at a configurable, identifiable frequency and cadence which provides a recognizable signature;

analyzing the monitor signal to detect changes therein caused by said fiber disturbance actuator; 5
and when expected changes in response to said at least one disturbance having said recognizable signature from said fiber disturbance actuator are not detected, actuating a warning that the detection system is not properly operating. 10

2. The method according to claim 1 wherein the fiber disturbance actuator generates a predetermined pattern of disturbances of said at least one disturbance. 15

3. The method according to claim 1 wherein the fiber disturbance actuator generates disturbances of said at least one disturbance at a predetermined frequency.

4. The method according to claim 1 wherein the fiber disturbance actuator generates a series of spaced envelopes each containing disturbances of said at least one disturbance. 20

5. The method according to claim 1 wherein the fiber disturbance actuator generates a pattern of disturbances of said at least one disturbance defining said recognizable signature. 25

6. A method for verifying operation of an optical fiber monitoring system comprising:

using a detection system to detect changes in an optical fiber caused by an event to be monitored by:

transmitting from a source of light at a transmit location a monitor signal along the optical fiber; 30
receiving the monitor signal after transmission along the optical fiber;

analyzing the monitor signal after transmission along the optical fiber to detect changes therein caused by the event to be monitored; 35

and generating an alarm in response to said detected changes which are indicative of the event;

and repeatedly checking proper operation of the optical fiber monitoring system by: 40

providing a fiber disturbance actuator to cause at least one disturbance of a portion of the optical fiber at a predetermined location thereon where said at least one disturbance is characteristic of the event to be monitored; 45

repeatedly operating the fiber disturbance actuator; analyzing the monitor signal to detect changes therein caused by said fiber disturbance actuator;

and when expected changes in response to said fiber disturbance actuator are not detected, actuating a warning that the detection system is not properly operating. 50

wherein the fiber disturbance actuator generates disturbances of said at least one disturbance at a modulation frequency which is chosen to be out of band with ambient disturbances. 55

7. A method for verifying operation of an optical fiber monitoring system comprising:

using a detection system to detect changes in an optical fiber caused by an event to be monitored by: 60

transmitting from a source of light at a transmit location a monitor signal along the optical fiber; receiving the monitor signal after transmission along the optical fiber;

analyzing the monitor signal after transmission along the optical fiber to detect changes therein caused by the event to be monitored; 65

12

and generating an alarm in response to said detected changes which are indicative of the event; and repeatedly checking proper operation of the optical fiber monitoring system by:

providing a fiber disturbance actuator to cause at least one disturbance of a portion of the optical fiber at a predetermined location thereon where said at least one disturbance is characteristic of the event to be monitored;

repeatedly operating the fiber disturbance actuator; analyzing the monitor signal to detect changes therein caused by said fiber disturbance actuator;

and when expected changes in response to said fiber disturbance actuator are not detected, actuating a warning that the detection system is not properly operating;

wherein the fiber disturbance actuator generates disturbances of said at least one disturbance at a modulation frequency which provides a duty cycle defining frequency bursts which is chosen to be dissimilar to natural occurrences.

8. The method according to claim 1 including analyzing the monitor signal and adjusting a magnitude of said disturbances of said at least one disturbance caused by the fiber disturbance actuator in response thereto.

9. A method for verifying operation of an optical fiber monitoring system comprising:

using a detection system to detect changes in an optical fiber caused by an event to be monitored by:

transmitting from a source of light at a transmit location a monitor signal along the optical fiber; receiving the monitor signal after transmission along the optical fiber;

analyzing the monitor signal after transmission along the optical fiber to detect changes therein caused by the event to be monitored;

and generating an alarm in response to said detected changes which are indicative of the event;

and repeatedly checking proper operation of the optical fiber monitoring system by:

providing a fiber disturbance actuator to cause at least one disturbance of a portion of the optical fiber at a predetermined location thereon where said at least one disturbance is characteristic of the event to be monitored;

repeatedly operating the fiber disturbance actuator; analyzing the monitor signal to detect changes therein caused by said fiber disturbance actuator;

and when expected changes in response to said fiber disturbance actuator are not detected, actuating a warning that the detection system is not properly operating,

wherein the optical fiber includes an input fiber length isolating the fiber disturbance actuator from the detection system.

10. The method according to claim 9 wherein the input fiber length is used for near end applications.

11. The method according to claim 9 wherein there is provided an output isolating fiber which isolates a front connector and a main portion of the optical fiber from the input fiber length.

12. The method according to claim 11 wherein the output isolating fiber connects the fiber disturbance actuator to the main portion of the optical fiber bidirectionally.

13. The method according to claim 1 wherein the detection system determines location of the event on the optical

US 11,515,940 B2

13

fiber and wherein the monitor signal is analyzed to determine a specific location on the optical fiber of the fiber disturbance actuator.

14. The method according to claim 13 wherein the determination of the specific location ensures that the fiber disturbance actuator is still connected to the optical fiber, and that a substitute optical fiber is not used to bypass the optical fiber. 5

15. The method according to claim 1 wherein a communicating device is provided for causing operation of the fiber disturbance actuator. 10

16. The method according to claim 1 wherein a manual trigger is provided for causing operation of the fiber disturbance actuator where the manual trigger causes the operation immediately or after a predetermined or random time. 15

17. The method according to claim 1 wherein operation of the fiber disturbance actuator is caused autonomously; where the operation can be scheduled or random in occurrence.

18. The method according to claim 1 wherein a communications interface communicates with the fiber disturbance actuator using a dual wavelength/single fiber ethernet connection. 20

19. The method according to claim 1 wherein the detection system comprises a zone network or a perimeter protection device which detects the frequency with a frequency detecting method. 25

20. The method according to claim 1 wherein the fiber disturbance actuator operates to cause said disturbances of said at least one disturbance of the optical fiber by any one or more of bending, shaking, heating, cooling, compressing or stretching the optical fiber. 30

21. A method for verifying operation of an optical fiber monitoring system comprising:

using an detection system to detect changes in an optical fiber caused by an event to be monitored by: 35

transmitting from a source of light at a transmit location a monitor signal along the optical fiber;

receiving the monitor signal after transmission along the optical fiber; 40

analyzing the monitor signal after transmission along the optical fiber to detect changes therein caused by the event to be monitored;

14

and generating an alarm in response to said detected changes which are indicative of the event;

and repeatedly checking proper operation of the optical fiber monitoring system by:

providing a fiber disturbance actuator to cause at least one disturbance of a portion of the optical fiber at a predetermined location thereon where said at least one disturbance is characteristic of the event to be monitored;

repeatedly operating the fiber disturbance actuator;

analyzing the monitor signal to detect changes therein caused by said fiber disturbance actuator;

and when expected changes in response to said fiber disturbance actuator are not detected, actuating a warning that the detection system is not properly operating;

wherein the fiber disturbance actuator operates to cause said at least one disturbance by physical movement of the portion of the fiber by energizing an electromagnetic device.

22. The method according to claim 21 wherein the fiber disturbance actuator operates to cause said at least one disturbance by physical movement of the optical fiber by coating a sensitive material to the portion of the optical fiber and placing it within a field.

23. The method according to claim 21 wherein the fiber disturbance actuator is arranged to produce said at least one disturbance of said portion of the optical fiber by any one or more of bending, shaking, compressing or stretching the portion of the optical fiber.

24. The method according to claim 21 wherein a recognizable signature is applied to the fiber by the fiber disturbance actuator by varying a disturbance repetition rate, a disturbance frequency, or combination of these.

25. The method according to claim 21 wherein the fiber disturbance actuator has a manual trigger.

26. The method according to claim 21 wherein the fiber disturbance actuator is actuated by a self-initiate test at a scheduled or random time.

* * * * *

Exhibit 2

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

(10) **Patent No.:** **US 11,388,181 B2**

(45) **Date of Patent:** **Jul. 12, 2022**

(54) **CABLE ASSEMBLY DISTURBANCE
DETECTION METHOD**

(71) Applicant: **CyberSecure IPS, LLC**, Upper
Marlboro, MD (US)

(72) Inventors: **Bobby Nakanelua**, Elizabethtown, KY
(US); **Stephen Sohn**, Cummings, GA
(US); **Scott Rye**, La Plata, MD (US)

(73) Assignee: **CyberSecure IPS, LLC**, Upper
Marlboro, MD (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 0 days.

(21) Appl. No.: **17/146,214**

(22) Filed: **Jan. 11, 2021**

(65) **Prior Publication Data**

US 2021/0136093 A1 May 6, 2021

Related U.S. Application Data

(63) Continuation of application No. 16/860,789, filed on
Apr. 28, 2020, now Pat. No. 10,893,062, which is a
(Continued)

(51) **Int. Cl.**
H04L 9/40 (2022.01)
H04L 43/16 (2022.01)
(Continued)

(52) **U.S. Cl.**
CPC **H04L 63/1416** (2013.01); **G08B 13/186**
(2013.01); **H04L 41/22** (2013.01);
(Continued)

(58) **Field of Classification Search**

CPC H04L 63/1416; H04L 63/1425; H04L
63/1408; H04L 63/1433; H04L 41/22;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,735,353 A 5/1973 Donovan et al.
3,942,859 A 3/1976 Korodi
(Continued)

OTHER PUBLICATIONS

Notice of Allowance issued in corresponding U.S. Appl. No. 16/860,789
dated Sep. 8, 2020 (10 pages).

(Continued)

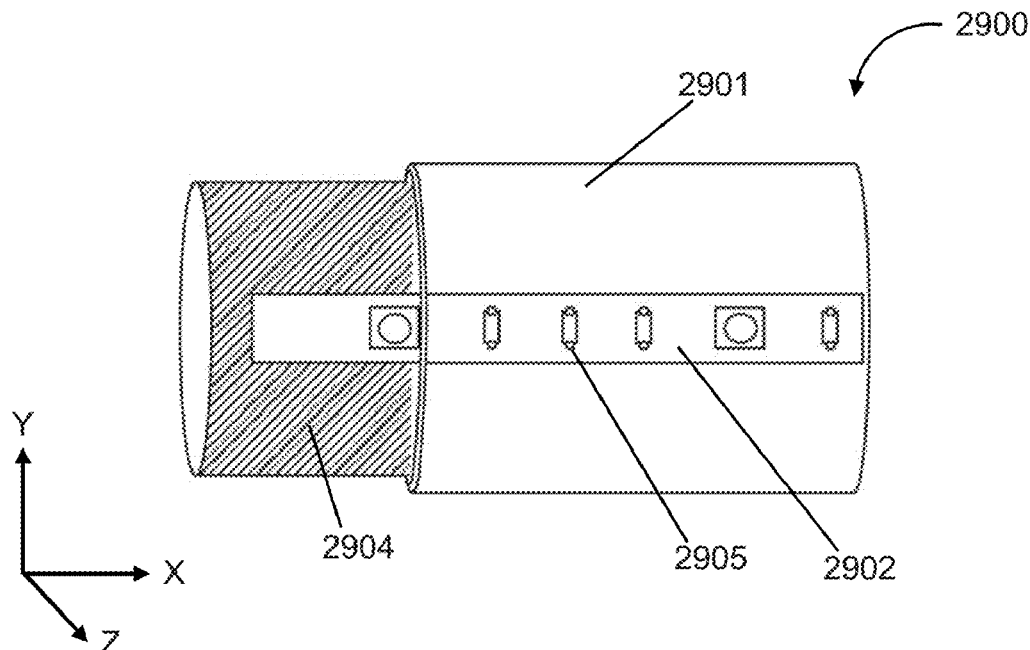
Primary Examiner — Andrew Jordan

(74) *Attorney, Agent, or Firm* — Perkins Coie LLP

(57) **ABSTRACT**

In some embodiments, a cable assembly may include an outer jacket, a printer circuit board including light emitting diodes, and a cable configured to transmit information. In some embodiments, the outer jacket may include a channel opening and the printed circuit board may be configured to be positioned within the channel opening and between the cable and the outer jacket. In some embodiments, the cable assembly may include an inner jacket, an outer jacket, a printed circuit board including light emitting diodes, and a cable configured to transmit information. The inner jacket may include a channel opening, and the printer circuit board may be configured to be positioned within the channel opening and between the inner jacket and the outer jacket.

20 Claims, 34 Drawing Sheets



US 11,388,181 B2

Page 2

Related U.S. Application Data

- continuation of application No. 16/008,729, filed on Jun. 14, 2018, now Pat. No. 10,652,253, which is a continuation of application No. 15/246,635, filed on Aug. 25, 2016, now abandoned, which is a continuation of application No. 14/849,746, filed on Sep. 10, 2015, now Pat. No. 9,455,999, which is a continuation of application No. 14/217,259, filed on Mar. 17, 2014, now Pat. No. 9,160,758.
- (60) Provisional application No. 62/554,912, filed on Sep. 6, 2017, provisional application No. 61/786,460, filed on Mar. 15, 2013.

(51) Int. Cl.

H04L 43/0864 (2022.01)
H04L 41/22 (2022.01)
G08B 13/186 (2006.01)
H04L 41/0213 (2022.01)
H04L 67/12 (2022.01)

(52) U.S. Cl.

CPC **H04L 43/0864** (2013.01); **H04L 43/16** (2013.01); **H04L 63/1425** (2013.01); **H04L 41/0213** (2013.01); **H04L 63/1408** (2013.01); **H04L 63/1433** (2013.01); **H04L 67/12** (2013.01)

(58) Field of Classification Search

CPC . H04L 41/0213; H04L 43/0864; H04L 43/16;
H04L 67/12; G08B 13/186
See application file for complete search history.

(56)

References Cited

U.S. PATENT DOCUMENTS

4,538,140 A 8/1985 Prestel
4,673,935 A 6/1987 Spencer
5,194,847 A 3/1993 Taylor et al.
5,355,208 A 10/1994 Crawford
5,680,104 A 10/1997 Siemon
6,288,640 B1 9/2001 Gagnon
6,421,632 B1 7/2002 LeCorney
6,577,794 B1 6/2003 Currie
6,775,657 B1 8/2004 Baker
6,819,849 B1 11/2004 Tangonan et al.
6,974,239 B2 12/2005 Currie
6,980,108 B1 12/2005 Gebbia et al.
7,092,586 B2 8/2006 Vokey et al.
7,292,758 B2 11/2007 Bayindir
7,293,238 B1 11/2007 Brook
7,356,585 B1 4/2008 Brook
7,403,674 B2 7/2008 Murphy et al.
8,135,278 B2 3/2012 Lee et al.
8,165,723 B2 4/2012 Nasle
8,355,406 B1 1/2013 Shimamoto
8,670,111 B1 3/2014 Brown
8,909,013 B1 12/2014 Jiang
8,947,232 B2 2/2015 Strong et al.

9,160,758 B2 10/2015 Sohn
9,455,999 B2 9/2016 Sohn
9,628,502 B2 4/2017 Clark
10,379,309 B2 8/2019 Bauco
2002/0066034 A1 5/2002 Schlossberg
2006/0031446 A1 2/2006 Hamedi
2006/0103835 A1 5/2006 Artsyukhovich
2006/0153491 A1 7/2006 Murphy
2007/0071393 A1 3/2007 Robertson
2007/0253662 A1 11/2007 Patel et al.
2007/0280591 A1 12/2007 Nelson
2008/0025229 A1 1/2008 Beliles
2009/0031426 A1 1/2009 Dal Lago et al.
2009/0040046 A1 2/2009 Browning, Jr. et al.
2009/0208212 A1 8/2009 Lee
2010/0091676 A1 4/2010 Moran et al.
2010/0117830 A1 5/2010 Strong et al.
2010/0209047 A1 8/2010 Cheung et al.
2011/0241881 A1 10/2011 Badinelli
2013/0312092 A1 11/2013 Parker
2013/0322490 A1 12/2013 Bell
2013/0335219 A1 12/2013 Malkowski
2014/0056582 A1 2/2014 Roberts
2014/0091929 A1 4/2014 Murphy et al.
2014/0109182 A1 4/2014 Smith
2014/0167952 A1 6/2014 Zhevelev
2014/0283074 A1 9/2014 Sohn
2015/0358345 A1 12/2015 Clark
2015/0381640 A1 12/2015 Sohn
2016/0139353 A1 5/2016 Bauco
2016/0330225 A1 11/2016 Kroyzer
2016/0366163 A1 12/2016 Sohn
2017/0295031 A1 10/2017 Bush
2018/0302420 A1 10/2018 Nakanelua
2018/0324194 A1 11/2018 Nakanelua
2019/0373856 A1* 12/2019 Eidus A01K 15/021
2021/0136093 A1* 5/2021 Nakanelua H04L 63/1425

OTHER PUBLICATIONS

International Search Report and Written Opinion dated Aug. 28, 2014 for Appln. No. PCT/US14/30330.
Virgil, "An Evaluation of Fiber Optic Intrusion Detection Systems in Interior Applications," Mar. 1994, pp. 1-46.
Mahmoud, "Nuisance Alarm Suppression Techniques for Fibre-Optic Intrusion Detection Systems," Third Asia Pacific Optical Sensors Conference, 2012, pp. 1-8.
NSTISS, "Protective Distribution Systems," Dec. 13, 1996, pp. 1-13.
Accu-tech Guardian, retrieved from <https://web.archive.org/web/20121115040632/http://www.accu-tech.com/protected-distribution-system/>, Nov. 15, 2012, pp. 1-4.
Alcon-Tech iSPY Fiber Optic Intrusion Detection System Data Sheet, retrieved from <http://www.alcon-tech.com/pdf/iSPY.pdf>, Jun. 2006, pp. 1-5.
Allwood, Fibre Optic Acoustic Sensing for Intrusion Detection Systems, Edith Cowan University, Research Online, ECU Publications 2011, pp. 1-7.
International Preliminary Report on Patentability dated Sep. 15, 2015 for Appln. No. PCT/US2014/030330.

* cited by examiner

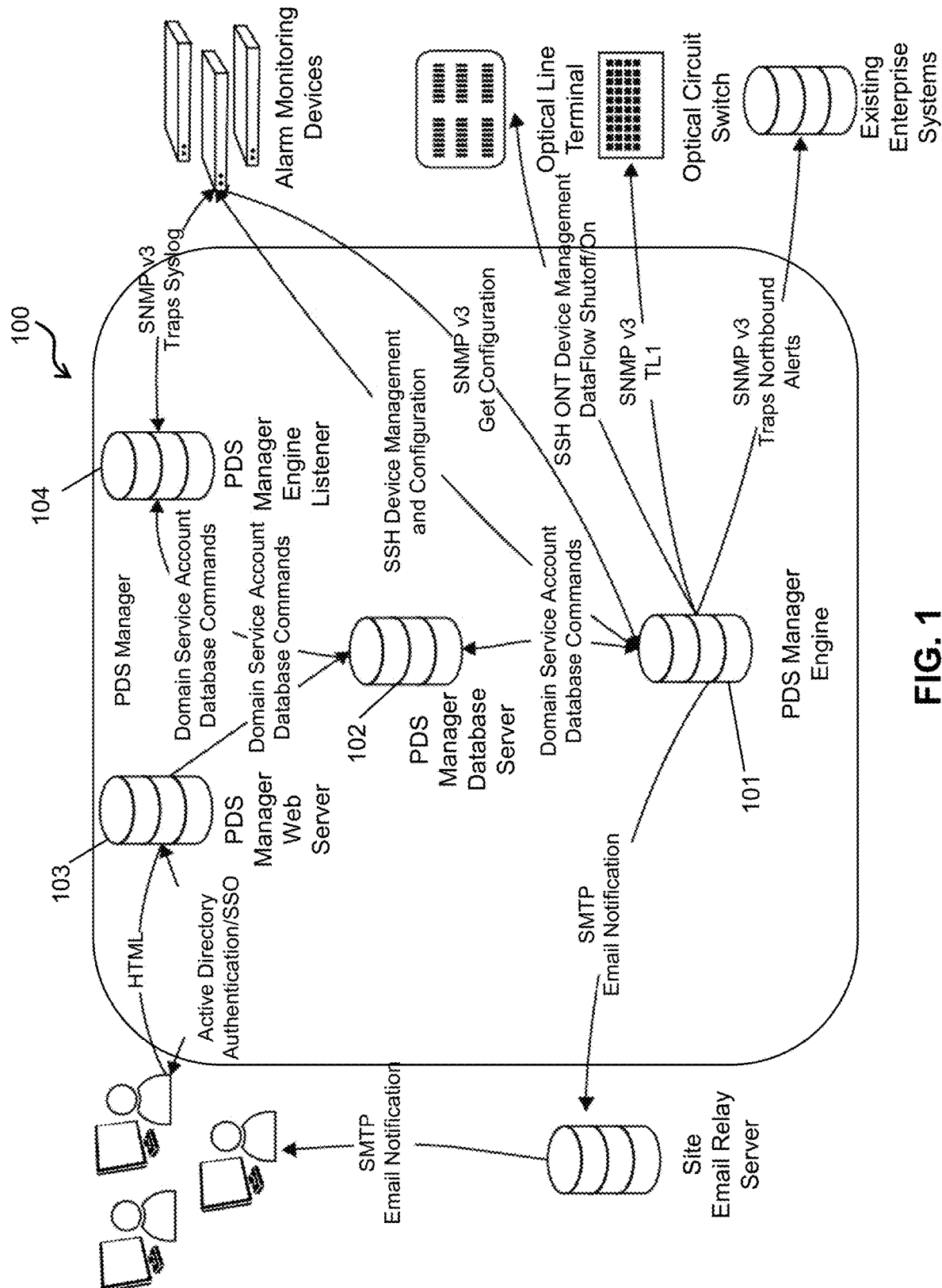


FIG. 1

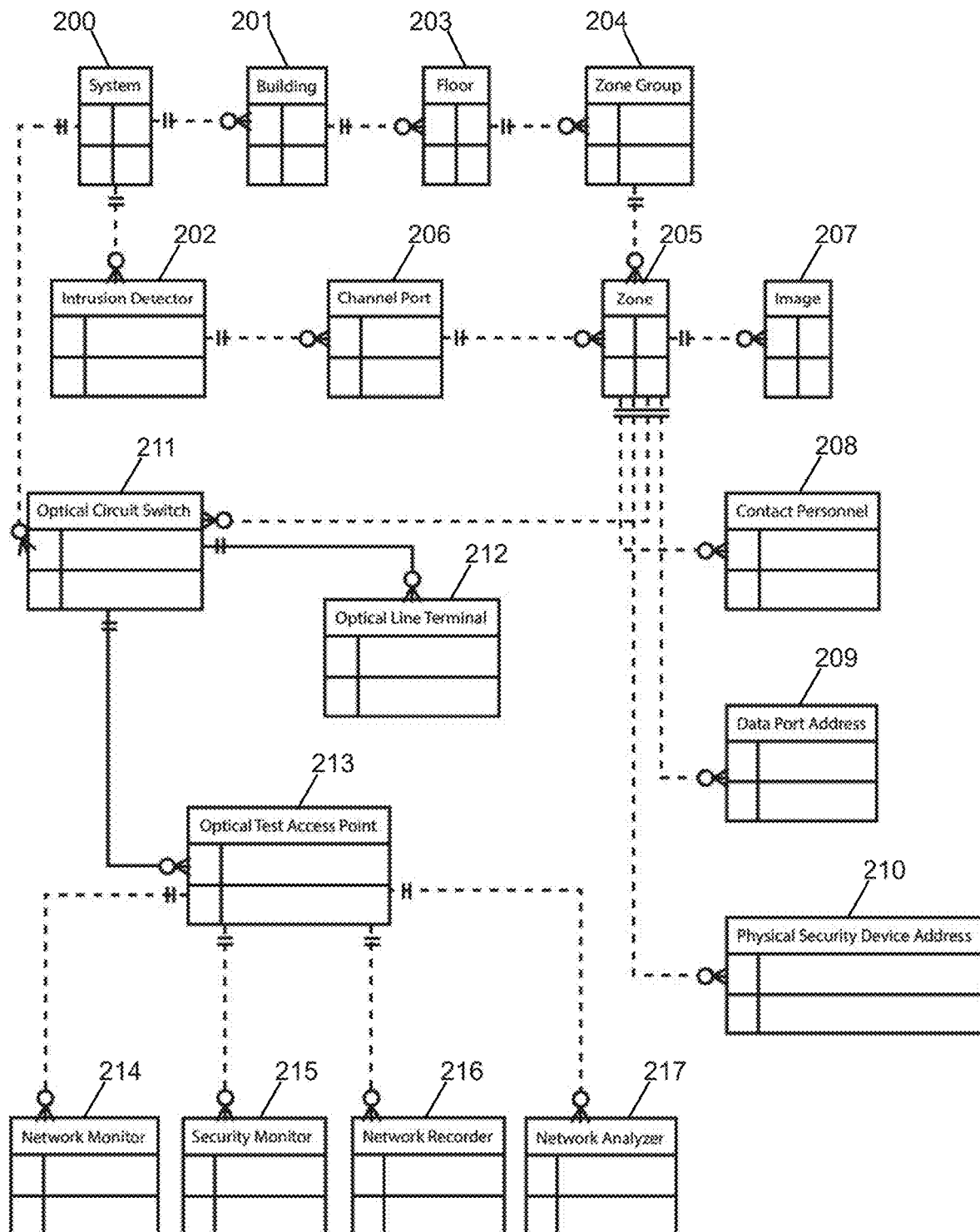


FIG. 2

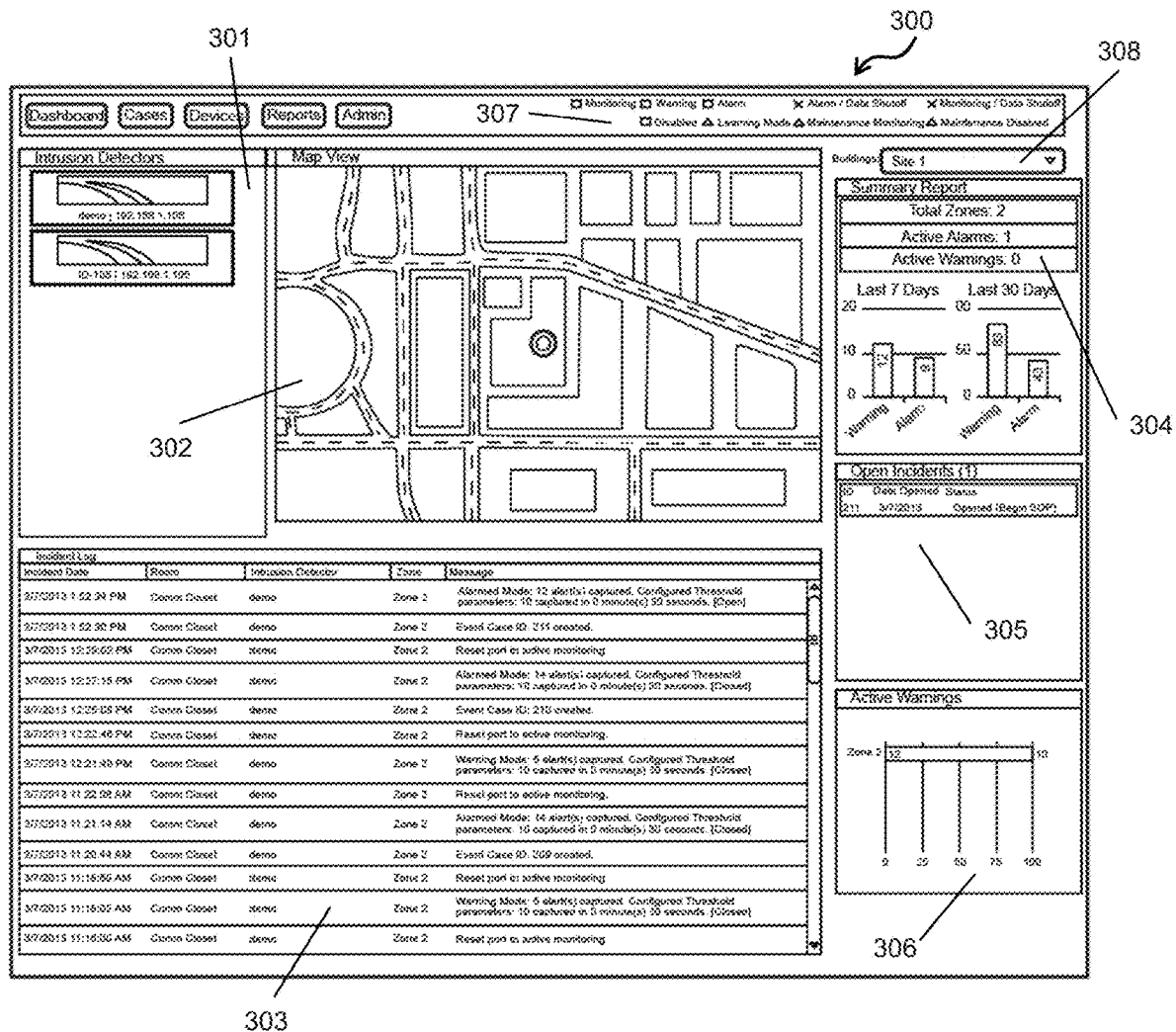


FIG. 3

U.S. Patent

Jul. 12, 2022

Sheet 4 of 34

US 11,388,181 B2

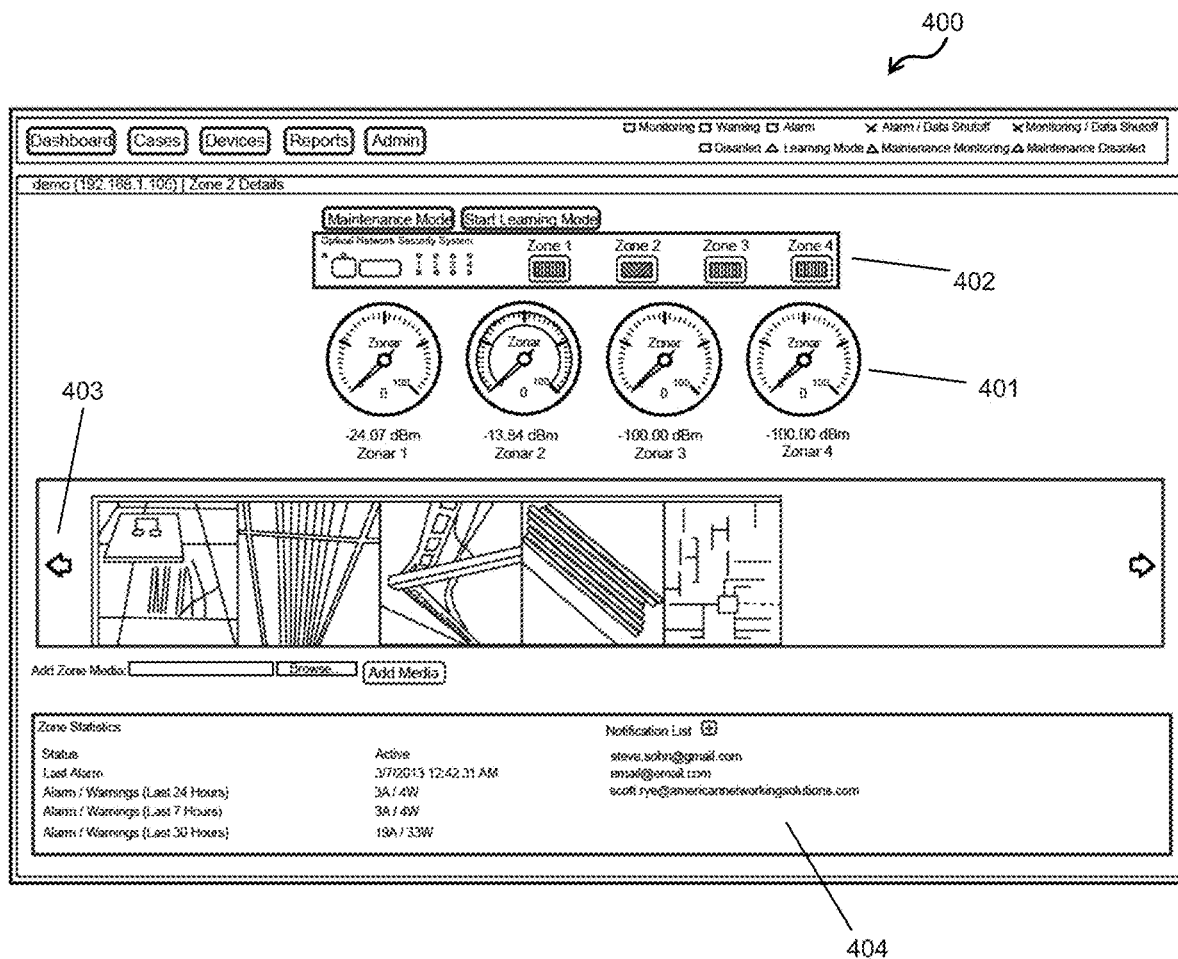


FIG. 4

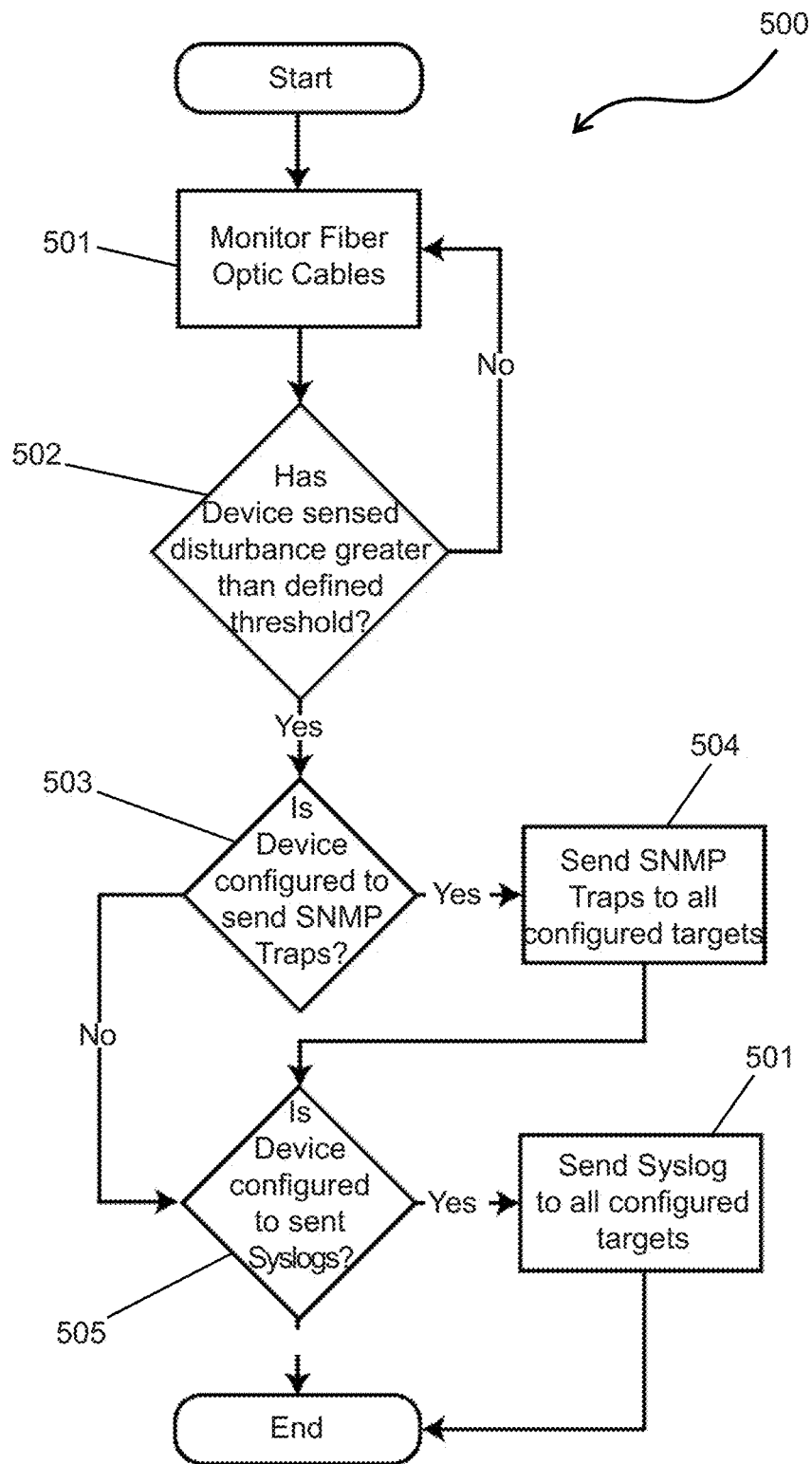


FIG. 5

U.S. Patent

Jul. 12, 2022

Sheet 6 of 34

US 11,388,181 B2

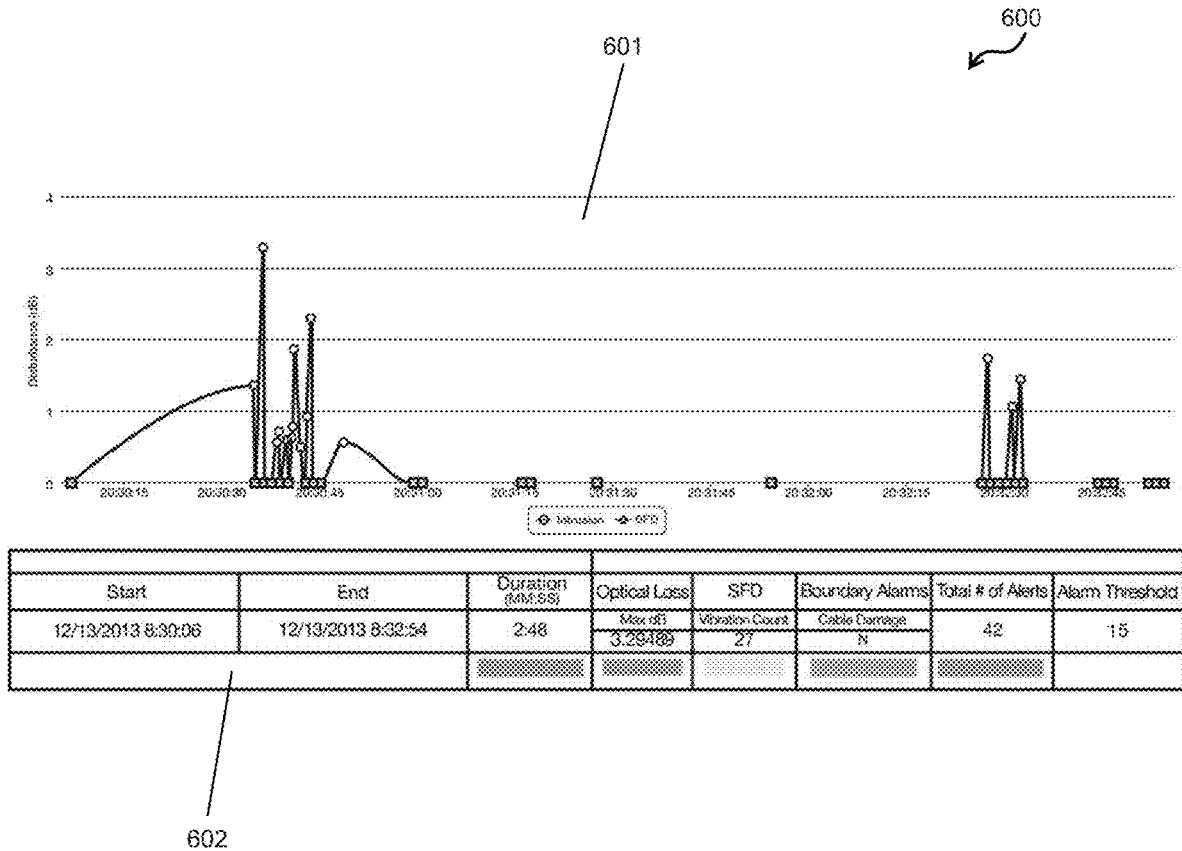


FIG. 6

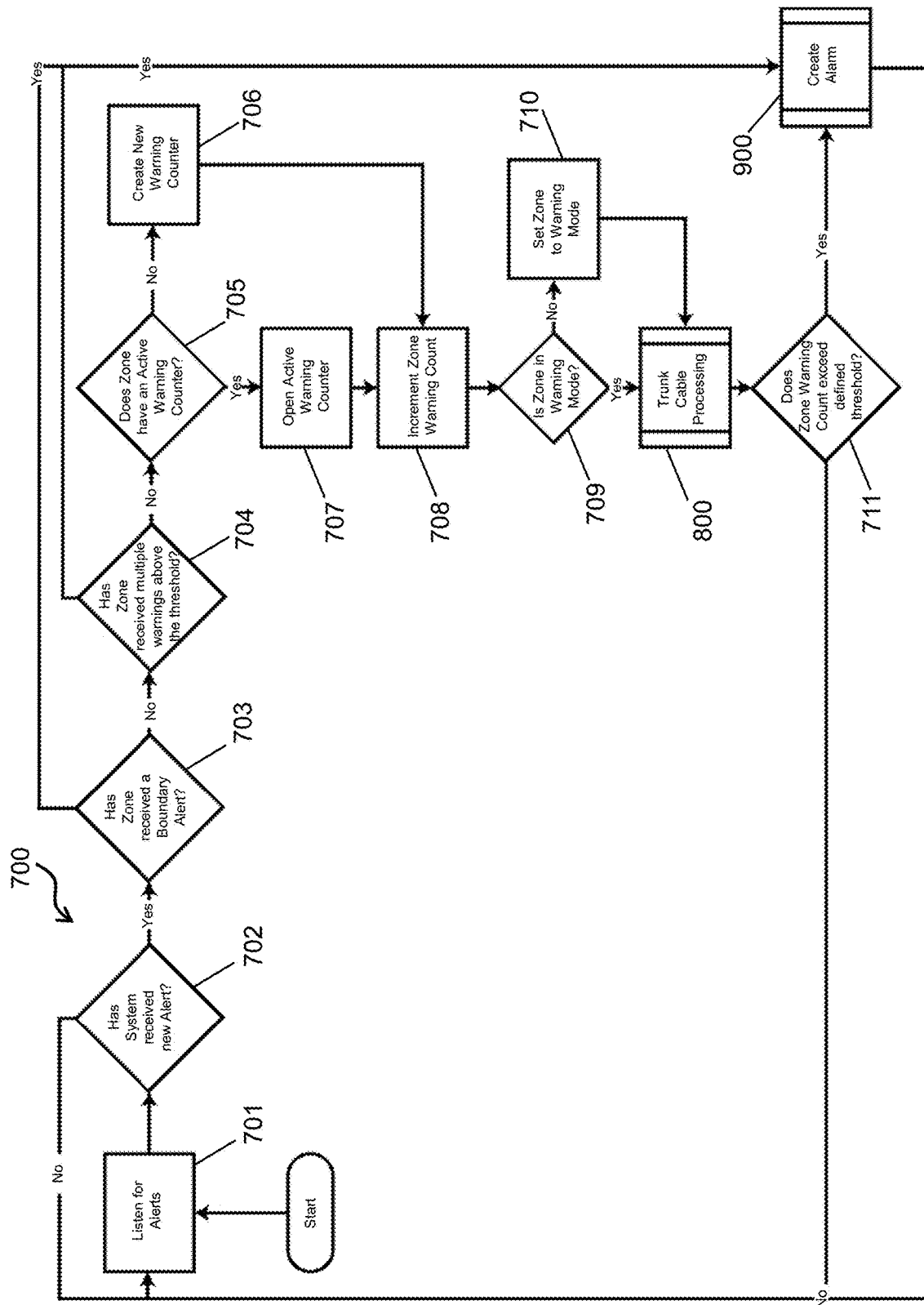


FIG. 7

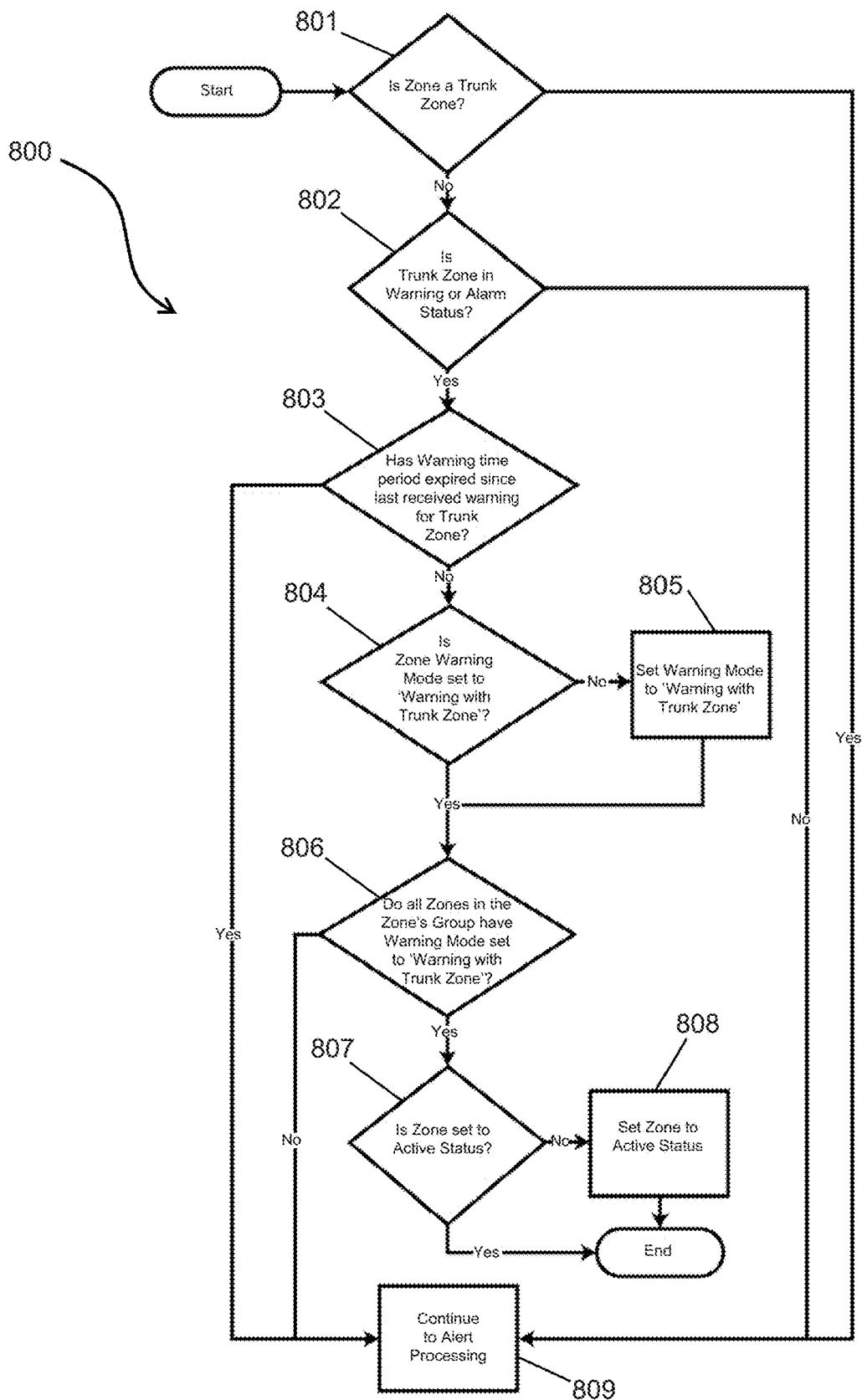


FIG. 8

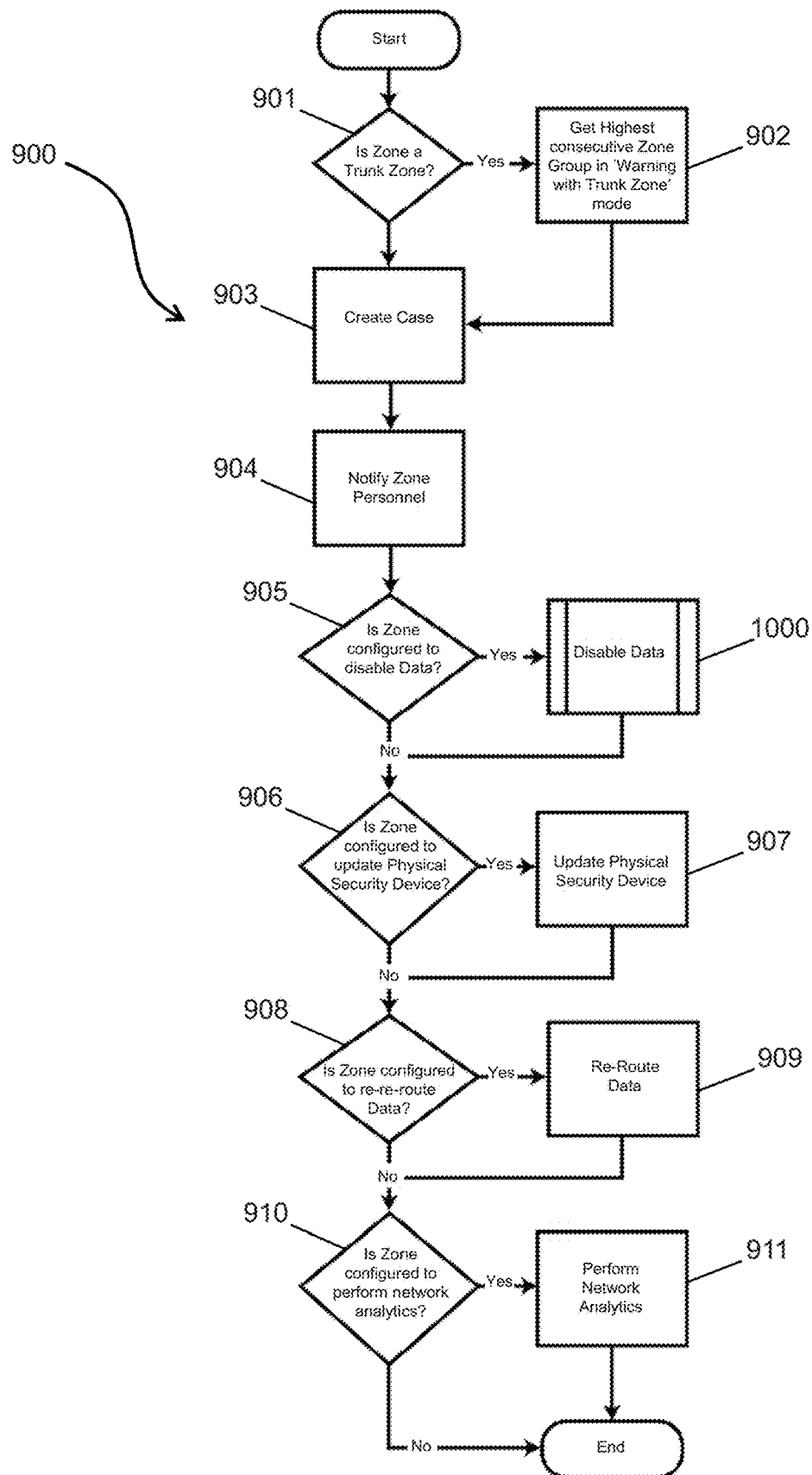


FIG. 9

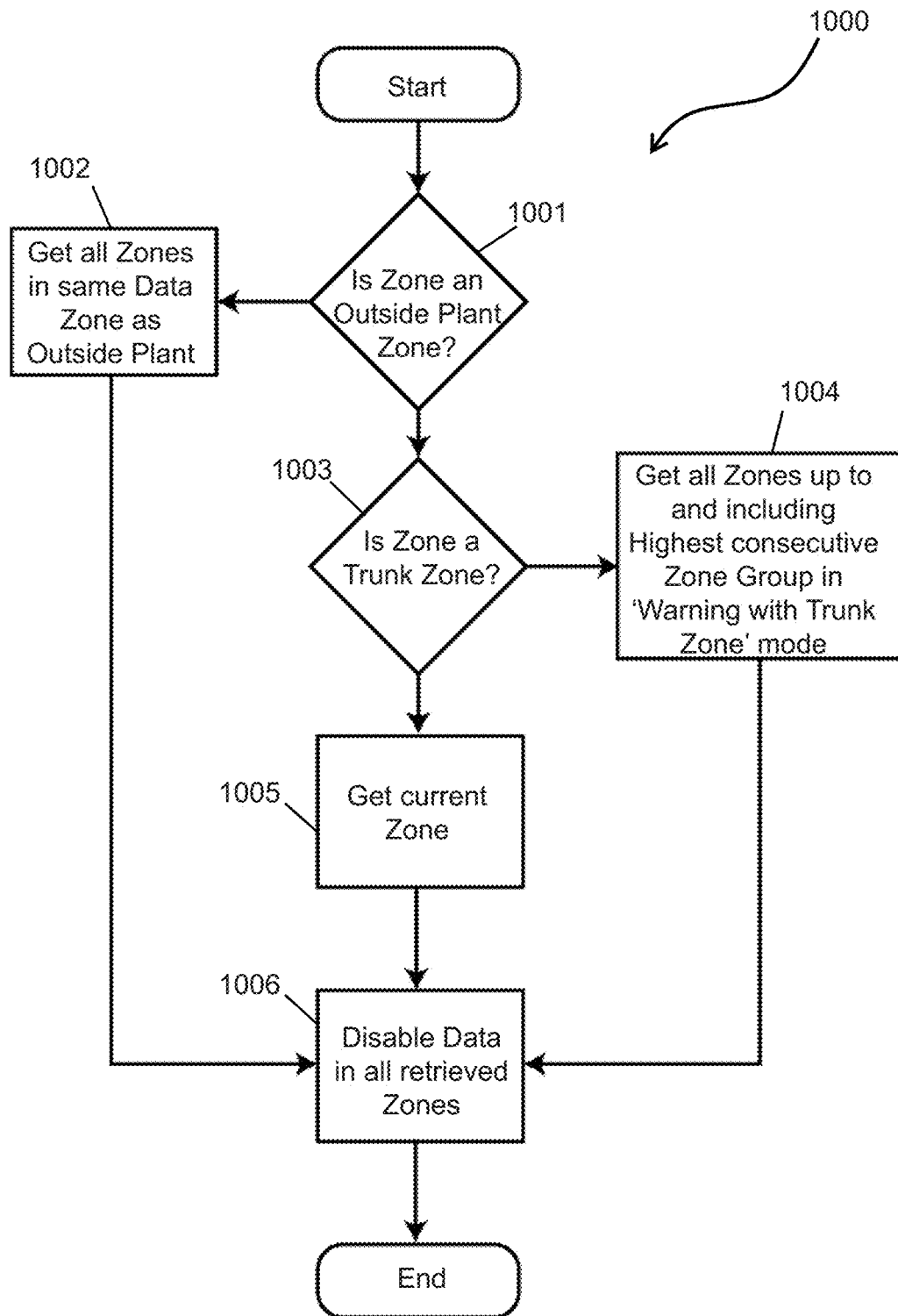


FIG. 10

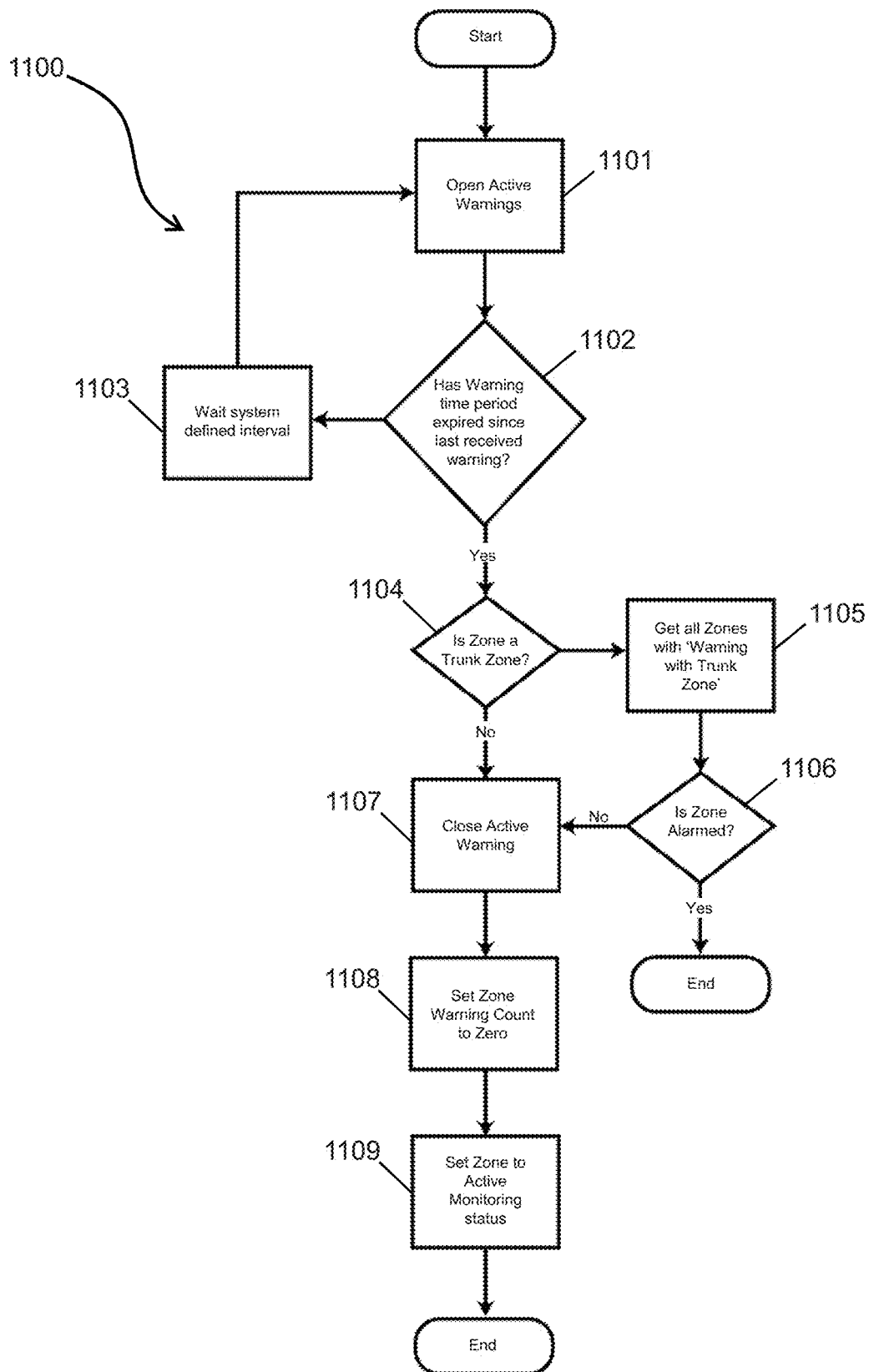


FIG. 11

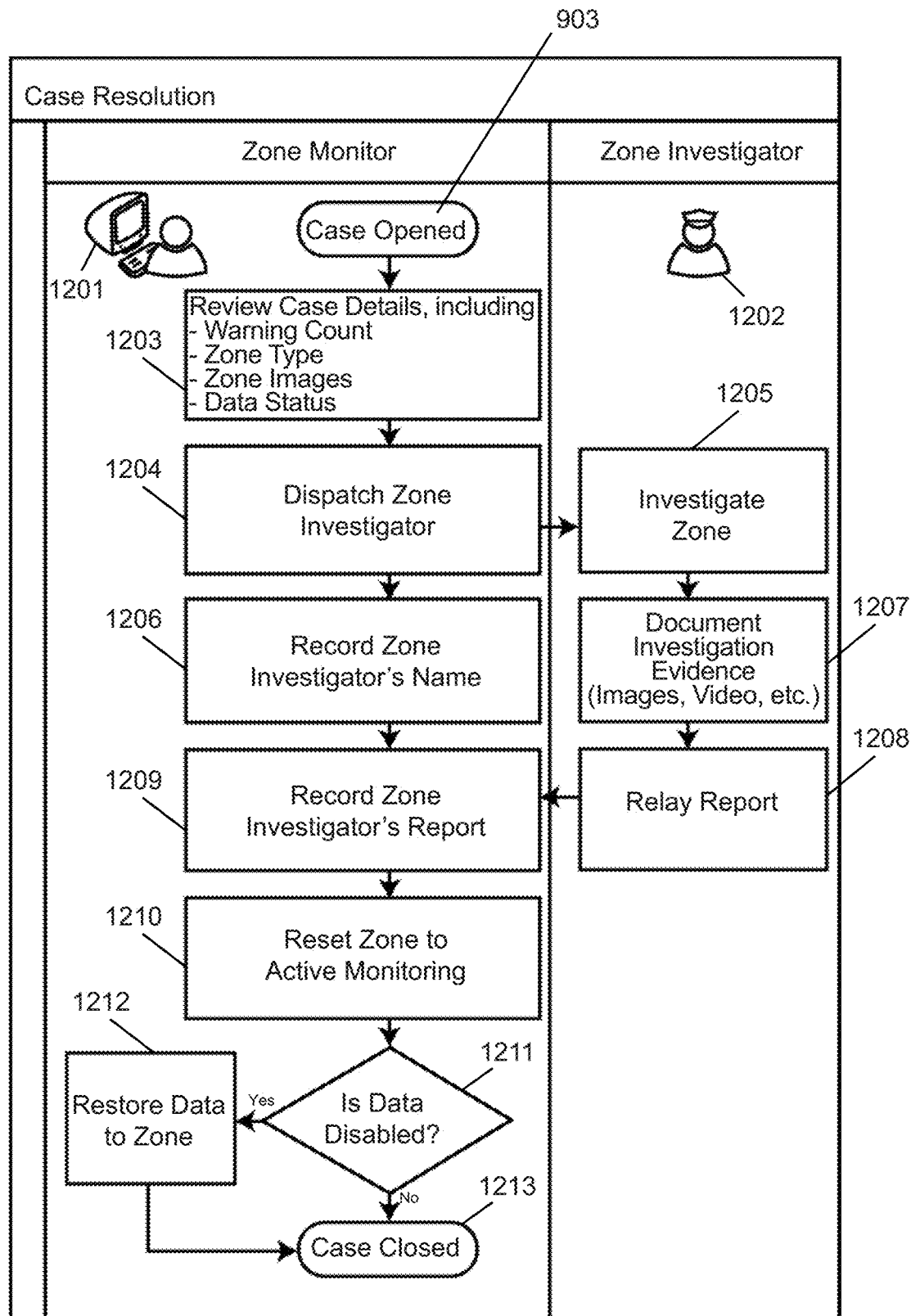


FIG. 12

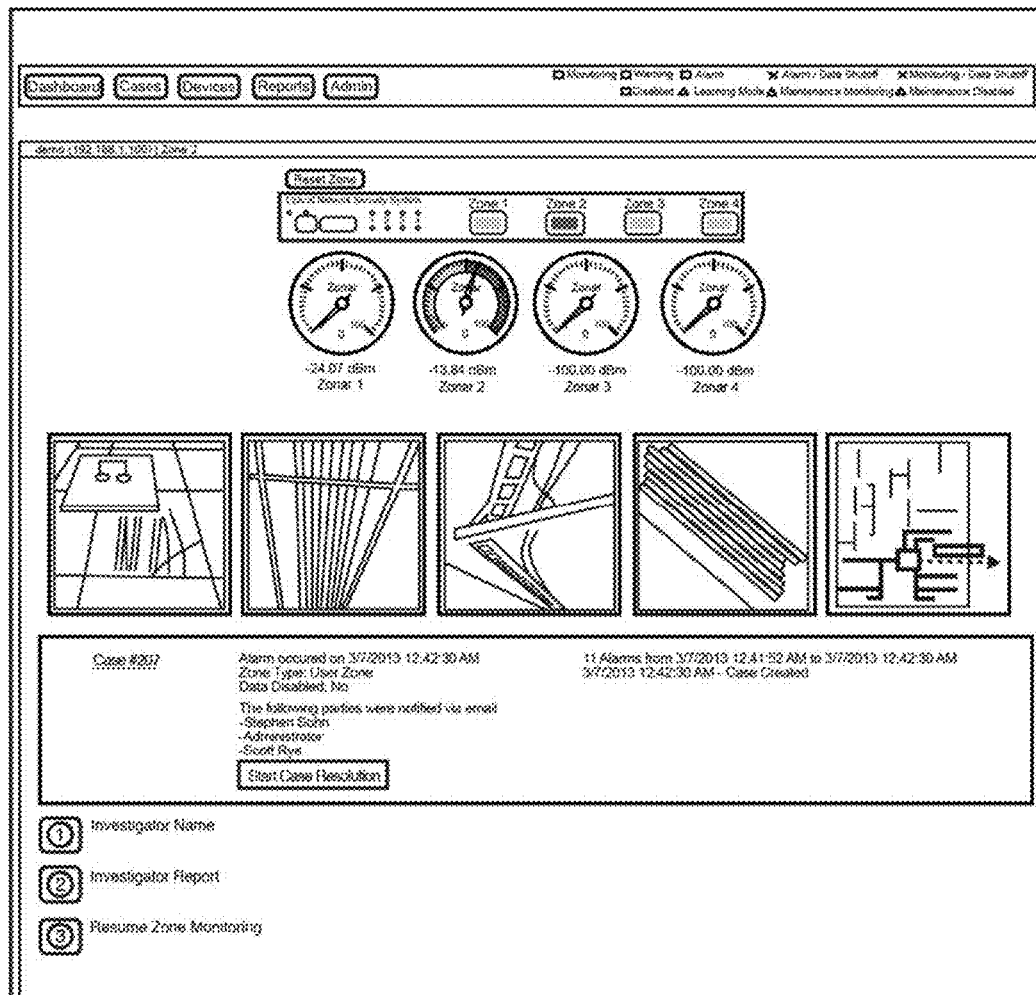


FIG. 13

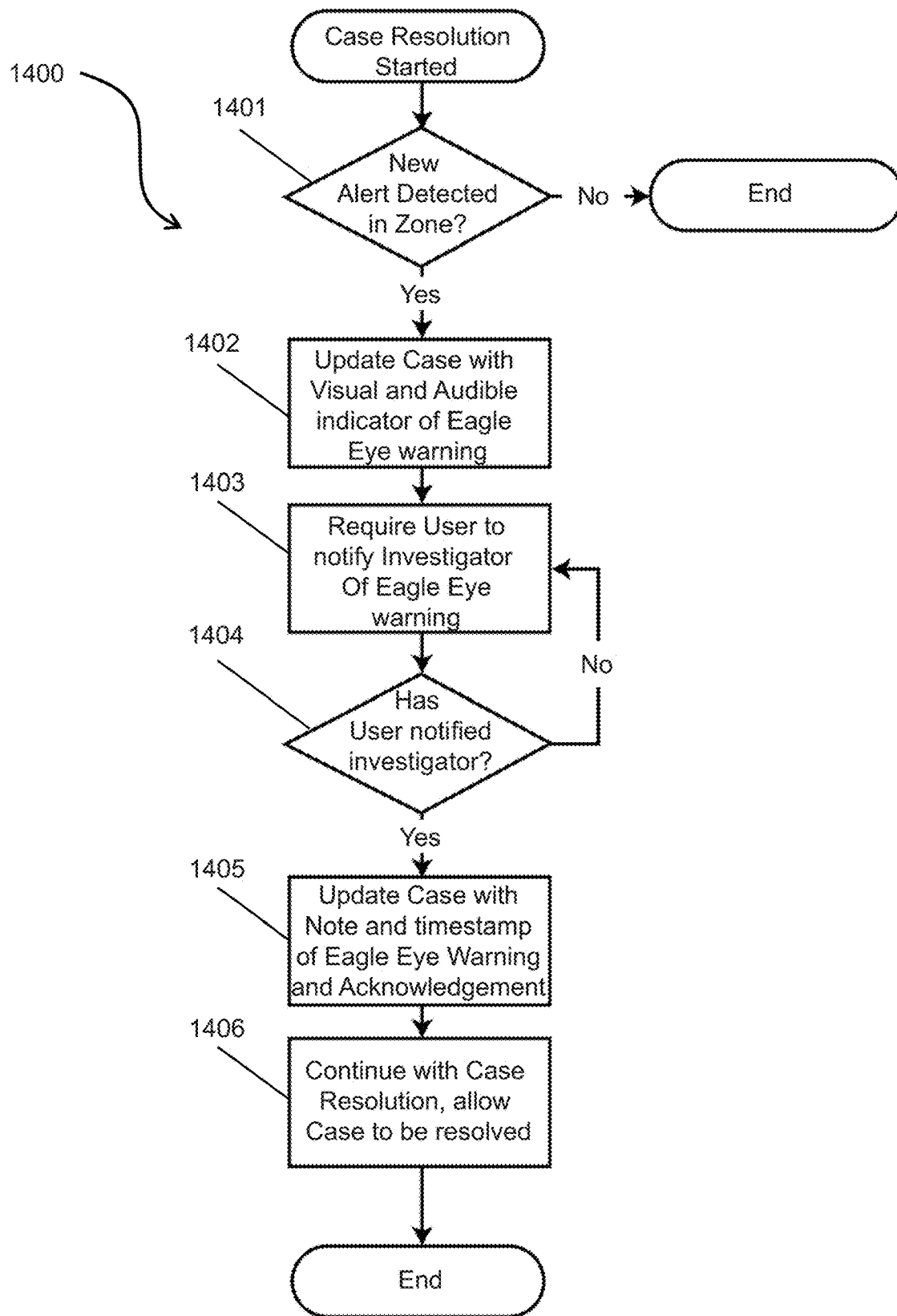


FIG. 14

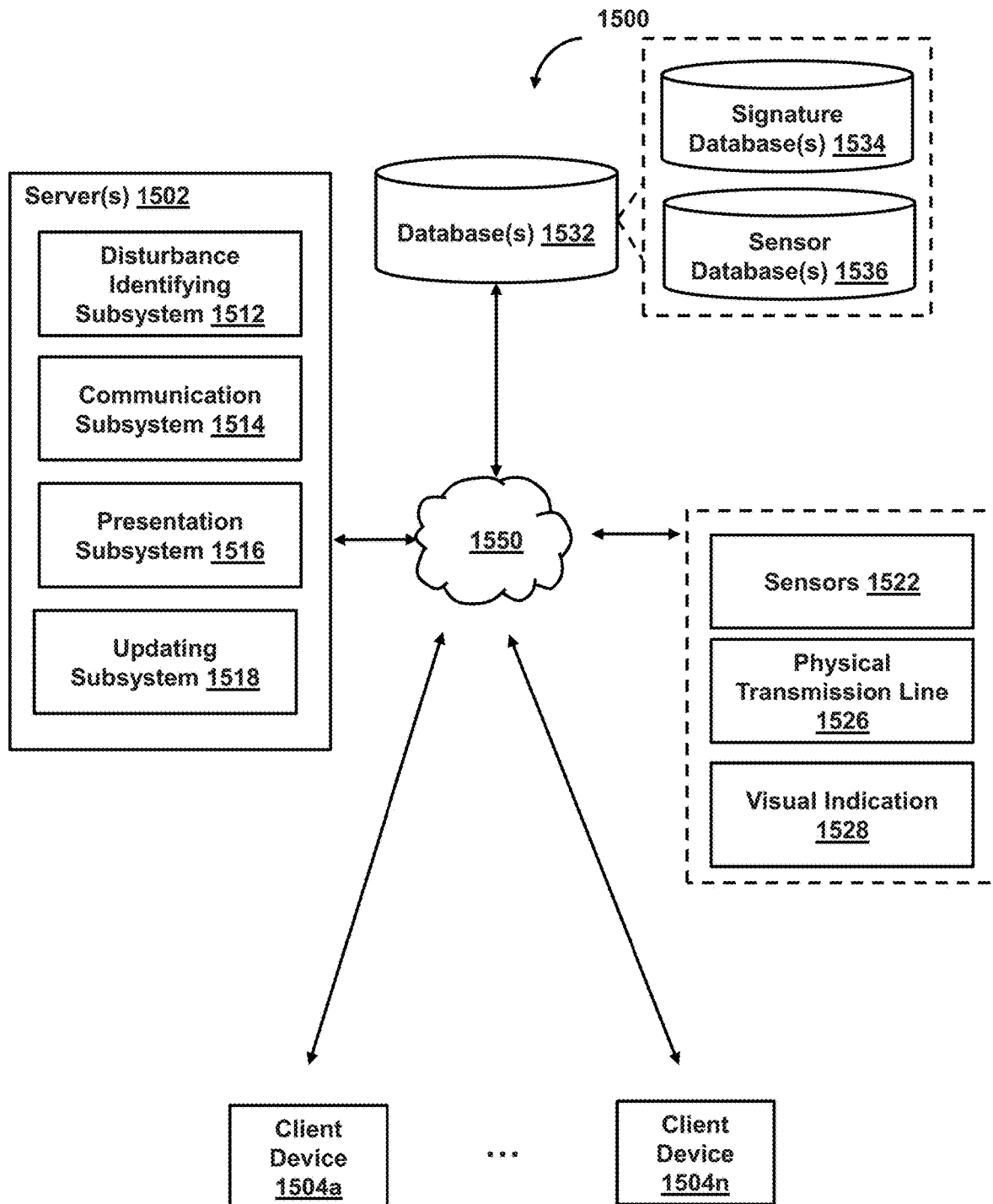


FIG. 15

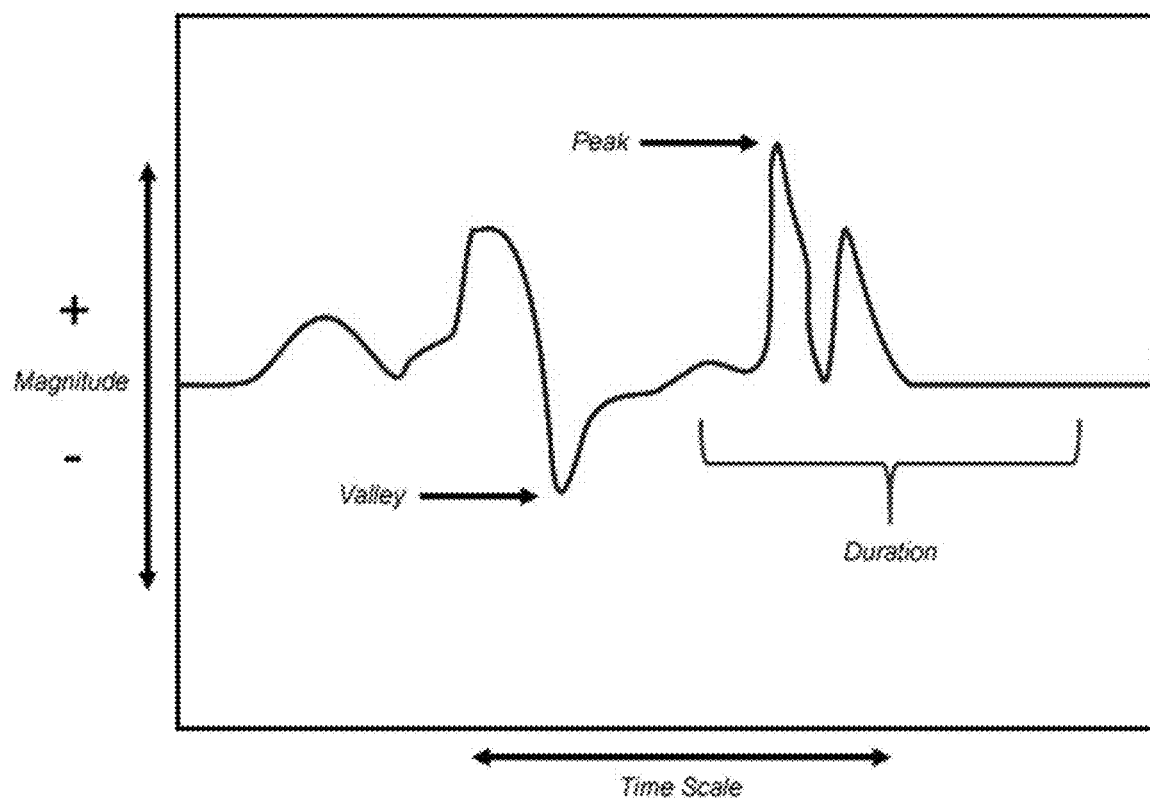


FIG. 16

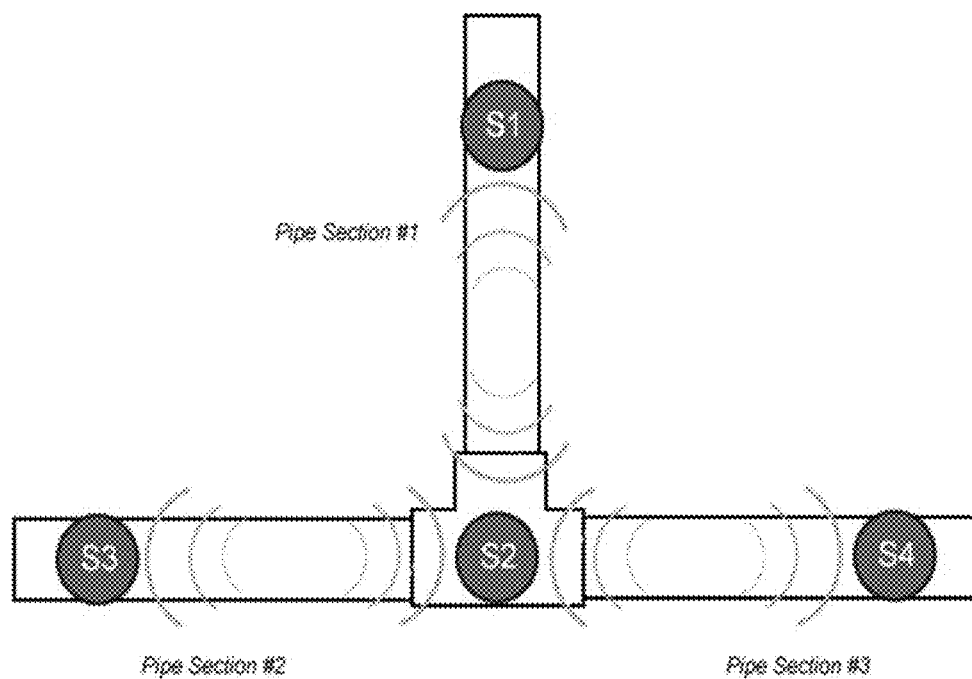


FIG. 17

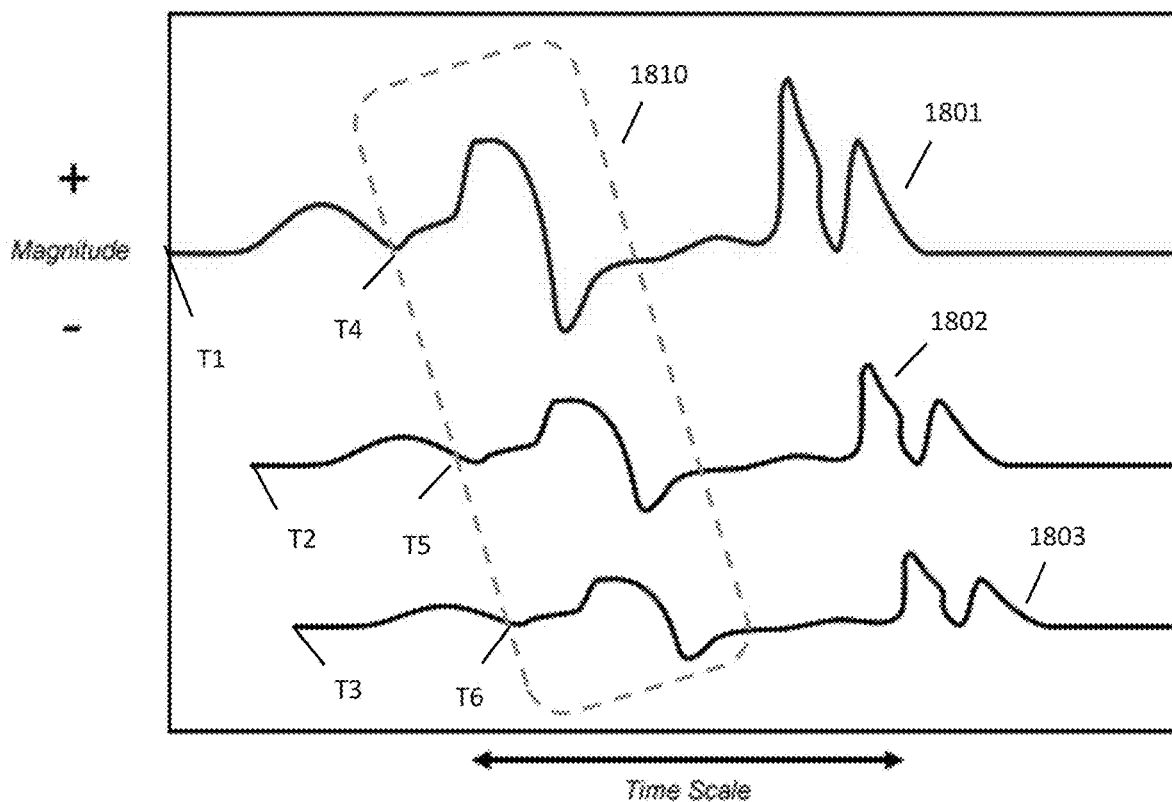


FIG. 18

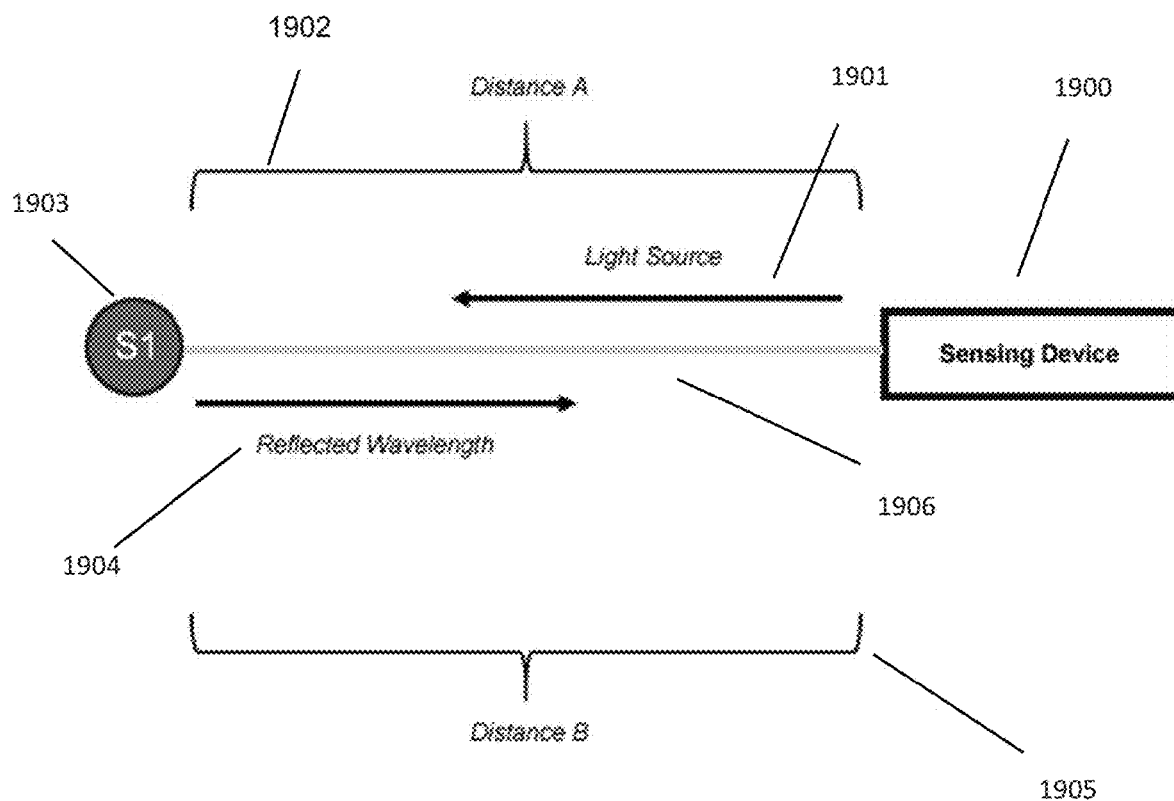


FIG. 19

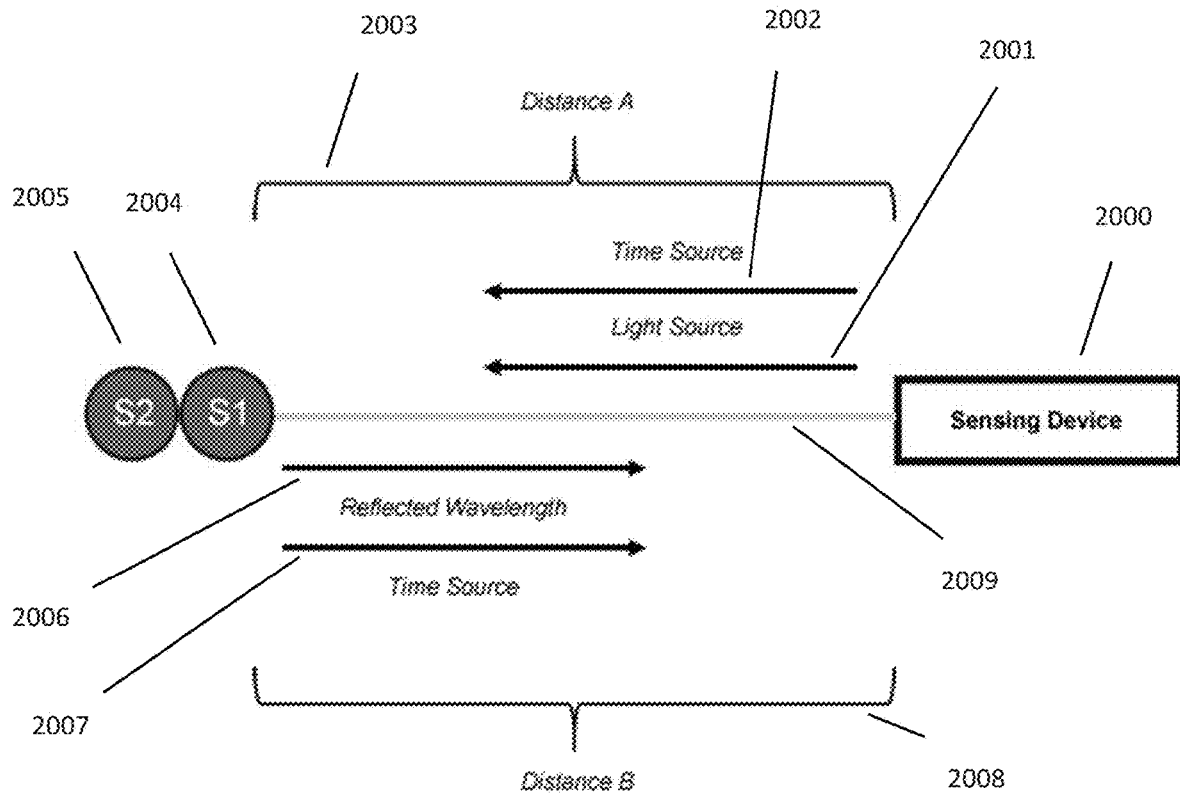


FIG. 20

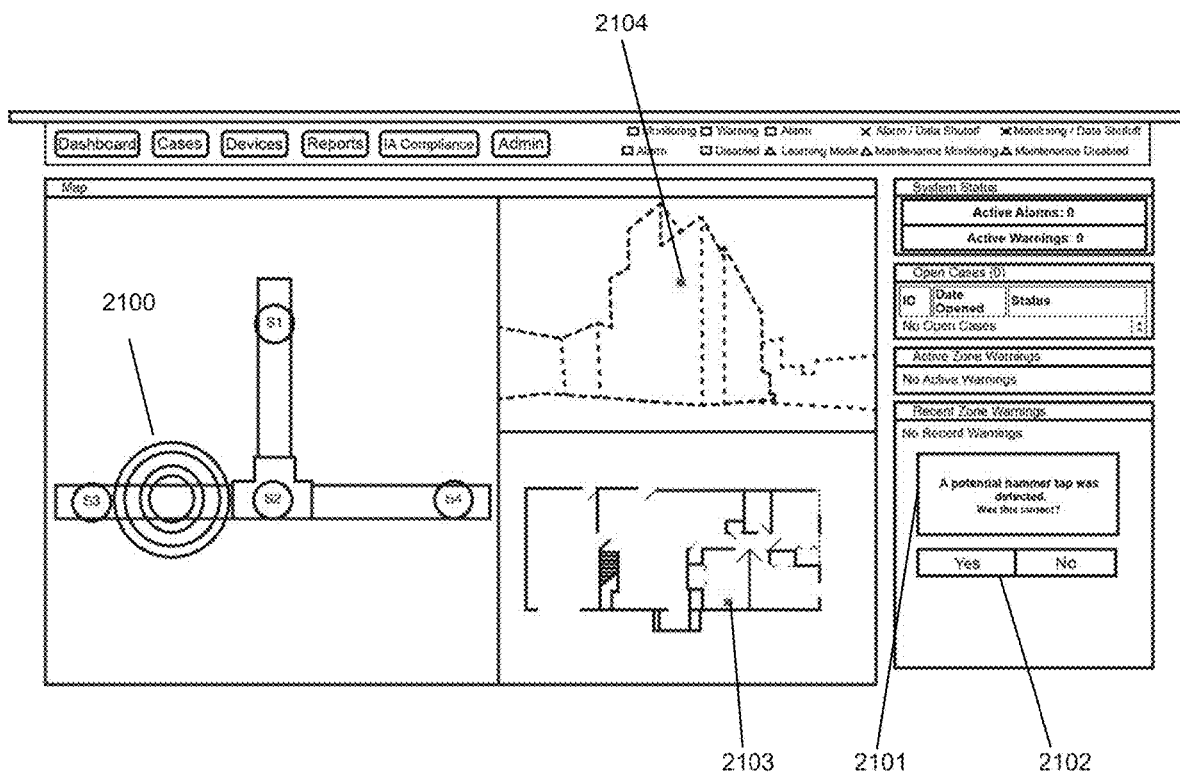


FIG. 21

U.S. Patent

Jul. 12, 2022

Sheet 22 of 34

US 11,388,181 B2

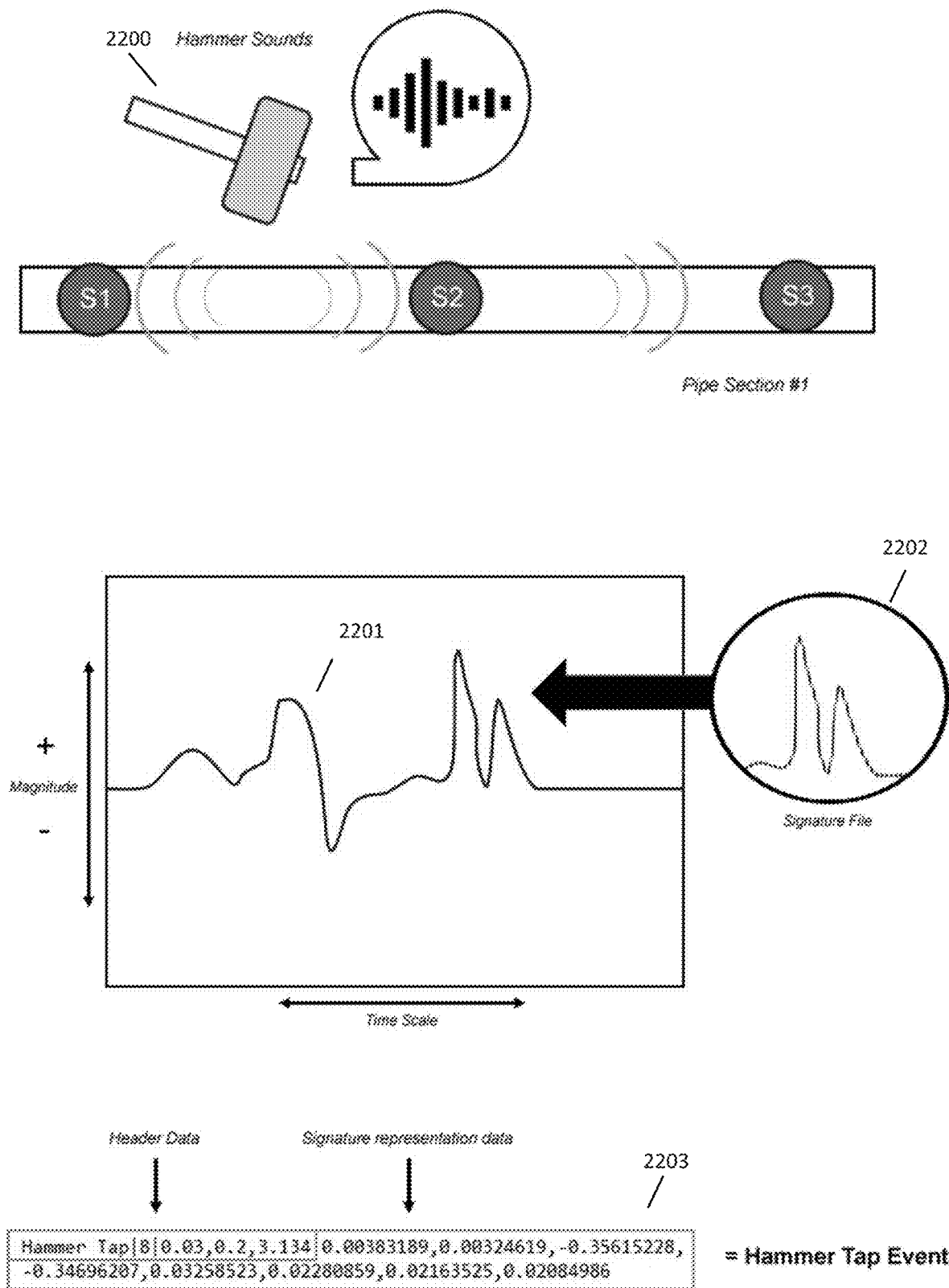


FIG. 22

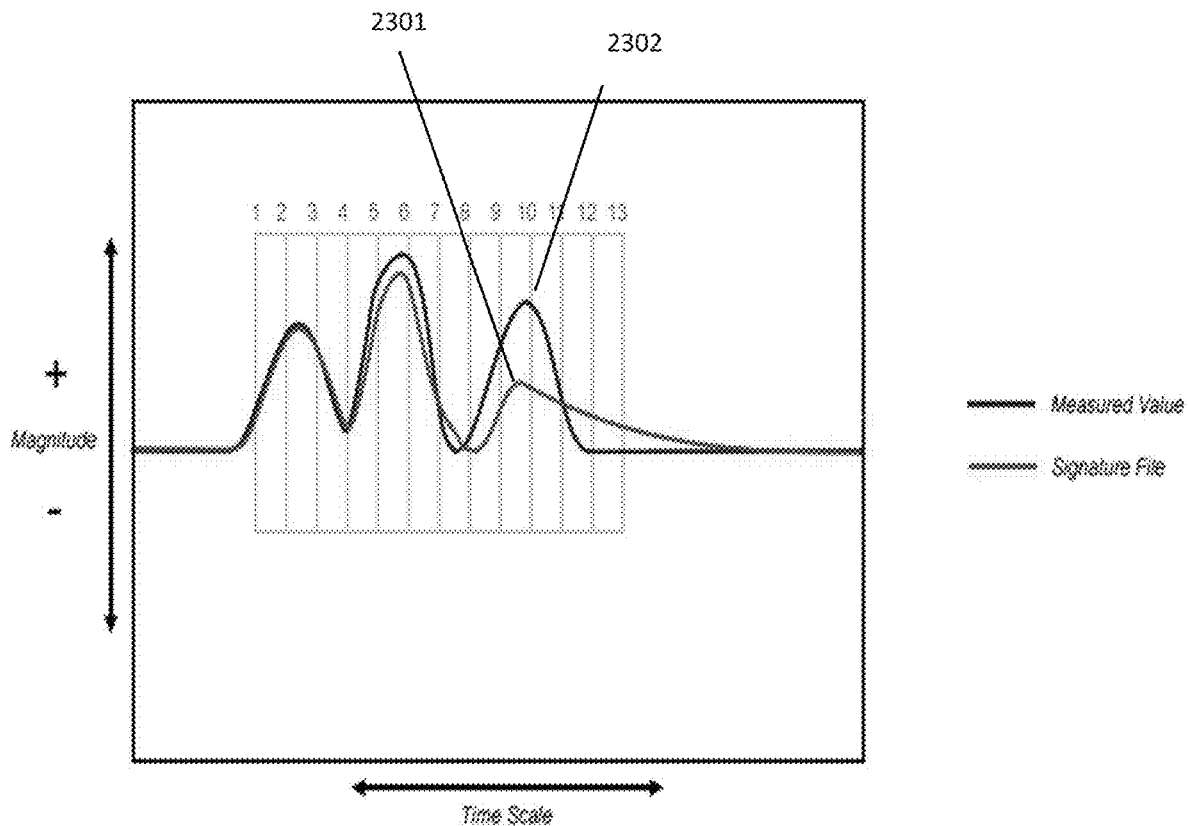


FIG. 23

U.S. Patent

Jul. 12, 2022

Sheet 24 of 34

US 11,388,181 B2

2401

Event Name	Signature Time	Signature Sample Time	Signature Point Variance	Event
Signature 1	19	500	0.03	0.01986278, 0.01360435, 0.04929434, 0.02358059, 0.3377867, -0.31270392, 0.02709874, 0.04391951, -0.31700547, -0.33270982, 0.01746801, 0.02514189, -0.0088283, -0.33348216, 0.09066777, -0.00204435, -0.005356, -0.06791087, 0.00810864
Signature 2	11	250	0.03	-0.03936336, -0.03506037, -0.35630405, -0.35122164, -0.02117199, -0.02136783, -0.35230049, 0.07992185, -0.00553015, -0.00778907, -0.00846291
Signature 3	13	1000	0.03	0.02182732, 0.02163145, 0.0353218, 0.02456575, 0.00481314, -0.0156861, 0.01654826, 0.01517906, 0.01361399, 0.01540075, 0.04432268, 0.04536207, 0.04530207
Signature 4	8	250	0.03	0.00183189, 0.06324615, -0.35415228, -0.34696307, 0.03258523, 0.02388859, 0.02163525, 0.02084986

2402

Initial Variance Limit: 0.5003

Date/Time of Event	Event Name	Capture Time Period	Event Time Period	Total Exact Point Values	Total Continuous Exact Point Values	Total Variable Point Values	Total Continuous Variable Points	Confidence Value	User Confirmed	User Confirmed Result
1/1/2017 8:42	Signature 1	19	13	2	2	3	2	12%	No	0
1/1/2017 8:42	Signature 2	11	11	0	0	0	0	0%	No	0
1/1/2017 8:42	Signature 3	13	11	0	0	7	4	21%	No	0
1/1/2017 8:42	Signature 4	8	11	3	5	5	6	52%	Yes	1
1/1/2017 10:33	Signature 1	19	17	0	0	0	0	0%	No	0
1/1/2017 10:33	Signature 2	11	17	0	0	6	4	61%	No	0
1/1/2017 10:33	Signature 3	13	17	0	0	3	0	8%	No	0
1/1/2017 10:33	Signature 4	8	17	0	0	4	0	12%	No	0
1/1/2017 9:27	Signature 1	19	22	0	0	0	0	0%	No	0
1/1/2017 9:27	Signature 2	11	22	1	0	8	5	73%	Yes	2
1/1/2017 9:27	Signature 3	13	22	0	0	0	0	0%	No	0
1/1/2017 9:27	Signature 4	8	22	0	0	0	0	0%	No	0

FIG. 24

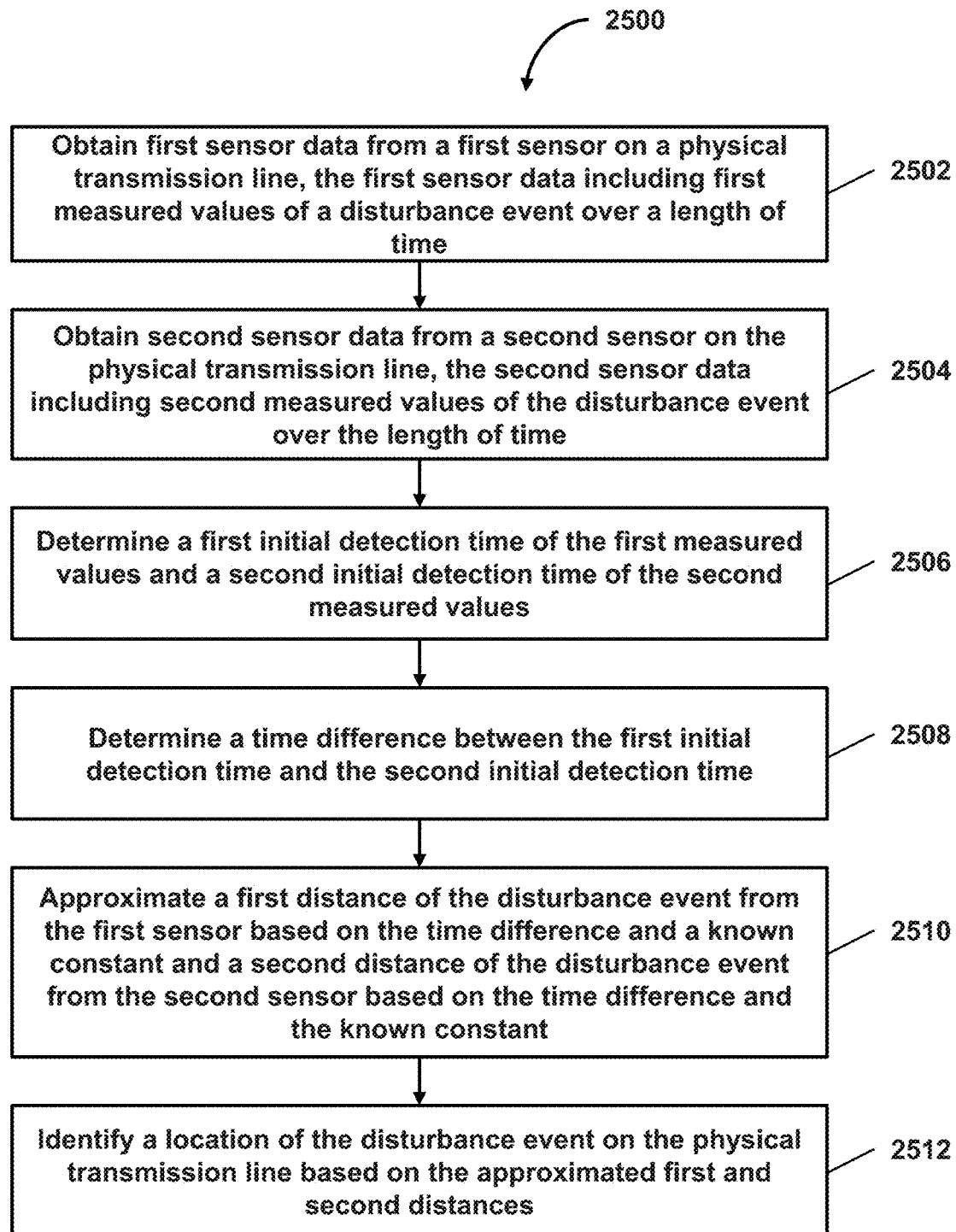


FIG. 25

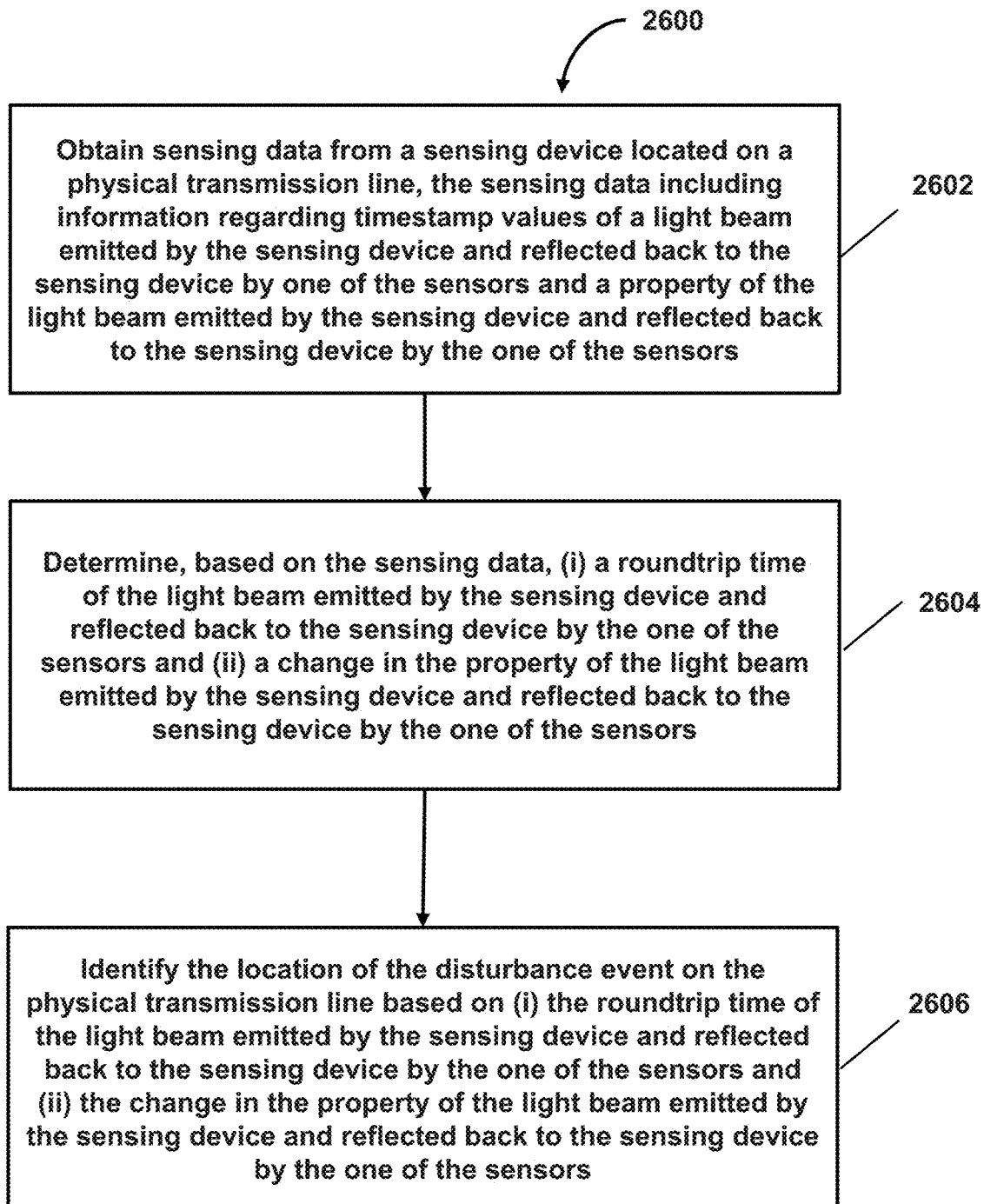


FIG. 26

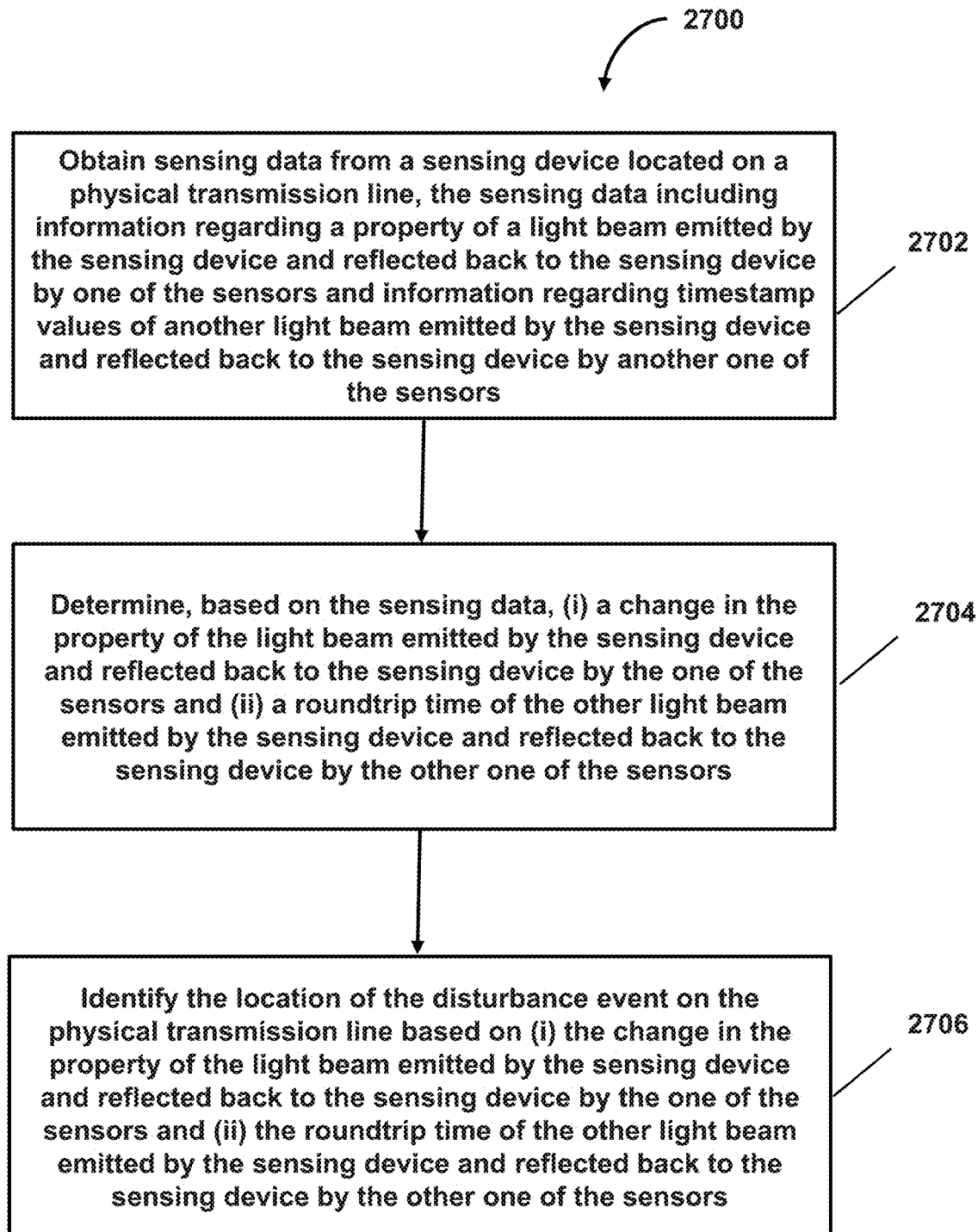


FIG. 27

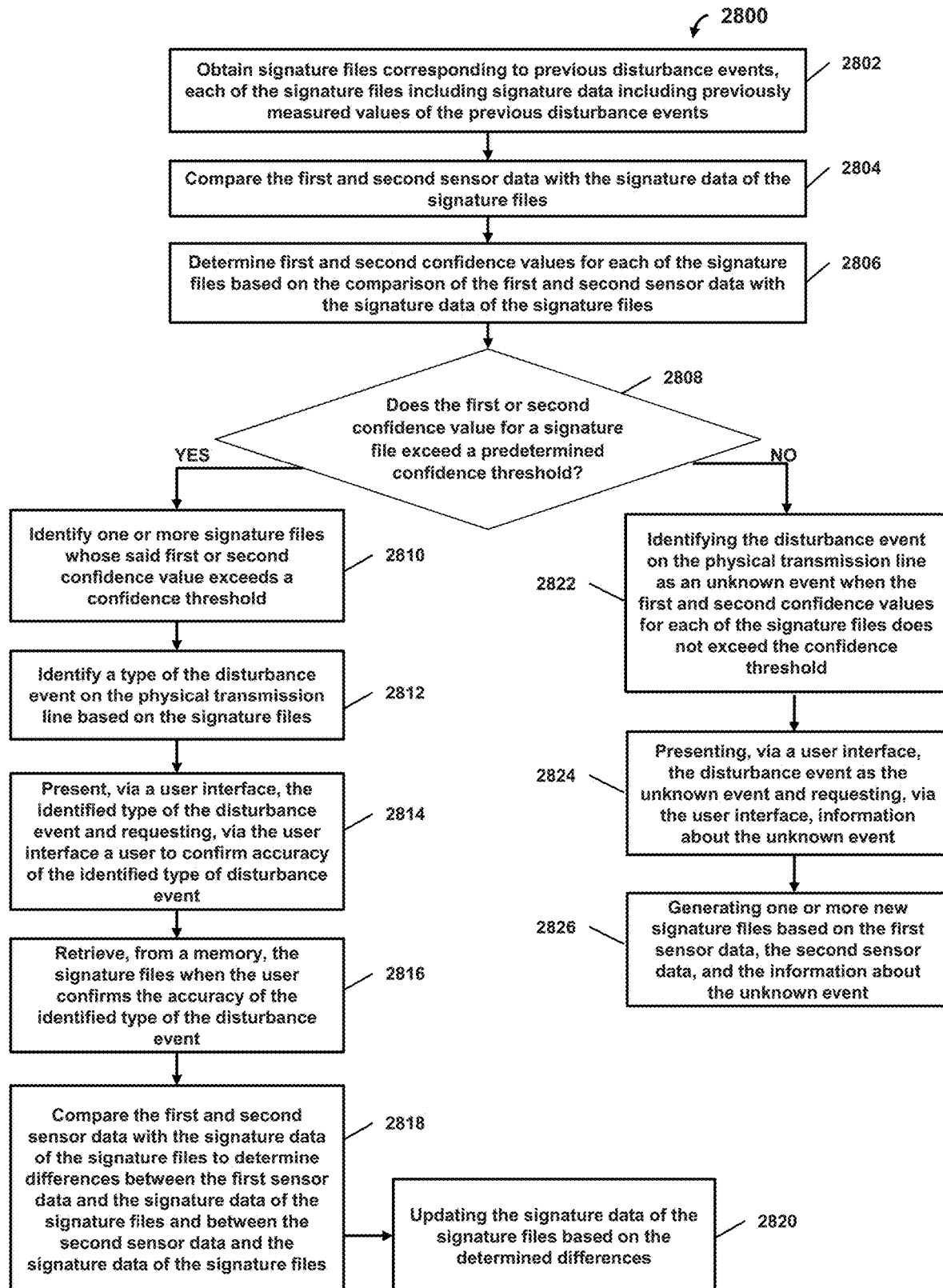


FIG. 28

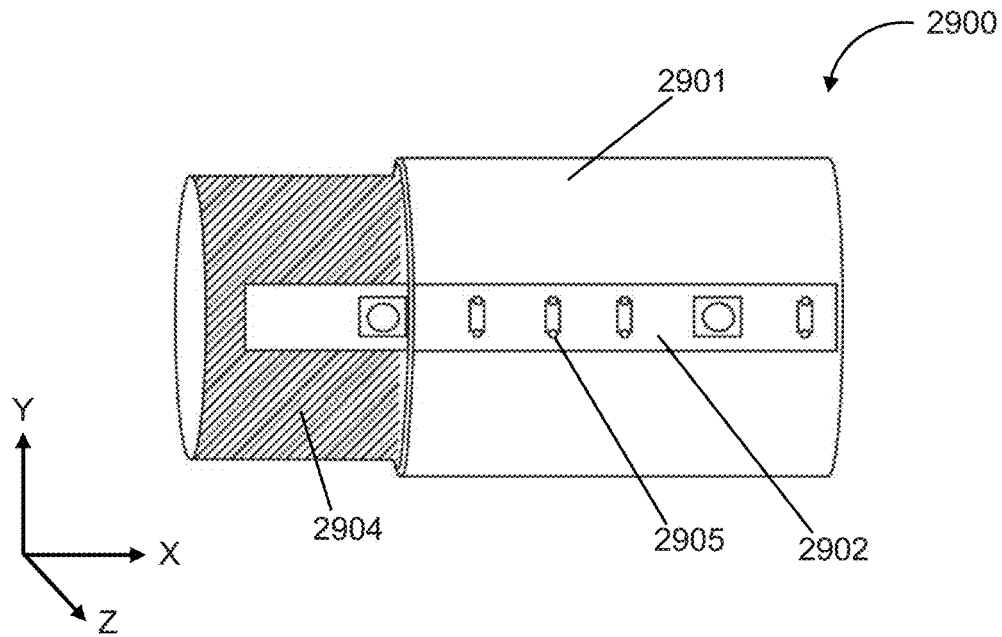


FIG. 29A

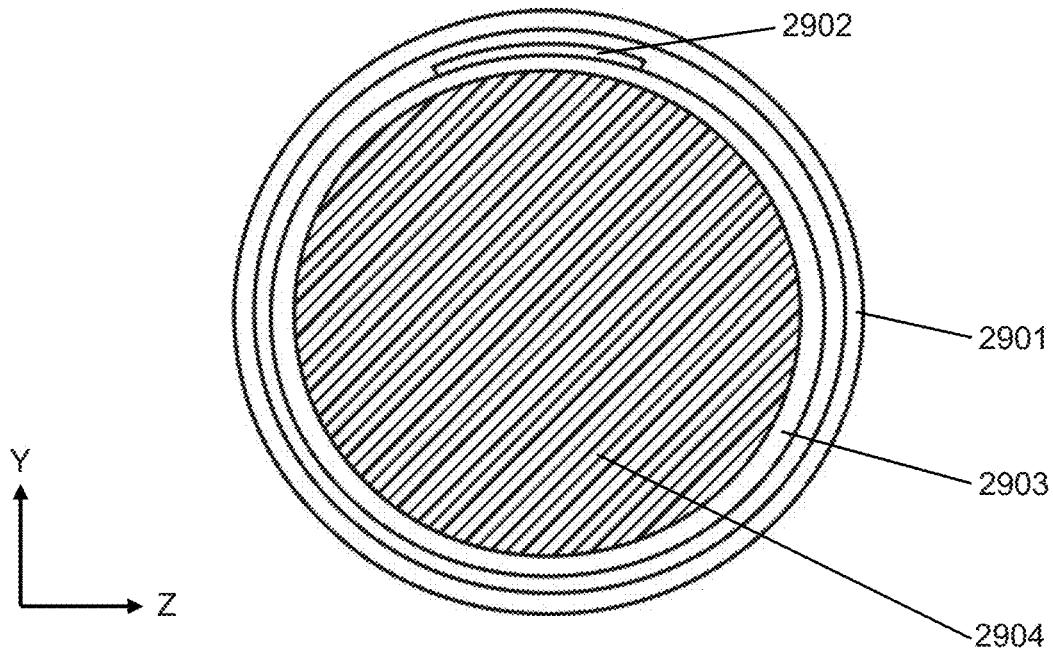


FIG. 29B

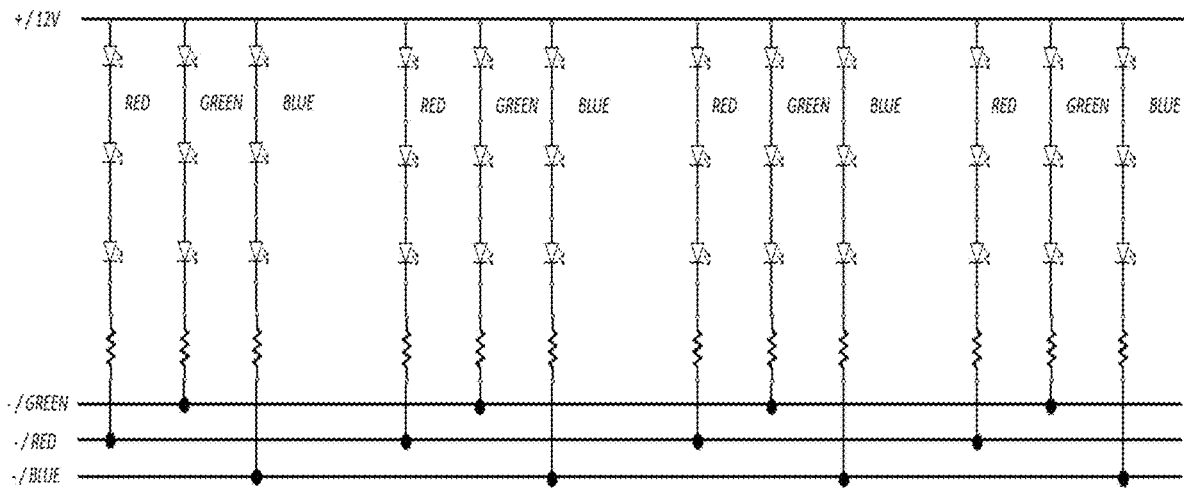


FIG. 30

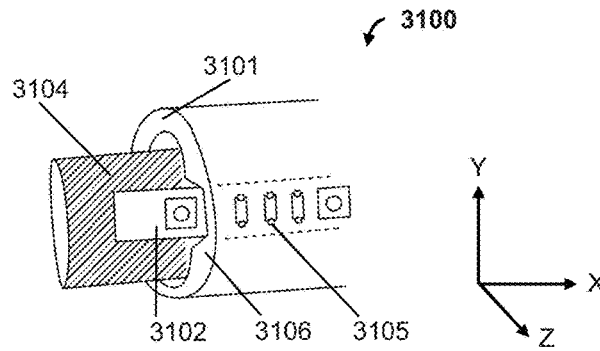


FIG. 31A

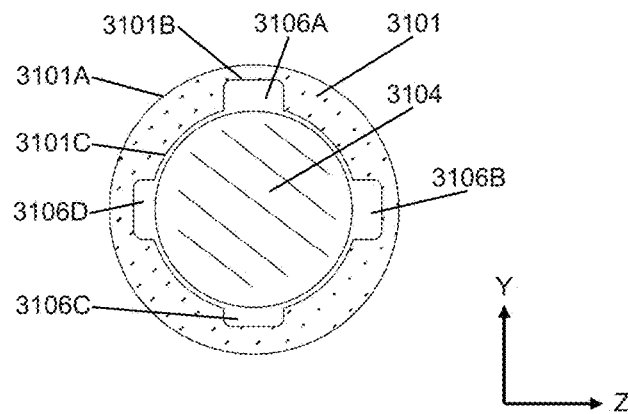


FIG. 31B

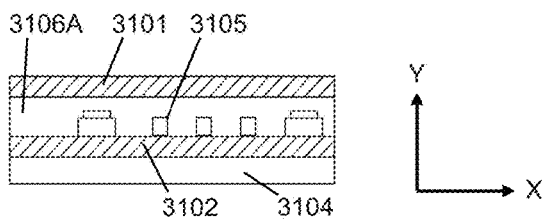


FIG. 31C

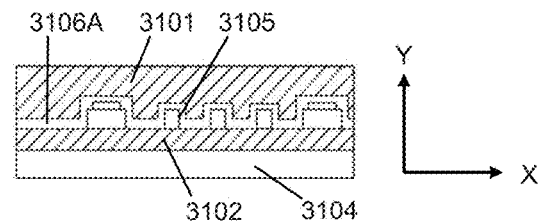


FIG. 31D

U.S. Patent

Jul. 12, 2022

Sheet 32 of 34

US 11,388,181 B2

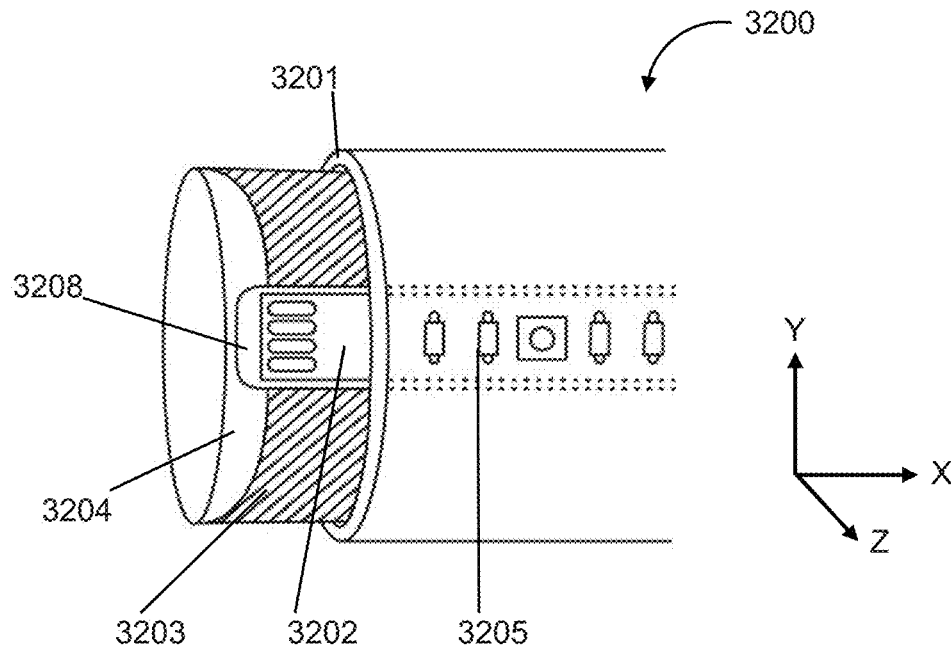


FIG. 32A

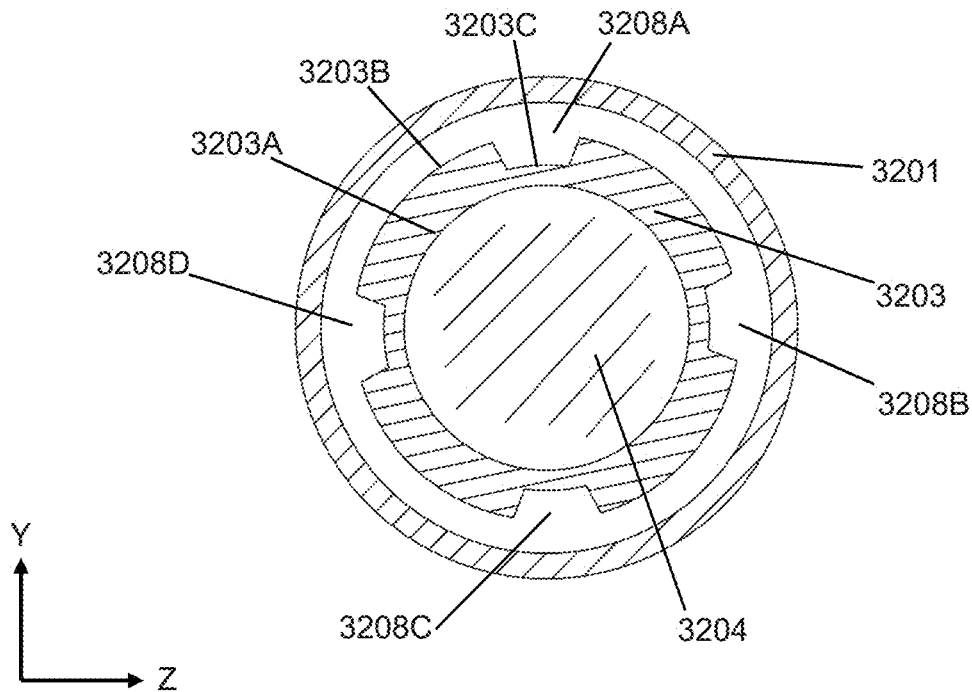


FIG. 32B

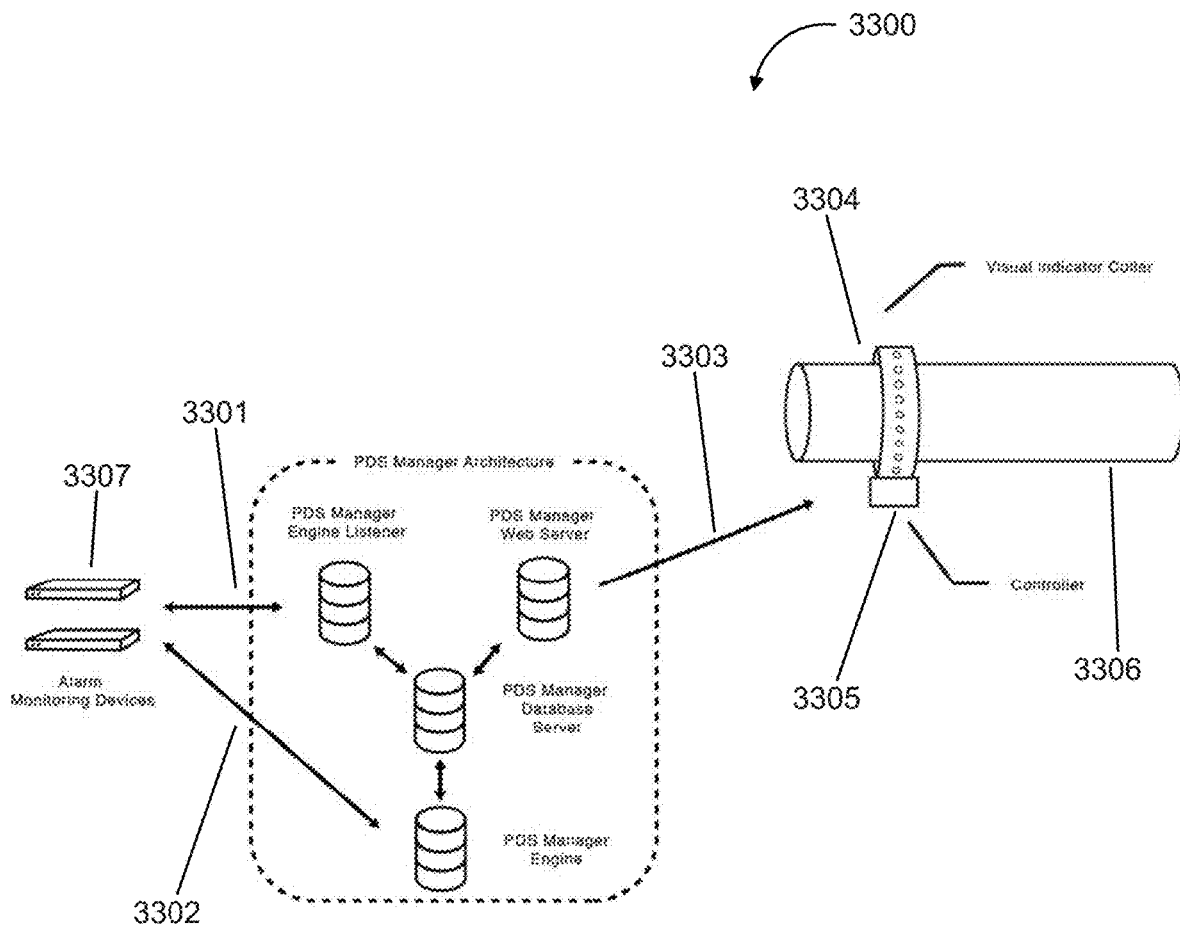


FIG. 33

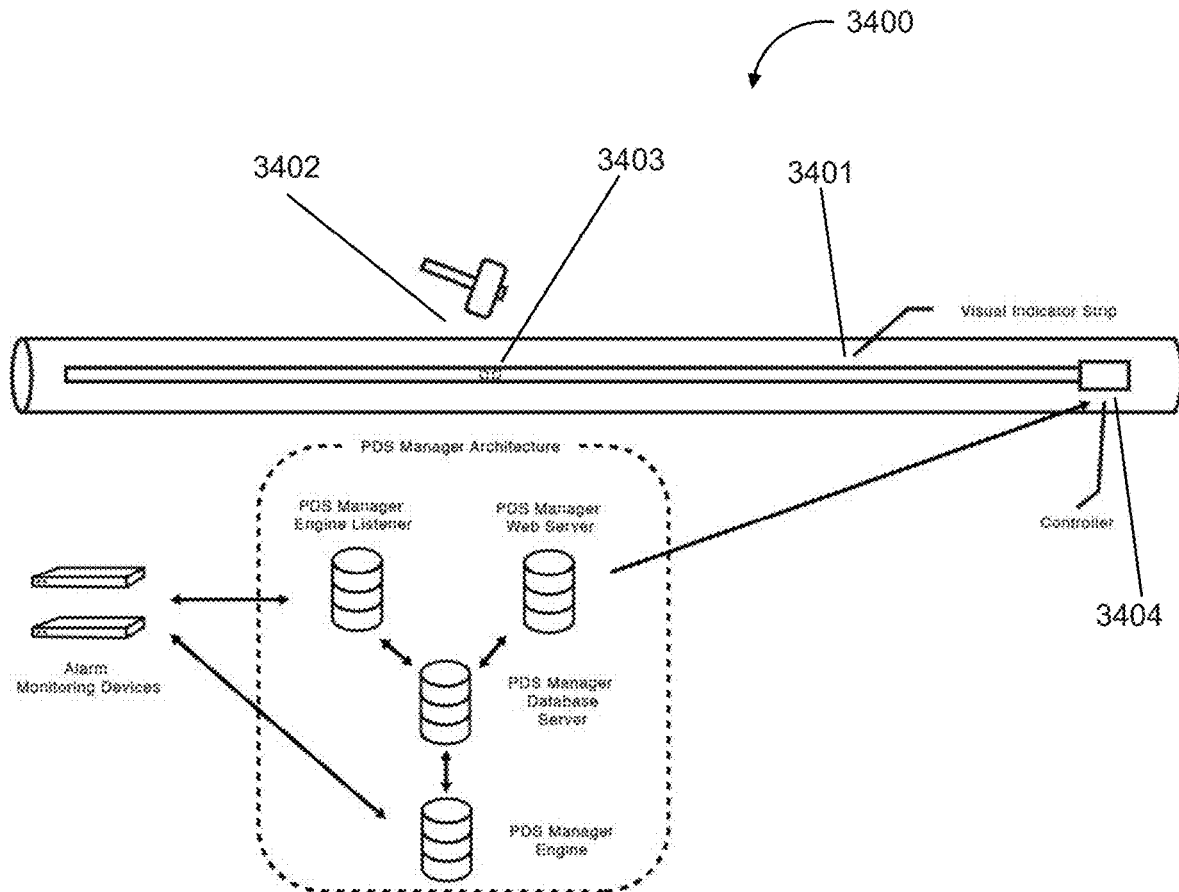


FIG. 34

US 11,388,181 B2

1

**CABLE ASSEMBLY DISTURBANCE
DETECTION METHOD****CROSS-REFERENCE TO RELATED
APPLICATIONS**

This application is a continuation of U.S. application Ser. No. 16/860,789, filed Apr. 28, 2020, which is a continuation of U.S. application Ser. No. 16/008,729, filed Jun. 14, 2018, which claims the benefit of U.S. Provisional Application No. 62/554,912, filed Sep. 6, 2017, and is also a continuation-in-part of U.S. application Ser. No. 15/246,635, filed Aug. 25, 2016, which is a continuation of U.S. patent application Ser. No. 14/849,746, filed Sep. 10, 2015, which is a continuation of U.S. patent application Ser. No. 14/217,259, filed Mar. 17, 2014, which claims the benefit of U.S. Provisional Application No. 61/786,460 filed on Mar. 15, 2013, each of which is incorporated by reference herein in its entirety.

FIELD OF INVENTION

The present invention relates to detection of a disturbance on an information transmission line, including, for example, disturbance location identification, disturbance type identification, disturbance-triggered sensory indicators, disturbance detection handling, or cable assemblies with respect to a physical transmission line.

SUMMARY

Aspects of the invention relate to a cable assembly with respect to a physical transmission line.

In some embodiments, a cable assembly may include an outer jacket, a printed circuit board including light emitting diodes, and a cable configured to transmit information. The outer jacket may include a channel opening, and the printed circuit board may be configured to be positioned within the channel opening and between the cable and the outer jacket.

In some embodiments, a cable assembly may include an inner jacket, an outer jacket, a printed circuit board including light emitting diodes, and a cable configured to transmit information. The inner jacket may include a channel opening, and the printed circuit board may be configured to be positioned within the channel opening and between the inner jacket and the outer jacket.

In some embodiment, an outer jacket for a cable that transmits information may include an outer layer, and an inner layer, where the inner layer comprises a channel opening to allow a plurality of light emitting diodes to be housed within the channel opening.

In some embodiments, an inner jacket for a cable that transmit information may include an inner layer, and an outer layer, where the outer layer comprises a channel opening to allow a plurality of light emitting diodes to be housed within the channel opening.

These and other aspects of the present patent application, as well as the methods of operation and functions of the related elements of structure and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the

2

present patent application. It shall also be appreciated that the features of one embodiment disclosed herein can be used in other embodiments disclosed herein. As used in the specification and in the claims, the singular form of “a”, “an”, and “the” include plural referents unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a system architecture, in accordance with one or more embodiments;

FIG. 2 illustrates an infrastructure management system, in accordance with one or more embodiments;

FIG. 3 illustrates a dashboard, in accordance with one or more embodiments;

FIG. 4 illustrates a zone screen, in accordance with one or more embodiments;

FIG. 5 illustrates a flowchart for monitoring alerts, in accordance with one or more embodiments;

FIG. 6 illustrates a fiber forensic graphical display, in accordance with one or more embodiments;

FIG. 7 illustrates a flowchart for processing alerts, in accordance with one or more embodiments;

FIG. 8 illustrates a flowchart of a trunk cable processing subprocess, in accordance with one or more embodiments;

FIG. 9 illustrates a flowchart of a create alarm subprocess, in accordance with one or more embodiments;

FIG. 10 illustrates a flowchart for a process to disable data, in accordance with one or more embodiments;

FIG. 11 illustrates a flowchart for processing open warnings, in accordance with one or more embodiments;

FIG. 12 illustrates a chart showing a process for case resolution, in accordance with one or more embodiments;

FIG. 13 illustrates a case detail screen, in accordance with one or more embodiments;

FIG. 14 illustrates a flowchart for continued monitoring during case management, in accordance with one or more embodiments;

FIG. 15 illustrates a system for facilitating detection of a disturbance on an information transmission line, in accordance with one or more embodiments;

FIG. 16 illustrates sensor data obtained from a sensor, in accordance with one or more embodiments;

FIG. 17 illustrates a physical transmission line and sensors placed at different locations on a physical transmission line, in accordance with one or more embodiments;

FIG. 18 illustrates sensor data obtained from sensors, in accordance with one or more embodiments;

FIG. 19 illustrates a system for identifying a location of a disturbance event, in accordance with one or more embodiments;

FIG. 20 illustrates a system for identifying a location of a disturbance event, in accordance with one or more embodiments;

FIG. 21 illustrates a user interface, in accordance with one or more embodiments;

FIG. 22 illustrates sensor data and signature data, in accordance with one or more embodiments;

FIG. 23 illustrates a comparison between sensor data and signature data, in accordance with one or more embodiments;

FIG. 24 illustrates tables including data, in accordance with one or more embodiments;

FIG. 25 illustrates a flowchart describing a method for identifying a location of a disturbance event on a physical transmission line, in accordance with one or more embodiments;

US 11,388,181 B2

3

FIG. 26 illustrates a flowchart describing a method for identifying a location of a disturbance event on a physical transmission line, in accordance with one or more embodiments;

FIG. 27 illustrates a flowchart describing a method for identifying a location of a disturbance event on a physical transmission line, in accordance with one or more embodiments;

FIG. 28 illustrates a flowchart describing a method for identifying a type of a disturbance event on a physical transmission line, in accordance with one or more embodiments;

FIGS. 29A and 29B illustrate a cable assembly, in accordance with one or more embodiments;

FIG. 30 illustrates a circuit, in accordance with one or more embodiments;

FIGS. 31A, 31B, 31C, and 31D illustrate a cable assembly, in accordance with one or more embodiments;

FIGS. 32A and 32B illustrate a cable assembly, in accordance with one or more embodiments;

FIG. 33 illustrates an architecture and operation of a visual indication system; and

FIG. 34 illustrates an architecture and operation of a visual indication system, in accordance with one or more embodiments.

DETAILED DESCRIPTION

All publications, patents, and patent applications cited in this specification are hereby incorporated by reference in their entirety. The detailed description provided below in connection with the appended drawings is intended as a description of exemplary embodiments and is not intended to represent the only forms in which the invention may be constructed or utilized. The same or equivalent functions and sequences may be accomplished by different embodiments as will be appreciated by those skilled in the art.

FIG. 1 illustrates a block diagram of a system 100 according to an embodiment. System 100 may be used to provide proactive real-time alarm monitoring of dark fiber intrusions and may distribute notification of alarms of suspected tampering to a variety of endpoints. System 100 may include a manager engine 101, a manager database server 102, a manager web server 103, and a manager engine listener 104. In an embodiment, system 100 may include one or more components that functions as any of the manager engine, manager database server, manager web server, and manager engine listener.

System 100 may integrate with a variety of network devices to offer alarm detection and alarm response capabilities in a consolidated system. In an embodiment, system 100 may integrate with Passive Optical Network (PON) equipment, Optical Circuit Switch equipment, Optical Test Access Point equipment, and Network Analyzers to stop and start data flow to network endpoints, re-route data flow, and record or further analyze data when alarms are detected and resolved. Alarm events may be captured in a case management oriented workflow for auditing and analytics.

System 100 may provide the ability for complete network mapping of components starting from a source Optical Line Terminal (OLT) down to an end user Optical Network Terminal (ONT). Network components may be enrolled and maintained in system 100 in a logical and efficient manner. System views and reports may be leveraged to inspect an entire network as well as each data run.

System 100 may handle the coordination of tasks between dark fiber alarm monitoring devices and PON equipment

4

through backend adapters leveraging Simple Network Management Protocol (SNMP) traps and Secure Shell (SSH) protocols. System 100 may be monitored actively and passively to assure events are not missed.

System 100 may offer a secure web user interface to provide network operations center (NOC) oriented dashboards for proactive monitoring. Notification of events may be handled in a guaranteed delivery manner over SMTP and HTTP to assure best effort notification to a targeted endpoint so first responders can focus on the status of the remaining system. Maps and images may be immediately provided with floor plan layouts overlaid with network diagrams for an alarmed area to reduce critical decision times for resolving alarms. System 100 may allow staff to identify a suspected intrusion event, isolate its location, notify responder groups, execute planned remediation, and track its history.

In an embodiment, system 100 offers a warning threshold technology to suppress the occurrence of nuisance alarms. A configurable threshold may allow system 100 to filter out accidental or environmental disturbances from actual intrusion attempts.

System 100 may integrate into an existing enterprise by providing consolidated alerts to 'north-bound' systems over SNMP. System 100 may also integrate with any existing Active Directory authentication system to assure its operation is consistent with pre-established IT security policies and site practices. System 100 may be supported by a relational database to provide redundancy, durability, recovery protection, and tools for data extraction and analysis.

In an embodiment, system 100 may provide health reports by providing analytics and reporting on all warnings and alarms captured by system 100. System 100 may provide trend reporting and predictive analysis. System 100 may publish and disseminate the results of the analysis to a configurable group of users at a configurable time period and frequency.

In an embodiment, system 100 may provide infrastructure management for PON Systems. System 100 may provide a graphical and textual depiction of an end to end path for a circuit. For example, one end may start from a port on an optical line terminal and/or network switch joined with a port on an intrusion detector then continue to an optical circuit switch then continue through a trunk cable then continue to a splitter then continue to a zone box then continue to a fiber run to an user area then continue to a user end device, such as an optical network terminal. Each of the devices, passive or active, and each cable run may be represented in the system graphically and textually.

System 100 may provide the ability to add, modify, or delete representative circuit paths. System 100 may track device types, identification numbers, and locations for each device. System 100 may display each circuit path overlaid on a physical diagram, such as a building or floor computer-aided design (CAD) diagram. System 100 may provide querying and reporting capabilities for each device. System 100 may highlight a circuit path when displayed in a graphical view.

Turning to FIG. 2, a schematic diagram showing an overview of a Protective Distribution System (PDS) and information technology (IT) infrastructure management system according to an embodiment is shown. In one embodiment, system 200 may be system 100 described above. In one embodiment, system 200 may manage an intrusion detector 202, which monitors a building 201. System 200 may provide the ability to receive alerts when intrusion detector 202 detects intrusion attempts. System 200 may

US 11,388,181 B2

5

also provide the ability to manage certain features of intrusion detector **202**. As will be explained in greater detail below, such features may include learning mode, configuration, enabling and disabling monitoring on a channel port, and reading and updating a threshold setting. Exemplary intrusion detectors that system **200** may integrate with are Network Integrity Systems' INTERCEPTOR, VANGUARD, and INTERCEPTOR LD2.

In one embodiment, system **200** tracks a floor **203** of building **201** that is monitored by intrusion detector **202**. Each monitored floor **203** may contain one or more zone groups **204**. Within each zone group **204** may be a collection of zones **205**, each of which may correspond to a single channel port **206** on intrusion detector **202**. Though not depicted in the figure, system **200** may also be used to manage a collection of campuses, each of which may contain a collection of buildings.

System **200** may manage a collection of intrusion detectors **202**. Intrusion detector **202** may contain a channel port **206**, which corresponds to a zone **205**. A zone **205** correlates to a physical location that is being monitored by system **200**. A zone **205** may have an image **207**, which may include computer-aided design drawings, first person perspective images, or video, to aid users in inspections. A zone **105** may also be associated with a contact personnel **208**. Contact personnel **208** may be notified in the event of an intrusion attempt.

System **200** may be configured so that a zone **205** has a data port address **209** associated with the zone to integrate with a data providing networking equipment, such as an optical circuit switch or optical line terminal and/or network switch. In the event of an intrusion attempt in zone **205**, system **200** may disable or re-route data by sending a command to a networking equipment using data port address **209**. System **200** provides the ability to enable or disable data on a specific port and also provide the ability to read and update details for a port. Some example devices that system **200** may integrate with are Tellabs PON, Zhong PON, and Motorola POL.

Zone **205** may also have a physical security device address **210** associated with the zone. In the event of an intrusion attempt in zone **205**, system **200** may adjust physical security including locking doors, recording on IP based cameras, etc. by sending a command to physical security address **210**.

System **200** may also manage an optical circuit switch **211**. Optical circuit switch **211** may provide the ability to disable, enable, or re-route an optical transmission. Optical circuit switch **211** may have an optical line terminal and/or network switch **212**. Optical line terminal and/or network switch **212** may convert and provide a fiber optical signal to a data network. System **200** may also provide the ability to perform a bulk enrollment of a cross connect defined during initial installation or subsequent reconfiguration. An example device that system **200** may integrate with is the Calient 5320 or CyberSecure Cyber Patch Panel.

Optical circuit switch **211** may have an optical test access point **213**. Optical test access point **213** may allow system **200** to provide an ability to route or copy network data. Optical test access point **213** may deliver an identical copy of network traffic to a network analytic tool, such as a network monitor **214**, a security monitor **215**, a network recorder **216**, a network analyzer **217**, and other analytic tools. An example of an optical test access point device that system **200** may integrate with is the Mimatrix OpticalTAP.

Turning to FIG. 3, a dashboard **300** according to an embodiment is shown. Dashboard **300** may provide a con-

6

solidate view from a system and allow network personnel to determine the health of a network with multiple visual indicators.

Intrusion detectors panel **301** may display a list of all intrusion detectors managed by a system. Each intrusion detector displays a colored icon for a channel port. The colored icons may correlate to a label provided in legend **307**. Each intrusion detector may be associated with a unique label, which may include information such as a user defined name, IP Address, etc. The background for the intrusion detector as shown in intrusion detector panel **301** may be programmed to change according to the status of the intrusion detector. For example, the background for an intrusion detector with a channel port in an alarmed state may be colored red. The list of intrusion detectors may be filtered to a building specific intrusion detector when a building is selected in a building drop down list **308** or when a building icon is selected in a map view panel **302**.

Map view panel **302** may be configured to display a map image with visual indicators for a building managed by a system. The location of the visual indicators may be based on the geographic coordinates of a building. The color of the visual indicator may provide a combined status for each of the intrusion detector's channel ports managed in a building. According to one embodiment, the background colors may be determined in the following hierarchy:

If one or more channel ports are in an alarmed state, the color will be red.

If one or more channel ports are in a warning state and no channel ports are in an alarmed state, the color will be yellow.

If no channel ports are in an alarmed or a warning state, the color will be green.

Building list **308** may contain the building names for all of the buildings managed by a system. Building list **308** may be set to a default option, e.g. option 'A1', if there are multiple buildings managed by a system. Otherwise, the list may default to a single building managed by a system. When a user selects a building, a system may filter a list of intrusion detectors in intrusion detector panel **301** to only show the devices managed in the selected building.

An incident log panel **303** may display a list of events captured or enacted by a system in response to an alert. In one embodiment, incident log panel **303** may display Incident Date, Room Name, Intrusion Detector Name, Zone Name, and Incident Message for an incident. An incident log may contain the most recent incidents for a given time parameter which may be configured in a system.

A summary report panel **304** may display a total number of zones monitored by a system. Also included may be the number of active alarms in a system as well as the number of active warnings. Summary report panel **304** may also include a chart of all warnings and alarms captured by a system in a specified time period, such as the last 7 days or the last 30 days.

An open incidents panel **305** may include a list of open cases. Open incidents panel **305** may list the ID, Date Opened, and Status for an open case.

An active warnings panel **306** may include a list of all open and active warnings. As will be described in more detail below, active warnings may be set when a set number of disturbances or alerts are captured in a defined amount of time before reaching a configured alarm threshold. The active warning feature may be known as a Zonar Warning System, a Visual Active Alert Indicator. Active warnings panel **306** may also display a graphical chart to show the number of disturbances or alerts captured by a system for a

US 11,388,181 B2

7

given zone as well as the alarm threshold level for the given zone. When there are no active incidents, a system may display the last number of warning events on the screen, such as the last 5 warning events.

Turning to FIG. 4, a zone screen display **400** according to an embodiment is shown. Zone screen display **400** may show a live representative view of a zone monitored by an intrusion detector. Zone screen display **400** may show a gauge **401**, which may be known as a Zonar Warning Gauge, which displays a current active warning count received by a zone and a current power level reading for a zone. In the event of receiving an alert, zone screen display **400** may show the current alert count and the numeric alarm threshold value by displaying the values in a gauge **401**. Similarly, in the event of receiving an alert, zone screen display **400** may show the severity of the alert by displaying a disturbance level in a power meter icon **402**.

In one embodiment, power meter icon **402** may display the following levels:

Minor—based on a configurable threshold on a lower end of a disturbance spectrum.

Moderate—based on a configurable threshold in between a Minor and a Major threshold.

Major—based on a configurable threshold on a higher end of a disturbance spectrum.

Critical—indicates a boundary alarm, which may occur when a cable is damaged or removed from an intrusion detector port.

Zone screen display **400** may also show a media **403** related to a zone. Media **403** may be in an image, video, or document format. A system may allow users with the appropriate privileges to add or remove a zone media and enter the required descriptive text for each media item. Zone screen display **400** may include additional section **404** to display information such as status of the zone, time of last alarm, alarm/warnings in the past 24 hours/7 days/30 days, and notification list for the zone.

Turning to FIG. 5, a flowchart for creating an alert **500** according to an embodiment is shown. In **501**, an intrusion detector monitors a fiber optic cable. In one embodiment, monitoring may be performed by comparing a light transmitted to a light received in order to detect if a disturbance has occurred. In other embodiments, monitoring may be performed on vibration readings, frequency readings, changes in dB, optical time-domain reflectometer (OTDR), acoustic readings, distance determination based on reflective sensors, or combinations thereof. When a disturbance is detected, the disturbance may be compared to a defined threshold in **502**. If the disturbance is less than the defined threshold, the intrusion detector may return to monitoring a fiber optic cable in **501**. If the disturbance is greater than a defined threshold, the intrusion detector may send an alert to a target based on a configured setting.

In one embodiment, in **503** and **504**, an intrusion detector configured to send simple network management protocol (SNMP) traps may send SNMP traps to configured targets. In **505** and **506**, an intrusion detector configured to send Syslog entries may send Syslog entries to configured targets.

In one embodiment, a detected disturbance may be presented to a user as a graphical representation. FIG. 6 shows a screen shot of one embodiment of a graphical representation of detected disturbances. Graph **601** shows a detected disturbance as a function of time. The graphical points may be plotted based on the level of dB difference registered on the transmission line during the disturbance and represented accordingly with a unique graphical icon. Additional graphical points may be plotted based on vibration and acoustic

8

calculations registered on the transmission line during the disturbance and represented accordingly with a unique graphical icon. Summary section **602** shows different characteristics of the detected disturbances. The graphical representation may include time characteristics of the detected disturbance including the start time, end time, and total duration of the detected disturbance. The graphical representation may include disturbance characteristics of the detected disturbance including the maximum optical loss measured in dB, the number of registered vibration or acoustic events, the detection of cable damage, and the total number of distinct disturbances. The graphical representation may be used by a user to determine whether an immediate alarm response is required and which alarm response team member would be able to perform the on-site inspection. Similarly, the graphical representation may be used to indicate to the user where to perform the onsite inspection first. The graphical representation showing a short duration with fluctuating dB loss may indicate that inspection starts where the transmission line is readily exposed such as in a telecommunications closet. The graphical representation showing a long duration starting with many vibration or acoustic disturbances followed by multiple fluctuating dB loss disturbances may indicate an injection of an optical tap and that the inspection include a visual inspection of the entire transmission line. The graphical representation showing optical signatures indicative of accidental contact with a low severity would be represented accordingly. Similarly, optical signatures of a sever event such as the insertion of a fiber optic tap would be represented accordingly. While the graphical representation shown in FIG. 6 and described herein depicts an exemplary graphical representation of the detected disturbance, other graphical representations arranged with different plot points may be implemented based on different interfaces with various intrusion detection hardware.

In FIG. 7, a flowchart for alert processing **700** by a system according to an embodiment is shown. In **701**, a system may keep an open port to listen for an alert. In **702**, the system determines if an alert has been received by a target. If an alert has been received, the system translates the alert to determine a zone number for the alert. In **703**, the system determines if the alert is a boundary alarm. Boundary alarms may be classified as critical severity. If the alert is a boundary alarm, the system creates an alarm as defined in 'create alarm' sub process **900**.

If the system determines that the alert is not a boundary alarm in **703**, the system may check in **704** to see if multiple warnings above a defined threshold or criteria in a have been received in a defined period of time. For example, the system may check to see if there have been 3 other previous warnings occurring within the past 24 hours for the zone. If the zone does have multiple warnings that meet a defined criteria, the system creates an alarm as defined in 'create alarm' sub process **900**.

If the system determines in **704** that the zone has not have multiple warnings that meet a defined criteria, the system may check to see if the zone has an active warning counter in **705**. The system creates a new warning counter for a zone in **706** if the zone does not have an active warning counter. If the zone does have an active warning counter, the system opens the warning counter in **707**. With an active warning counter identified for the zone, the system increments the warning count for the zone in **708**. In **709**, the system determines the status of the zone. If the zone is in a warning mode, the system proceeds to a trunk cable processing sub process **800**. A warning mode may be defined as a warning

US 11,388,181 B2

9

count of greater than 1. If the zone is not in a warning mode, the system sets the zone to a warning status in **710** and then proceeds to 'trunk cable processing' sub process **800**.

In one embodiment, the system evaluates trunk cable processing in a 'trunk cable processing' sub process **800**. After the trunk cable processing sub process, the system moves on to **711** to determine if the warning count exceeds the defined threshold for the zone. If the warning count exceeds the defined threshold for the zone, the system creates an alarm in 'create alarm' sub process **900** and then returns to **701** to listen for alerts. If the warning count does not exceed the defined threshold for the zone, the system returns to **701** to listen for alerts. While the flowchart shown in FIG. 7 and described herein depicts an exemplary workflow for processing an alert, other workflows arranged in a different order may be implemented.

In FIG. 8, a flowchart for 'trunk cable processing' sub process **800** according to an embodiment is shown. In **801**, a system determines if the zone is a trunk zone. In one embodiment, a trunk zone may be defined as a zone that includes a trunk cable. A trunk cable may be co-bundled with monitoring cables for each floor. At each floor, the cables dedicated to that floor may distribute out to the floors. A trunk cable and remaining floor cables may continue down a riser closet (e.g. communication network closets that traverse up and down an area of a building). Having a dedicated trunk zone that may be monitored by a system may allow for a logical separation of user zones (e.g. network cables distributing data throughout a floor of a building) from a riser closet and a source closet (e.g. place where network data for a building originates). Without a trunk cable, on an intrusion or disturbance, an investigator may be required to inspect an entire user zone and then back up a riser closet and back to a source closet. Logical separation may allow for meeting an inspection requirement, such as an inspection being required within 15 minute of an alert.

If the zone is a trunk zone, the system proceeds to **809** to evaluate the alert as a standard zone and returns to step **711** as described above. If the zone is not a trunk zone, the system continues to **802** to determine if the trunk zone is in a warning or an alarmed status. If the system is not in a warning or alarmed status, the system proceeds to **809** to evaluate the alert as a standard zone and returns to step **711** as described above. If the trunk zone is in a warning or an alarmed status, the system proceeds to **803** and determines if a warning time period has expired since the last received warning for the trunk zone. The warning time period may be configured by a user to a desired length. If the warning time period has expired, this may indicate an intrusion attempt on a separate zone in addition to an intrusion attempt on the trunk zone and the system proceeds to **809** to evaluate the alert as a standard zone and returns to step **711**.

If the system determines in **803** that the warning time period has not expired, this may indicate that there is an alert in a zone in conjunction with the trunk zone and the system proceeds to **804**. In **804**, the system determines if the zone warning mode has been set to a predetermined setting. In one embodiment, the predetermined setting may be 'Warning with Trunk Zone'. In one embodiment, if the zone does not have a warning mode of 'Warning with Trunk Zone' **804**, the system sets the warning mode to 'Warning with Trunk Zone' in **805** prior to moving onto **806**. In **806**, the system evaluates if all zones in the zone's zone group have warning modes set to 'Warning with Trunk Zone'. In one scenario, if a cable in a riser closet is disturbed, the trunk cable and all of the cables that are monitoring the floors below will set off

10

alerts. In this case, the floor cables will have a 'Warning with Trunk Zone' status so the system can separate these from a user zone. If not, the system proceeds to **809** to evaluate the alert as a standard zone and returns to step **711**.

If all zones in the zone's zone group have warning modes set to 'Warning with Trunk Zone', this may indicate that the entire zone group has received alerts in conjunction with the trunk zone. In that instance, the system will not evaluate the alert as a standard zone, but instead the system may suppress it. The system then proceeds to **807** to determine if the zone is set to active status. If not, the system sets the zone to active status in **808** and proceeds to continue to alert processing. While the flowchart shown in FIG. 8 and described herein depicts an exemplary workflow for a trunk cable processing sub process, other workflows arranged in a different order may be implemented.

Turning to FIG. 9, a flowchart for 'create alarm' sub process **900** according to an embodiment is shown. A system may create an alarm according to 'create alarm' sub process **900** when a zone receives a boundary alert, when a zone receives multiple warnings above a criteria, or when a zone warning count exceeds a defined threshold for the zone. In **901**, a system evaluates if a zone is a trunk zone. If the zone is a trunk zone, the system may retrieve the highest consecutive zone group with a warning mode of 'Warning with Trunk Zone' in **902**. A system may indicate this information in a case as described in more detail below.

A system may create and opens a case in **903**. If a case was opened due to a boundary alert, a system may notate the case accordingly. In **904**, a system may notify a personnel related to a zone. If a case was opened due to a boundary alert, a system may notate the notification accordingly. In **905**, a system may determine if a zone is configured to disable data. If yes, the system may perform a disable data sub process **1000**. In **906**, a system may determine if a zone is configured to update a physical security device. If yes, the system may perform the action based on a zone setting by sending a command to the physical security device management platform in **907**. In **908**, a system may determine if a zone is configured to re-route network data. If yes, the system re-routes data based on a zone setting by sending a command to an optical circuit switch in **909**. In **910**, a system may determine if a zone is configured to perform network analysis. If yes, the system performs an action based on a zone setting by sending a command to an optical test access point in **911**. A system may communicate with a network analytic tool based on a defined action. While the flowchart shown in FIG. 9 and described herein depicts an exemplary workflow for a create alarm sub process, other workflows arranged in a different order may be implemented.

In FIG. 10, a flowchart for 'disable data' sub process **1000** according to an embodiment is shown. In **1001**, a system may evaluate a zone type. In **1002**, if a zone is an outside plant zone, the system may collect all zones in a same data zone as the outside plant zone. The system may then proceed to **1006** to disable data in all of these zones.

In **1003**, a system may evaluate if a zone is a trunk zone. If yes, the system collects all zones up to and including the highest consecutive zone group with a warning mode of 'Warning with Trunk Zone' in **1004**. The system may then proceed to **1006** to disable data in all of these zones. In **1003**, if a system determines that a zone is not a trunk zone but is a user zone, the system may retrieve the current zone in **1005** and proceed to disable data in this zone in **1006**.

A system may be configured to disable data by directly communicating with an optical line terminal and/or network switch by sending a command to the optical line terminal

US 11,388,181 B2

11

and/or network switch. A system may also be configured to disabled data by communicating with an optical circuit switch by sending a command to the optical circuit switch. While the flowchart shown in FIG. 10 and described herein depicts an exemplary workflow for a disable data sub process, other workflows arranged in a different order may be implemented.

Turning to FIG. 11, a work flow for processing open warnings 1100 according to an embodiment is shown. In 1101, on a defined interval, a system may open all active warnings. In 1102, a system may determine if a warning time period has elapsed since last receiving a warning timestamp. If the warning time period has not elapse, the system may proceed to 1103 and wait for a defined interval before returning to check all active warnings. If the warning time period has elapsed, the system may proceed to 1104 to determine if a zone is a trunk zone. If the zone is not a trunk zone, the system may proceed to 1107 and close an active warning. If the zone is a trunk zone, the system may collect all zones up to and including the highest consecutive zone group with a warning mode of 'Warning with Trunk Zone' in 1105 and may then proceed to 1106. In 1106, a system may check if the trunk zone is alarmed. If not, the system may close the active warning in 1107. In 1108, a system may set a zone warning count to zero. In 1109, a system may set a zone status to active monitoring. While the flowchart shown in FIG. 11 and described herein depicts an exemplary workflow for processing open warnings, other workflows arranged in a different order may be implemented.

FIG. 12 shows a case resolution process according to an embodiment. In 1203, when a case is created, a zone monitor 1201 may open the case and review the case details. The case details displayed by a system may include warning count, zone type, zone images, zone inspection guide, notified contact personnel, and status of the data network. A case detail screen according to one embodiment is shown in FIG. 13.

In 1204, zone monitor 1201 may dispatch an investigator 1202 assigned to a zone. In 1206, zone monitor 1201 may record zone investigator's 1202 name. In 1205, zone investigator 1202 may investigate a zone based on a Standard Operating Procedure defined by a system for a zone. In 1207, zone investigator 1202 may document evidence such as images or videos of the inspection. In 1208, upon completion of an investigation, zone investigator 1202 may relay a full report in back to zone monitor 1201, including investigation evidence, a written report, and a final determination. Final determinations may include items such as intrusion, accidental contact, unscheduled maintenance, natural disaster, and other items.

In 1209, zone monitor 1201 may record zone investigator's 1202 report into a system. In 1210, a system may enable zone monitor 1201 to reset monitoring on a zone.

In 1211, when zone monitor 1201 resets monitoring on a zone, a system may check to see if data was disabled in a zone. If so, the system may allow zone monitor 1201 to restore data to the zone in 1212. Zone monitor 1201 may then restore data to the zone.

In 1213, a system may then close a case and track a time stamp for each event for audit and reporting purposes. While the workflow for a case resolution process as shown in FIG. 12 and described herein depicts an exemplary workflow, other workflows arranged in a different order may be implemented.

In an embodiment, when a case is open and under review, a system may continue to monitor for new alerts in a zone. FIG. 14 shows a flowchart 1400 of a process for a system to

12

continue monitoring during a case management. In 1401, a system may determine if a new alert is detected in a zone. In 1402, if a new alert is detected, the system may update an interface with visual and audible indicators, such as an Eagle Eye Zonar warning. This scenario may occur if an intrusion attempted is continuing. This process may provide an investigator situational awareness and allow for additional safety or response measures.

In 1403, a system may require a user to notify an investigator of the Eagle Eye Zonar warning. In 1404, a system may determine if a user has notified an investigator. If not, the system may return to 1403 to require a user to notify an investigator. In 1405, after a user notifies an investigator, the system may update a case note with information and timestamp for the Eagle Eye warning detection and user acknowledgement. In 1406, a system may then allow a user to continue with a case resolution process. While the flowchart shown in FIG. 14 and described herein depicts an exemplary workflow for a process to continue monitoring during a case management, other workflows arranged in a different order may be implemented.

According to an embodiment, a system may allow a user with an appropriate privilege the ability to modify a case resolution workflow. A system may allow for adding or removing steps into a workflow. A system may allow for routing and re-routing approval or disapproval functions to a user, collection of users, roles or a collection of roles in a system. Where appropriate, a system may allow for modification of a workflow through a graphically based user interface.

In one embodiment, a system may be configured for predictive analysis. A system may calculate the captured alert signatures (duration, count, maximum/minimum/average power, etc.) for a case as well as an associated case resolution status. A system may provide artificial intelligence capabilities in analyzing an alert signature and a resolution to compute likelihood scores for possible causes for an alert.

For a case, a system may use a predictive analysis to offer likelihood scores on the case resolutions status. For each warning, a system may provide a real-time likelihood score for a cause of an alert.

Other features of a system may provide the ability to continuously monitor a given IP address range to discover and enroll unregistered intrusion detectors. A system may allow a user to create a new enrollment task. An enrollment task may include:

- Starting IP Address
- Ending IP Address
- Login ID for Intrusion Detector
- Password for Login ID for Intrusion Detector
- Frequency at which the Enrollment Task should run (Never, Daily, Weekly)
- SNMP Credentials for communication with the Intrusion Detector
- Option to All Remote Reset of the Channel Ports of the Intrusion Detector
- Option to Disable Data in the Zones when an Alarm occurs
- Warning Threshold Count
- Warning Threshold Time Period
- Alarm Response for Intrusion Alerts (None, Report, Report & Halt, Halt)
- Alarm Response for Boundary Alerts (None, Report, Report & Halt, Halt)
- Alarm Response for Smart Filter Detect Alerts (None, Report, Report & Halt, Halt)

US 11,388,181 B2

13

Device Availability Time Period

During enrollment, a system may query a discovered device and gather device specific information such as the model and the port count of the device. A system may use the information to dynamically enroll the device. A system may provide the ability to discover a variety of device models and types from one enrollment task.

After enrollment completes, a system may read an intrusion detector threshold setting. A system may disable monitoring on channel ports that are determined to not have a fiber cable plugged into it. A system may provide a wizard based workflow to allow a user to provide additional information to configure an enrolled device.

According to another embodiment, a system may provide the ability to set a specific channel port on an intrusion detector into a Learning Mode or Auto Configure. In this mode, an intrusion detector observes a fiber for a channel port for a configurable period of time to determine an optimal monitoring parameter that may be used for monitoring intrusions, excessive optical gains/losses or environmental changes.

A system may be configured to allow a user with an appropriate privilege an option to perform Learning Mode. When the option is selected, the system may present an allowed user with a screen offering various time periods. When a user initiates a task in a system, the system sends an appropriate command to an intrusion detector to begin Learning Mode. A system may set the channel port Report only for any alert and not send Halt alerts. At any time during Learning Mode, a system may allow a user to abort Learning Mode. A system may continue to receive a detected alert during Learning Mode and may record the results in the system for further consideration by a user.

When Learning Mode completes, a system may receive a notification from an intrusion detector. A system may read and record a threshold setting determined during Learning Mode and associate the setting to a specific zone. A system may reset a channel port back from Report only to a previous setting.

A system may read and record a current threshold setting of a channel port of an intrusion detector and associate the setting to a specific zone. For a setting, a system may indicate if the setting was Learned, set by Default, or set by a User.

A system may allow a user with an appropriate privilege the ability to sync a setting from a device to a system. A system may allow a user with an appropriate privilege the ability to edit any or all of the settings. When a user initiates a task in a system to update a setting, the system may send an appropriate command to an intrusion detector to update the settings based on the user provided values. Any settings unchanged by a user remain unaffected.

A system may be deployed for various purposes. In one embodiment, a system may be used to verify whether a data infrastructure is suitable for alarmed carrier PDS. This testing process maybe used pre-deployment on existing cables and conduit or during post-deployment testing process to validate new installations of alarmed cables and conduit.

FIG. 15 shows a system 1500 for facilitating detection of a disturbance on an information transmission line, in accordance with one or more embodiments. As shown in FIG. 15, system 1500 may include server(s) 1502, client device 1504 (or client devices 1504a-1504n), network 1550, database 1532, sensors 1522, physical transmission line 1526, visual indication 1528, and/or other components. Server 1502 may include disturbance identifying subsystem 1512, communi-

14

cation subsystem 1514, presentation subsystem 1516, updating subsystem 1518, and/or other components. Each client device 1504 may include any type of mobile terminal, fixed terminal, or other device. By way of example, client device 1504 may include a desktop computer, a notebook computer, a tablet computer, a smartphone, a wearable device, or other client device. Users may, for instance, utilize one or more client devices 1504 to interact with one another, one or more servers, or other components of system 1500. It should be noted that, while one or more operations are described herein as being performed by particular components of server 1502, those operations may, in some embodiments, be performed by other components of server 1502 or other components of system 1500. As an example, while one or more operations are described herein as being performed by components of server 1502, those operations may, in some embodiments, be performed by components of client device 1504. Further, although the server 1502, client device 1504, sensors 1522, physical transmission line 1526, visual indication 1528, and database 1532 are illustrated as being separate and connected via network 1550, it should be understood that one or more of the server 1502, client device 1504, sensors 1522, physical transmission line 1526, visual indication 1528, and database 1532 may be co-located. Further, although the database 1532 is illustrated as being separate from the server 1502 and the client device 1504, the database 1532 may be located within the client device 1504 and/or server 1502. One or more components (and their functions) of the systems illustrated in FIGS. 1 and 2 may correspond to one or more components (and their functions) of the systems illustrated in FIGS. 15, 33, and 34, and vice versa. Further, one or more functions described above with regard FIGS. 1-14 may be performed by one or more components of the systems illustrated in FIGS. 15, 17, 19, 20, 33, and 34. One or more functions described below with regard to FIGS. 15-34 may be performed by one or more components of the systems illustrated in FIGS. 1 and 2.

Sensor-Based Disturbance Detection and Shutdown of Network Data Flow

In some embodiments, server 1502, via sensors 1522, may monitor the physical transmission line 1526 (e.g., a fiber optic information transmission line). As an example, FIG. 7 describes a system that may keep an open port to listen for an alert (see step 701 in FIG. 7). Further, in some embodiments, system 1500 may detect, via one or more sensors 1522, a disturbance on a physical transmission line, where the detected disturbance does not exceed a first present threshold for triggering alerts of a first alert type. With respect to FIG. 7, for example, a system may determine whether a zone has multiple warnings that meet one or more predefined criteria (see step 704 in FIG. 7). System 1500 may also detect, via one or more sensors 1522, a disturbance on the physical transmission line, wherein the detected disturbance does not exceed a first preset threshold for triggering a network data flow shutdown response. With respect to FIG. 2, for example, a system may disable or re-route data by sending a command to a networking equipment using data port address in the event of an intrusion attempt. The system may enable or disable data on a specific port and obtain details for the port.

Additionally, in some embodiments, the system 1500 (e.g., server 1502) may determine, responsive to the detection via the sensor 1522, a count for a number of disturbances within a preset time period that do not exceed the first preset threshold and determine, whether the count, for the number of disturbances that do not exceed the first preset threshold, exceeds a second preset threshold, wherein the

US 11,388,181 B2

15

second preset threshold corresponds to a preset number of allowable disturbances, not exceeding the first preset threshold and within the preset time period, before one or more alerts of the first alert type are to be triggered. Further, in some embodiments, an alert may be triggered of a first type responsive to a determination that the count exceeds the second preset threshold. With respect to FIG. 7, for example, a warning counter may increment a warning count for a zone when it is determined that the zone does not have multiple warnings that meet one or more predefined criteria (see steps 704, 705, 707, and 708 in FIG. 7), and an alarm may be triggered when the warning count exceeds a predefined threshold (see steps 711 and 900 in FIG. 7). Also, in some embodiments, the network data may be caused to be shut down to one or more network endpoints proximate to the detected disturbance on the physical transmission line response to a determination that the count exceeds the second preset threshold. As discussed, for example, a system may disable or re-route data by sending a command to a networking equipment using data port address in the event of an intrusion attempt. The system may enable or disable data on a specific port and obtain details for the port.

Disturbance Location and/or Type Identification

In some embodiments, system 1500 may identify a location of a disturbance on a physical transmission line. Server 1502 may obtain sensor data from sensors 1522 located on a physical transmission line 1526 (e.g., obtain first sensor data from a first sensor and second sensor data from a second sensor). The sensors 1522 may be optical sensors, electrical sensors, acoustical sensors, and/or fiber bragg grating (FBG) sensors and may be placed at different locations of the physical transmission line 1526. These sensors 1522 may be capable of detecting one or more disturbance events that occur on or near the physical transmission line 1526. For example, the optical sensors may be able to detect optical disturbance events, the electrical sensors may be able to detect electrical disturbance events, and the acoustical sensors may be able to detect acoustical disturbance events. Although only optical sensors, electrical sensors, acoustical sensors, and/or fiber bragg grating (FBG) sensors are discussed above, it should be understood that one or more other types of sensor may be used to detect disturbance events on the physical transmission line 1526. The sensor data may be received by the server 1502 from the sensors 1522 on a continuous basis or may be received upon request. Continuous reception of the sensor data from the sensors 1522 may allow the system 1500 to continuously monitor the physical transmission line 1526 and identify a location of a disturbance event on the physical transmission line 1526. The sensor data received from the sensors 1522 may include measured values of one or more disturbance events (e.g., first sensor data from a first sensor may include first measured values of the disturbance event, second sensor data from a second sensor may include second measured values of the disturbance event, etc.) over a length of time. For example, FIG. 16 illustrates sensor data obtained from a sensor (from among sensors 1522) that includes peaks and valleys (e.g., measured values of a disturbance event) over a length of time. These peaks and valleys over the length of time illustrate an occurrence of a disturbance event and these peaks and valleys can be used to identify a location of the disturbance event and a type of the disturbance event.

In some embodiments, the sensors 1522 may be located at predetermined positions on the physical transmission line 1526. Information regarding the location of the sensors 1522 on the physical transmission line 1526 may be stored in a sensor database 1536. In addition to the information regard-

16

ing the location of the sensors 1522, information regarding the distances between these sensors 1522 may also be stored in the sensor database 1526. FIG. 17 illustrates a physical transmission line (see pipe sections #1, #2, and #3) and sensors (see sensors S1, S2, S3, and S4) placed at different locations on the physical transmission line. The distance between sensors S1 and S2 may be equal to the distance between sensors S3 and S2 (and S2 and S4). Alternatively, the distances between adjacent sensors may be different. When sensors measure disturbance events (e.g., based on detected disturbance events), server 1502 (via, for example, communication subsystem 1514) may obtain sensor data that includes measured values of the disturbance events over a length of time. For example, FIG. 18 illustrates sensor data 1801, 1802, and 1803 obtained from sensors S1, S2, and S3, respectively. The sensor data 1801, 1802, and 1803 may include measured values (e.g., as measured in gain or loss in optical power, acoustical power, and/or electrical resistance) of a disturbance event over a length of time. The measured values may correspond to either light or sound disturbances (e.g., changes in ambient environmental conditions) that the sensors may detect. Sensor data 1801 may include measured values of a disturbance event by sensor S1, sensor data 1802 may include measured values of the same disturbance event by sensor S2, and sensor data 1803 may include measured values of the same disturbance event by sensor S3. For example, when there is a disturbance event, more than one sensor may detect the disturbance event and output its own corresponding sensor data. The sensor data 1801, 1802, and 1803 that include measured values of a disturbance event by the sensors S1, S2, and S3, respectively, may correspond to a single disturbance event or multiple different disturbance events.

In some embodiments, the server 1502 (e.g., disturbance identifying subsystem 1512) may determine an initial detection time of the measured values based on the obtained sensor data (or a portion of the obtained sensor data). For example, server 1502 may determine a first initial detection time T1 of the first measured values (see sensor data 1801 in FIG. 18), a second initial detection time T2 of the second measured values (see sensor data 1802 in FIG. 18), and a third initial detection time T3 of the third measured values (see sensor data 1803 in FIG. 18). Additionally or alternatively, the server 1502 may determine other detection times. For example, server 1502 may determine detection times T4, T5, and T6 (see broken line of box 1810 intersecting sensor data 1801, 1802, and 1803) of the first measured values (see sensor data 1801 in FIG. 18), the second measured values (see sensor data 1802 in FIG. 18), and the third measured values (see sensor data 1803 in FIG. 18), respectively, based on the obtained sensor data 1801, 1802, and 1803. The server 1502 (e.g., disturbance identifying subsystem 1512) may determine a time difference between detections times (e.g., difference between T1 and T2, T2 and T3, T1 and T3, T4 and T5, T5 and T6, and/or T4 and T6) and may approximate (i) a first distance between the disturbance event and the first sensor based on a determined time difference, a known constant (e.g., speed of sound and/or speed of light), and a known length of the physical transmission line (or a section of the physical transmission line), (ii) a second distance between the disturbance event and the second sensor based on a determined time difference, the known constant, and a known length of the physical transmission line (or a section of the physical transmission line), and (iii) a third distance between the disturbance event and the third sensor based on a determined time difference, the

US 11,388,181 B2

17

known constant, and a known length of the physical transmission line (or a section of the physical transmission line).

The server **1502** (e.g., disturbance identifying subsystem **1512**) may identify a location of the disturbance event on the physical transmission line based on the approximated distances of the sensors from the disturbance event. In addition, the location of the disturbance event on the physical transmission line may be identified further based on locations of these sensors on the physical transmission line. For example, the server **1502** may retrieve the information regarding the location of the sensors from the sensor database **1536** and utilize this information to identify the location of the disturbance event on the physical transmission line. Additionally, the server **1502** may retrieve information regarding the distance between the sensors from the sensor database **1536** and utilize this information to identify the location of the disturbance event on the physical transmission line. Although the example provided above describes three sensors and three sensor data, it should be understood that a location of the disturbance event on the physical transmission line may be identified based on sensor data obtained from two sensors. In summary, the system **1500** may use time difference (e.g., time of flight) between sensor data of different sensors to determine and identify a location of the disturbance event on the physical transmission line. Additionally, the server **1502** (for example disturbance identifying subsystem **1512**) may compare the sensor data **1801**, **1802**, and **1803** to each other (e.g., by comparing the time durations of the sensor data, peak/valley magnitudes of the sensor data, etc.) to determine whether the sensor data **1801**, **1802**, and **1803** correspond to a single disturbance event or multiple different disturbance events on the physical transmission line. For example, in FIG. **18**, the comparison of the sensor data **1801**, **1802**, and **1803** within box **1810** suggests that the sensor data **1801**, **1802**, and **1803** correspond to a single disturbance event.

Further, in some embodiments, the location of a disturbance event on a physical transmission line (e.g., a sensing fiber) may be determined/identified using a sensing device **1900** (e.g., a circuit or meter that reads resistance and/or current, or an optical interrogator) and a sensor **1903** (e.g., a fiber bragg grating (FBG) sensor) illustrated in FIG. **19**. The sensing device **1900** may be connected to the sensor **1903** via a port/channel and may acquire data sensed by the sensor **1903**.

FIG. **19** illustrates a sensing device **1900** that emits a beam of light **1901** to a reflecting sensor **1903** via the sensing fiber **1906**, and based on the sensor **1903**, a specific and known wavelength of light **1904** is reflected via the sensing fiber **1906**. A disturbance event on the sensing fiber **1906** may alter the reflected light's wavelength, amplitude, and/or other properties of light along distance B (e.g., **1905** in FIG. **19**). The sensing device **1900** may gather sensing data based on the reflected light **1904**. The sensing data may include information regarding timestamp values assigned to a light beam **1901** emitted by the sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903** and information regarding a property of the light beam **1904** reflected back to the sensing device **1900**. The sensing device **1900** may provide the sensing data to the server **1502** (based on a wired or wireless connection between the server **1502** and the sensing device **1900**). The server **1502** may then calculate a roundtrip time of the light beam **1901** emitted by the sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903** based on the assigned timestamp values. Further, the server **1502**, based on the received sensing data

18

from the sensing device **1900**, may determine a change in properties of the light beam **1901** emitted by the sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903** by comparing the properties (e.g., amplitude, frequency, wavelength, power variance, etc.) of the reflected light beam **1904** to the properties of a known light beam that is reflected by sensor **1903** with and/or without a disturbance event on the sensing fiber **1906**. In other words, the sensing device **1900** may provide raw data to the server **1502**, and the server **1502** may calculate the roundtrip time and determine the change in properties based on such raw data. Alternatively, the sensing device **1900** may calculate the roundtrip time of the light beam **1901** emitted by the sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903** based on the assigned time stamp values. Also, alternatively, the sensing device **1900** may determine the change in properties of the light beam **1901** emitted by the sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903** by comparing the properties (e.g., amplitude, frequency, wavelength, power variance, etc.) of the reflected light beam **1904** to the properties of a known light beam that is reflected by sensor **1903** with and/or without a disturbance event on the sensing fiber **1906**. The properties of known light beams may be stored in the database **1532** and may be retrieved by the server **1502** and/or sensing device **1900** for comparisons with the reflected light beam **1904**.

Based on the sensing data, the server **1502** (e.g., the disturbance identifying subsystem **1512**) may identify the location of the disturbance event on the physical transmission line. In other words, the server **1502** may identify the location of the disturbance event on the physical transmission line **1906** (and may identify the distance of the disturbance event from the sensing device **1900**) based on the roundtrip time of the light beam **1901** emitted by the sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903** and the change in the property (or multiple properties) of the light beam **1901** emitted by the sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903**. The server **1502** may also be able to determine a length of the distance event (e.g., start and end locations of the disturbance event) based on the comparison of the properties (e.g., wavelength, power variance, etc.) of the reflected light beam **1904** to the properties of a known light beam that is reflected by sensor **1903** with and/or without a disturbance event on the sensing fiber **1906**. For instance, the wavelength of the reflected light beam **1904** may be compared to a baseline wavelength to determine start and end locations of the disturbance event on the physical transmission line. Also, the power variance of the reflected light beam **1904** may be compared to a baseline power variance to determine start and end locations of the disturbance event on the physical transmission line. Further, the detection times of the start and end of peaks and valleys of the sensor data (along with a known constant) may also be used to determine the start and end locations of the disturbance event on the physical transmission line. Alternatively, the sensing device **1900**, based on the sensing data, may identify the location of the disturbance event on the physical transmission line **1906** (and may identify the distance of the disturbance event from the sensing device **1900**) based on the roundtrip time of the light beam **1901** emitted by the sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903** and the change in the property (or multiple properties) of the light beam **1901** emitted by the

US 11,388,181 B2

19

sensing device **1900** and reflected back (e.g., light **1904**) to the sensing device **1900** by the sensor **1903**. Also, alternatively, the sensing device **1900** may determine a length of the distance event (e.g., start and end locations of the disturbance event) based on the comparison of the properties (e.g., wavelength, power variance, etc.) of the reflected light beam **1904** to the properties of a known light beam that is reflected by sensor **1903** with and/or without a disturbance event on the sensing fiber **1906**. The properties of known light beams may be stored in the database **1532** and may be retrieved by the server **1502** and/or sensing device **1900** for comparisons with the reflected light beam **1904**.

Although only one sensor is illustrated in FIG. **19**, it should be understood that multiple sensors may be used and sensing data from each sensor may be gathered by the sensing device **1900**. Additionally, more than one sensing device **1900** may be placed at different locations of the physical transmission line to gather sensing data, which may then be obtained by the server **1502**. The known distances A (see **1902** in FIG. **19**) and B (see **1905** in FIG. **19**), a known constant (e.g., speed of light and/or sound), and time resolution capabilities of the sensing device **1900** can be taken into account to identify the location of the disturbance event on the physical transmission line. Additionally, the location of the disturbance event on the physical transmission line may be identified further based on a location of the sensing device on the physical transmission line. The information regarding a location of one or more sensing devices on the physical transmission line may be stored in the sensor database **1536**, and such information may be retrieved by, for example, the server **1502** and/or the sensing device **1900**.

Further, in some embodiments, the location of a disturbance event on a physical transmission line (e.g., a sensing fiber) may be determined/identified using a sensing device **2000** (e.g., a circuit or meter that reads resistance and/or current, or an optical interrogator) and sensors **2004** and **2005** (e.g., fiber bragg grating (FBG) sensors) illustrated in FIG. **20**. The sensors **2004** and **2005** may be connected to the sensing device **2000** either individually or in series to a port/channel on the sensing device **2000**, and the sensing device **2000** may acquire data sensed by the sensors **2004** and **2005**.

FIG. **20** illustrates a sensing device **2000** that emits a beam of light **2001** to a reflecting sensor **2004** via a sensing fiber **2009**, and based on the sensor **2004**, a specific and known wavelength of light **2006** is reflected via the sensing fiber **2009**. A disturbance event on the sensing fiber **2009** may alter the reflected light's wavelength, amplitude, and/or other properties of light along distance B (e.g., **2008** in FIG. **20**). Further, the sensing device **2000** may emit another beam of light **2002** (e.g., this may be a time source signal such as an alternating beam of light at a specific interval) that is reflected (see **2007** in FIG. **20**) against another sensor **2005** at an alternate wavelength from the light beam **2001** and/or **2006**. The other beam of light **2002** may be emitted via the sensing fiber **2009** and reflected (see **2007** in FIG. **20**) back to the sensing device **2000** via the sensing fiber **2009**. The sensing device **2000** may gather sensing data based on the reflected light **2006** and **2007**. The sensing data may include information regarding a change in a property of the light beam **2001** emitted by the sensing device **2000** and reflected back (e.g., light **2006** in FIG. **20**) to the sensing device **2000** by sensor **2004** and information regarding timestamp values assigned to light beam **2002** emitted by the sensing device **2000** and reflected (e.g., light **2007**) back to the sensing device **2000** by sensor **2005**. The sensing device **2000** may provide the sensing data to the server **1502** (based

20

on a wired or wireless connection between the server **1502** and the sensing device **2000**).

The server **1502** may then calculate a roundtrip time of the light beam **2002** emitted by the sensing device **2000** and reflected back (e.g., light **2007**) to the sensing device **2000** by sensor **2005** based on the assigned timestamp values. The time source signal (see **2002** and **2007** in FIG. **20**) may be used to establish a timing sequence, which based on a known distance can establish an internal timestamp that correlates to the detected light properties used for disturbance detection. Further, the server **1502**, based on the received sensing data from the sensing device **2000**, may determine the change in properties of the light beam **2001** emitted by the sensing device **2000** and reflected back (e.g., light **2006**) to the sensing device **2000** by sensor **2004** by comparing the properties (e.g., amplitude, frequency, wavelength, power variance, etc.) of the reflected light beam **2006** to the properties of a known light beam that is reflected by sensor **2004** with and/or without a disturbance event on the sensing fiber **2009**. In other words, the sensing device **2000** may provide raw data to the server **1502**, and the server **1502** may calculate the roundtrip time and determine the change in properties based on such raw data. Alternatively, the sensing device **2000** may calculate the roundtrip time of the light beam **2002** emitted by the sensing device **2000** and reflected back (e.g., light **2007**) to the sensing device **2000** by sensor **2005** based on the assigned timestamp values. Also, alternatively, the sensing device **2000** may determine the change in properties of the light beam **2001** emitted by the sensing device **2000** and reflected back (e.g., light **2006**) to the sensing device **2000** by sensor **2004** by comparing the properties (e.g., amplitude, frequency, wavelength, power variance, etc.) of the reflected light beam **2006** to the properties of a known light beam that is reflected by sensor **2004** with and/or without a disturbance event on the sensing fiber **2009**. The properties of known light beams may be stored in the database **1532** and may be retrieved by the server **1502** and/or sensing device **2000** for comparisons with the reflected light beam **2006**.

Based on the sensing data, the server **1502** (e.g., the disturbance identifying subsystem **1512**) may identify the location of the disturbance event on the physical transmission line. In other words, the server **1502** may identify the location of the disturbance event on the physical transmission line **2009** (and may identify the distance of the disturbance event from the sensing device **2000**) based on the roundtrip time of the light beam **2002** emitted by the sensing device **2000** and reflected back (e.g., light **2007**) to the sensing device **2000** by the sensor **2005** and the change in the property (or multiple properties) of the light beam **2001** emitted by the sensing device **2000** and reflected back (e.g., light **2006**) to the sensing device **2000** by the sensor **2004**. The server **1502** may also be able to determine a length of the distance event (e.g., start and end locations of the disturbance event) based on the comparison of the properties (e.g., wavelength, power variance, etc.) of the reflected light beam **2006** to the properties of a known light beam that is reflected by sensor **2004** with and/or without a disturbance event on the sensing fiber **2009**. For instance, the wavelength of the reflected light beam **2006** may be compared to a baseline wavelength to determine start and end locations of the disturbance event on the physical transmission line. Also, the power variance of the reflected light beam **2006** may be compared to a baseline power variance to determine start and end locations of the disturbance event on the physical transmission line. Alternatively, the sensing device **2000**, based on the sensing data, may identify the location of

US 11,388,181 B2

21

the disturbance event on the physical transmission line **2009** (and may identify the distance of the disturbance event from the sensing device **2000**) based on the roundtrip time of the light beam **2002** emitted by the sensing device **2000** and reflected back (e.g., light **2007**) to the sensing device **2000** by the sensor **2005** and the change in the property (or multiple properties) of the light beam **2001** emitted by the sensing device **2000** and reflected back (e.g., light **2006**) to the sensing device **2000** by the sensor **2004**. Also, alternatively, the sensing device **2000** may determine a length of the distance event (e.g., start and end locations of the disturbance event) based on the comparison of the properties (e.g., wavelength, power variance, etc.) of the reflected light beam **2006** to the properties of a known light beam that is reflected by sensor **2004** with and/or without a disturbance event on the sensing fiber **2009**. The properties of known light beams may be stored in the database **1532** and may be retrieved by the server **1502** and/or sensing device **2000** for comparisons with the reflected light beam **2006**.

Although only two sensors are illustrated in FIG. **20**, it should be understood that more than two sensors may be used and sensing data from each sensor may be gathered by the sensing device **2000**. Additionally, more than one sensing device **2000** may be placed at different locations of the physical transmission line to gather sensing data, which may then be obtained by the server **1502**. The known distances A (see **2003** in FIG. **20**) and B (see **2008** in FIG. **20**), a known constant (e.g., speed of light and/or sound), and internal timestamps can be taken into account to identify the location of the disturbance event on the physical transmission line. Additionally, the location of the disturbance event on the physical transmission line may be identified further based on a location of the sensing device on the physical transmission line. The information regarding a location of one or more sensing devices on the physical transmission line may be stored in the sensor database **1536**, and such information may be retrieved by, for example, the server **1502** and/or the sensing device **2000**.

The identified location of the disturbance event may be presented/displayed to a user via a user interface (see presentation subsystem **1516** in FIG. **15**). As illustrated in FIG. **21**, a location **2100** of a disturbance event can be identified on a physical transmission line that includes a plurality of sensors **S1**, **S2**, **S3**, and **S4**. The user interface may also present/display the identified location of the disturbance event as a location **2104** within a building and/or a location **2103** within a floor plan. The user interface may also present/display a type of the disturbance event. For example, in FIG. **21**, the disturbance event is identified as a potential hammer tap (see **2101** in FIG. **21**). The user interface may request a user to confirm the accuracy (via buttons **2102** in FIG. **21**) of the identified type of disturbance event.

When a location of the disturbance event is identified, the server **1502** (e.g., communication subsystem **1514**) may communicate a signal to the physical transmission line. Such a signal may disable (or cause shut down of) a portion of the physical transmission line that includes the disturbance event and re-route the information transmitted via the physical transmission line such that the portion of the physical transmission line that includes the disturbance event does not transmit the information. For example, as noted above, the server **1502** may be able to determine a length of the disturbance event (e.g., start and end locations of the disturbance event) based on the comparison of the properties (e.g., wavelength, power variance, etc.) of a reflected light beam (see FIGS. **19** and **20**) to the properties of a known

22

light beam that is reflected by sensor with and/or without a disturbance event on a sensing fiber. Based on the length of the disturbance event on the physical transmission line, the server **1502** may determine which portion of the physical transmission line needs to be disabled (e.g., temporarily) and determine a new route for the transmission of information via the physical transmission line. It should be understood that only a specific portion of the physical transmission line (e.g., the portion corresponding to the identified location of the disturbance event) may be disabled, while other portions of the physical transmission line may be allowed to function normally (e.g., other portions of the physical transmission line where no disturbance event has been identified).

In some embodiments, system **1500** may identify a type of a disturbance event on a physical transmission line based on a comparison of the obtained sensor data and stored signature data. Signature data may correspond to previous disturbance events and may include previously measured values over a length of time. Signatures files that include signature data may be stored in a signature database **1534** and may be retrieved by the server **1502**. The server **1502** may obtain (via, for example, the communication subsystem **1514**) signature files corresponding to previous disturbance events from the signature database **1534**. Each of the signature files may include signature data including previously measured values of the previous disturbance events over a length of time. For example, a first signature file may correspond to a hammer tap, a second signature file may correspond to a drill, a third signature file may correspond to a human voice, etc. FIG. **22** illustrates a hammer tap **2200** (which results in hammers sounds) on a physical transmission line (which includes a plurality of sensors **S1**, **S2**, and **S3**), which results in the generation of sensor data **2201** by one of the sensors. A signature file including a portion of the sensor data **2202** and other data **2203** may be generated based on the sensor data **2201** and the signature file may be stored in the signature database **1534**.

The server **1502** (e.g., disturbance identifying subsystem **1512**) may compare sensor data (which may be obtained from sensors **1522**) and signature data of the signature files obtained from the signature database **1534** and based on such a comparison, the server **1502** (e.g., disturbance identifying subsystem **1512**) may determine a confidence value for each of the signature files based on the comparison of the sensor data with the signature data of the signature files. For example, if the obtained sensor data includes first sensor data **1801**, second sensor data **1802**, and third sensor data **1803** (see FIG. **18**), the server **1502** may compare the first, second, and third sensor data with the signature data of the signature files, and determine a confidence value for each of the signature files based on the comparison of the first, second, and third sensor data with the signature data of the signature files.

For instance, comparing first sensor data with the signature data of the signature files may include determining, for each of the signature files, a first total number of overlapping values between the first sensor data and the signature data of the signature file, determining, for each of the signature files, a first total number of continuously overlapping values between the first sensor data and the signature data of the signature file, determining, for each of the signature files, a first total number of values of the signature data of the signature file that are within a predetermined threshold from the first sensor data, and determining, for each of the signature files, a first total number of continuous values of the signature data of the signature file that are within the predetermined threshold from the first sensor data. Similarly,

US 11,388,181 B2

23

second sensor data and third sensor data may also be compared with the signature data of the signature files. FIG. 23 illustrates a comparison between sensor data 2302 and signature data 2301 of a signature file. Although three sensor data are described above, it should be understood that sensor data from only a single sensor may be compared to signature data to identify a type of a disturbance event on a physical transmission line. In FIG. 23, a total number of overlapping values between the sensor data 2302 and the signature data 2301 of the signature file is 6 (e.g., in FIG. 23, points 1-4, 7, and 11 are the points that overlap), a total number of continuously overlapping values between the sensor data 2302 and the signature data 2301 of the signature file is 4 (e.g., points 1-4 in FIG. 23), a total number of values of the signature data 2301 of the signature file that are within a predetermined threshold from the sensor data 2302 is 9 (e.g., points 1-8 and 11 in FIG. 23), and a total number of continuous values of the signature data 2301 of the signature file that are within the predetermined threshold from the sensor data 2302 is 3 (e.g., points 5, 6, and 8 in FIG. 23). FIG. 24, for example, illustrates a table 2402 (this information along with table 2401 may be stored in the signature database 1534) that includes a total number of overlapping values between the sensor data and the signature data, a total number of continuously overlapping values between the first sensor data and the signature data of the signature file, a total number of values of the signature data of the signature file that are within a predetermined threshold from the sensor data, and a total number of continuous values of the signature data of the signature file that are within the predetermined threshold from the sensor data based on a comparison of the sensor data with signature data of the signature file. Although comparisons between sensor data and signature data are discussed above, it should be understood that similar comparisons can be made between first sensor data from a first sensor and second sensor data from a second sensor to determine a total number of overlapping values between the first sensor data and the second sensor data, a total number of continuously overlapping values between the first sensor data and the second sensor data, a total number of values of the second sensor data that are within a predetermined threshold from the first sensor data, and a total number of continuous values of the second sensor data that are within the predetermined threshold from the first sensor data based on a comparison of the first sensor data with second sensor data. Based on such a comparison between the first sensor data and the second sensor data, the server 1502 may determine whether the first sensor data and the second sensor data correspond to a single disturbance event or multiple different disturbance events.

The server 1502 may determine a first confidence value for each signature file based on a first total number of overlapping values between the first sensor data and the signature data, a first total number of continuously overlapping values between the first sensor data and the signature data of the signature file, a first total number of values of the signature data of the signature file that are within a predetermined threshold from the first sensor data, and a first total number of continuous values of the signature data of the signature file that are within the predetermined threshold from the first sensor data. Similarly, server 1502 may determine a second confidence value and a third confidence value for each signature file based on a comparison of the second sensor data and the third sensor data with the signature data of each signature file. FIG. 24 illustrates information regarding the signature files (e.g., signature 1, signature 2, signature 3, and signature 4) in table 2401 and

24

comparisons of different sensor data with the signature files in table 2402. The data in tables 2401 and 2402 may be stored in the signature database 1534. As an example, table 2402 in FIG. 24 illustrates a confidence value for each signature file based on a comparison of sensor data with signature data of the signature file. These confidence values may be compared to a predetermined threshold to identify a type of disturbance event on the physical transmission line. For example, FIG. 24 illustrates that a comparison of sensor data with signature data of the signature file 2 results in a determination of a confidence value of 73%. If this confidence value is greater than a predetermined threshold, a type of disturbance event associated with the signature file 2 is identified. For example, signature database 1534 may include information indicating that signature file 2 is associated with a hammer tap. Accordingly, when the confidence value for signature file 2 exceeds a predetermined confidence threshold based on a comparison of sensor data with the signature data of the signature file 2, the hammer tap is identified as a type of disturbance event on the physical transmission line. The server 1502 (e.g., the disturbance identifying subsystem 1512) may identify one or more signature files whose confidence value exceeds a predetermined confidence threshold, and identify a type of the disturbance event on the physical transmission line based on the identified one or more signature files. The identified type of disturbance event may be presented to a user via a user interface (see presentation subsystem 1516 and client device 1504 in FIG. 15). Alternatively, the server 1502 (e.g., the disturbance identifying subsystem 1512) may identify the disturbance event as an unknown event on the physical transmission line when the confidence value for each of the signature files does not exceed a predetermined confidence threshold. A notification that the disturbance event is an unknown event may also be presented to a user via a user interface (see presentation subsystem 1516 and client device 1504 in FIG. 15).

Once the type of disturbance event (e.g., a hammer tap) is presented to the user, the server 1502 may request a user to confirm the accuracy of the identified type of disturbance event (see 2101 and 2102 in FIG. 21). For example, a user may be requested to confirm that the disturbance event is a hammer tap via a user interface (see 2101 and 2102 in FIG. 21). When the user confirms the accuracy of the type of disturbance event presented to the user, the server 1502 may retrieve, from the signature database 1534, one or more signature files. These retrieved one or more signature files may correspond to signature files that were identified to have a confidence value exceeding a predetermined confidence threshold and that were used to identify the type of disturbance event on the physical transmission line. For example, if signature file 2 from FIG. 24 was identified to have a confidence value that exceeds a predetermined confidence threshold, and the hammer tap was identified as the type of disturbance event on the physical transmission line based on signature file 2, then signature file 2 is retrieved from the signature database 1534 when the user confirms the accuracy of the type of disturbance event (e.g., hammer tap) presented to the user. Once the signature files are retrieved from the signature database 1534 via communication subsystem 1514, the server 1502 (e.g., the updating subsystem 1518) may compare the sensor data with the signature data of the retrieved one or more signature files to determine differences between the sensor data and the signature data of the retrieved one or more signature files and may update the signature data of the retrieved one or more signature files based on the determined differences. The updated signature

US 11,388,181 B2

25

files may be stored in the signature database **1534**. It should be understood that multiple sensor data may be compared with the signature data of the retrieved signature files to determine differences between multiple sensor data and the signature data of the retrieved signatures files, and the signature data of the signature files may be updated based on such determined differences. Such update of the signature files may help refine accuracy of future detection of disturbance events.

In some embodiments, a neural network or other machine learning model may be trained and utilized to predict a location of a disturbance event on the physical transmission line and a type of the disturbance event on the physical transmission line. As an example, neural networks may be based on a large collection of neural units (or artificial neurons). Neural networks may loosely mimic the manner in which a biological brain works (e.g., via large clusters of biological neurons connected by axons). Each neural unit of a neural network may be connected with many other neural units of the neural network. Such connections can be enforcing or inhibitory in their effect on the activation state of connected neural units. In some embodiments, each individual neural unit may have a summation function that combines the values of all its inputs together. In some embodiments, each connection (or the neural unit itself) may have a threshold function such that the signal must surpass the threshold before it is allowed to propagate to other neural units. These neural network systems may be self-learning and trained, rather than explicitly programmed, and can perform significantly better in certain areas of problem solving, as compared to traditional computer programs. In some embodiments, neural networks may include multiple layers (e.g., where a signal path traverses from front layers to back layers). In some embodiments, back propagation techniques may be utilized by the neural networks, where forward stimulation is used to reset weights on the “front” neural units. In some embodiments, stimulation and inhibition for neural networks may be more free-flowing, with connections interacting in a more chaotic and complex fashion.

Alternatively, the disturbance event may be identified as an unknown event on the physical transmission line when the confidence value for each of the signature files in the signature database **1534** does not exceed a predetermined confidence threshold. When the disturbance event is identified as an unknown event, the disturbance event may be presented to a user via a user interface as an unknown event (see presentation subsystem **1516** and client device **1504**). Further, the user may be prompted to provide additional information about the disturbance event via the user interface so that the server **1502** can classify future disturbance events. For example, if the disturbance event is identified as an unknown event, then the user may be requested to identify the disturbance event and provide additional information regarding the disturbance event. In response to the user providing information regarding the disturbance event, the server **1502** (e.g., updating subsystem **1518**) may generate one or more new signature files including new signature data. The new signature files may be generated based on one or more sensor data (e.g., for which an unknown event was identified) and the information provided by the user of the disturbance event. Such generation of the new signature files may help identify future detection of disturbance events.

The system **1500** may also distinguish voice patterns and identify human presence in specific areas that surround the physical transmission line based on the above description. In

26

other words, system **1500** may distinguish between ambient environmental conditions, object interaction (e.g., a hammer tap) and minute optical, electrical, and wave distortions created by human voice.

When a type of a disturbance event on the physical transmission line is identified by the server **1502**, the server **1502** (e.g., communication subsystem **1514**) may communicate a signal to the physical transmission line based on the type of the identified type of disturbance event. For example, when a disturbance event is identified as a hammer tap, the server **1502** may communicate a signal to the physical transmission line to disable (or cause shut down of) a portion of the physical transmission line that includes the disturbance event and re-route the information transmitted via the physical transmission line such that the portion of the physical transmission line that includes the disturbance event does not transmit the information. It should be understood that only a specific portion of the physical transmission line (e.g., the portion corresponding to the identified location of the disturbance event) may be disabled, while other portions of the physical transmission line may be allowed to function normally (e.g., other portions of the physical transmission line where no disturbance event has been identified). Further, when a disturbance event is identified as a human voice, the sever **1502** may not communicate a signal to the physical transmission line to disable a portion of the physical transmission line that detected the human voice and to re-route information transmitted via the physical transmission line.

FIG. **25** illustrates a flowchart **2500** describing a method for identifying a location of a disturbance event on a physical transmission line, in accordance with one or more embodiments. The processing operations of the method presented below are intended to be illustrative and non-limiting. In some embodiments, for example, the method may be accomplished with one or more additional operations not described, and/or without one or more of the operations discussed. Additionally, the order in which the processing operations of the method are illustrated (and described below) is not intended to be limiting.

In some embodiments, the method may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The processing devices may include one or more devices executing some or all of the operations of the method in response to instructions stored electronically on an electronic storage medium. The processing devices may include one or more devices configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of the method.

In steps **2502** and **2504**, first and second sensor data may be obtained from first and second sensors, respectively, located on a physical transmission line. The first and second sensors may be optical sensors, electrical sensors, acoustical sensors, and/or fiber bragg grating (FBG) sensors and may be placed at different locations of the physical transmission line. The first and second sensor data received from the first and second sensors may include first and second measured values, respectively, of one or more disturbance events over a length of time. In some embodiments, the sensors may be located at predetermined positions on the physical transmission line and the information regarding the location of the sensors on the physical transmission line may be retrieved from a sensor database. In steps **2502** and **2504**, when the

US 11,388,181 B2

27

first and second sensors measure a disturbance event (e.g., based on a detected disturbance event), first and second sensor data that includes first and second measured values, respectively, of the disturbance event over a length of time may be obtained. The first and second measured values may be measured in gain or loss in optical power, acoustical power, and/or electrical resistance. The first and second sensors may detect a single disturbance event or may detect multiple different disturbance events. Accordingly, the first sensor data and the second sensor data may correspond to a single disturbance event or multiple different disturbance events.

In steps 2506, a first initial detection time of the first measured values and a second initial detection time of the second measured values may be determined and in step 2508, a time difference between the first initial detection time and the second initial detection time may be determined.

Further, in step 2510, a first distance of the disturbance event from the first sensor may be approximated based on the time difference and a known constant (e.g., speed of sound and/or speed of light) and a second distance of the disturbance event from the second sensor may be approximated based on the time difference and the known constant. In step 2512, location of the disturbance event on the physical transmission line may be identified based on the approximated first and second distances of the disturbance event from the first sensor and the second sensor, respectively. In addition, the location of the disturbance event on the physical transmission line may be identified further based on locations of these sensors on the physical transmission line. For example, the information regarding the location of the sensors may be retrieved from the sensor database and this information may be utilized to identify the location of the disturbance event on the physical transmission line. Additionally, the information regarding the distance between the sensors may be retrieved from the sensor database 1536 and this information may be utilized to identify the location of the disturbance event on the physical transmission line.

FIG. 26 illustrates a flowchart 2600 describing another method for identifying a location of a disturbance event on a physical transmission line, in accordance with one or more embodiments. In step 2602, sensing data may be obtained from a sensing device located on a physical transmission line. The sensing data may include information regarding a property of a light beam emitted by the sensing device and reflected back to the sensing device by one of the sensors and information regarding timestamp values of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors. In step 2604, based on the sensing data, a roundtrip time of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors may be determined. Further, in step 2604, based on the sensing data, a change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors may be determined. In step 2606, based on the sensing data, a location of the disturbance event on the physical transmission line may be identified. In other words, a location of the disturbance event on the physical transmission line may be identified based on (i) the roundtrip time of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors and (ii) the change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors. Additionally, information regarding

28

the location of the sensing device may be retrieved from a sensor database and this information may be utilized to identify the location of the disturbance event on the physical transmission line. Also, more than one sensing device may be placed at different locations of the physical transmission line to gather sensing data. Known distances between the sensors and the sensing device(s), a known constant (e.g., speed of light and/or sound), and time resolution capabilities of the sensing device(s) can be taken into account to identify the location of the disturbance event on the physical transmission line.

FIG. 27 illustrates a flowchart 2700 describing another method for identifying a location of a disturbance event on a physical transmission line, in accordance with one or more embodiments. In step 2702, sensing data may be obtained from a sensing device located on a physical transmission line. The sensing data may include information regarding a property of a light beam emitted by the sensing device and reflected back to the sensing device by one of the sensors and information regarding timestamp values of another light beam emitted by the sensing device and reflected back to the sensing device by another one of the sensors. In step 2704, based on the sensing data, a change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors may be determined. Further, in step 2704, based on the sensing data, a roundtrip time of the other light beam emitted by the sensing device and reflected back to the sensing device by the other one of the sensors may be determined. In step 2706, based on the sensing data, a location of the disturbance event on the physical transmission line may be identified. In other words, a location of the disturbance event on the physical transmission line may be identified based on (i) the change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors and (ii) the roundtrip time of the other light beam emitted by the sensing device and reflected back to the sensing device by the other one of the sensors. Additionally, information regarding the location of the sensing device may be retrieved from a sensor database and this information may be utilized to identify the location of the disturbance event on the physical transmission line. Also, more than one sensing device may be placed at different locations of the physical transmission line to gather sensing data. Known distances between the sensors and the sensing device(s), a known constant (e.g., speed of light and/or sound), and time resolution capabilities of the sensing device(s) can be taken into account to identify the location of the disturbance event on the physical transmission line.

FIG. 28 illustrates a flowchart 2800 describing a method for identifying a type of a disturbance event on a physical transmission line, in accordance with one or more embodiments. In step 2802, signature files corresponding to previous disturbance events may be obtained. Each of the signature files may include signature data including previously measured values of the previous disturbance events over a length of time. The signatures files may be stored in a signature database and may be retrieved from the signature database. In step 2804, the first and second sensor data (e.g., obtained from first sensor and second sensor located on the physical transmission line) may be compared with the signature data of the signature files. The first and second sensor data may be compared with the signature data of the signature files when at least a portion of the first and second measured values (of the first sensor data and the second sensor data) exceeds a predetermined threshold. Comparing the first and second sensor data with the signature data of the

US 11,388,181 B2

29

signature files may include determining, for each of the signature files, a first total number of overlapping values between the first sensor data and the signature data of the signature file, determining, for each of the signature files, a second total number of overlapping values between the second sensor data and the signature data of the signature file, determining, for each of the signature files, a first total number of continuously overlapping values between the first sensor data and the signature data of the signature file, determining, for each of the signature files, a second total number of continuously overlapping values between the second sensor data and the signature data of the signature file, determining, for each of the signature files, a first total number of values of the signature data of the signature file that are within a predetermined threshold from the first sensor data, determining, for each of the signature files, a second total number of values of the signature data of the signature file that are within a predetermined threshold from the second sensor data, determining, for each of the signature files, a first total number of continuous values of the signature data of the signature file that are within the predetermined threshold from the first sensor data, and determining, for each of the signature files, a second total number of continuous values of the signature data of the signature file that are within the predetermined threshold from the second sensor data.

In step **2806**, a first confidence value and a second confidence value for each of the signature files may be determined based on the comparison of the first and second sensor data with the signature data of the signature files. In step **2808**, a determination is made as to whether the first confidence value or the second confidence value for a signature file exceeds a predetermined confidence threshold. If the answer is YES, in step **2810**, one or more signature files whose confidence value exceeds a predetermined confidence threshold is identified. Further, in step **2812**, a type of disturbance event on the physical transmission line is identified based on the identified one or more signature files. For example, a hammer tap may be identified as a type of disturbance event on the physical transmission line.

In step **2814**, the identified type of disturbance event may be presented, via a user interface, to a user and the user may be requested, via the user interface, to confirm the accuracy of the identified type of disturbance event. For example, a user may be requested to confirm that the type of disturbance event is a hammer tap via a user interface. In step **2816**, when the user confirms the accuracy of the type of disturbance event presented to the user, one or more signature files may be retrieved from a signature database. These retrieved one or more signature files correspond to signature files that were identified to have a confidence value exceeding a predetermined confidence threshold and that were used to identify the type of disturbance event on the physical transmission line.

In step **2818**, the first and second sensor data (e.g., obtained from first sensor and second sensor located on the physical transmission line) may be compared with the signature data of the retrieved one or more signature files to determine differences between the first sensor data and the signature data of the retrieved one or more signature files and between the second sensor data and the signature data of the retrieved one or more signature files. In step **2820**, the signature data of the retrieved one or more signature files may be updated based on the determined differences. The updated one or more signature files may be stored in the

30

signature database. Such update of the signature files may help refine accuracy of future detection of disturbance events.

However, in step **2808**, if the first confidence value or the second confidence value for a signature file does not exceed a predetermined confidence threshold (e.g., NO in step **2808**), then we proceed to step **2822**. In step **2822**, the disturbance event on the physical transmission line is identified as an unknown event when the first confidence value and the second confidence value for each of the signature files does not exceed the predetermined confidence threshold. Further, in step **2824**, the disturbance event may be presented to a user via a user interface as an unknown event and the user, via the user interface, may be requested to provide information about the unknown event. For example, the user may be requested to provide a brief description of the disturbance event. In step **2826**, one or more new signature files may be generated based on the first sensor data, the second sensor data, and the information provided by the user about the unknown event. Although flowchart **2800** describes a method for identifying a type of a disturbance event on a physical transmission line based on first and second sensor data, it should be understood that only one of the first sensor data or the second sensor data may be used to identify a type of a disturbance event on a physical transmission line.

In some embodiments, one or more components described herein may be configured in accordance with one or more variables, functions, or other code represented by the following pseudocode:

```
// Variables
_DeviceOutputFrequency=5000 // number of data points per second
_DistanceTimingValue=0
_CompleteTimeCycle=0
_StartingTimeStampValue=0
_CenterDistance=0
_SpeedOfWave=0
_MatchVariance=0.15
_WavelengthVariance=0.15
_DBVariance=1
_BaselineWavelength=1450
_BaselineDB=-14
_CompareResultThresholdCEPoM=0.10
_CompareResultThresholdTEPoM=0.05
_CompareResultThresholdCPoVM=0.10
_CompareResultThresholdTPoVM=0.40
Structure DisturbanceResult
    DisturbanceStart=0
    DisturbanceEnd=0
    DisturbanceLength=0
End Structure
Structure CompareResults
    ContExactPointsofMatch=0
    TotalExactPointsofMatch=0
    TotalContinuousPointsofVariableMatch=0
    TotalPointsofVariableMatch=0
End Structure
Start Function Main
    // Sensor Data Time of Flight for Two Sensors
    If CalibrateTimeOfFlight( )=True Then
        // Calibrate Completed, and future disturbances can be
        determined by the following
        EstimatedDisturbanceLocation=ReturnDistance
        (SensorDisturbance1.DisturbanceStart,
        SensorDisturbance2.DisturbanceStart)
    End If
```

US 11,388,181 B2

31

```

// Device Timing Methods
If CalibrateTimingValue( )=True Then
// Calibration Completed, and future disturbances can be
determined by the following
EstimatedDisturbanceLocationByTime
(SensorDisturbance1.DisturbanceTimeStamp)
End If
End Function
Start Function GridMatch(LeftGridArray[], RightGridArray
[], PointVarianceThreshold) Returns
CompareResults Object
For r=0 to RightGridArray.Count
If LeftGridArray[r]=RightGridArray[r] then
TotalExactPointsofMatch=TotalExactPointsofMatch+1
End If
CheckValue=(LeftGridArray[r]-RightGridArray[r])
If CheckValue<=PointVarianceThreshold then
TotalPointsofVariableMatch=TotalPointsofVariable
Match+1
End If
Loop
Temp_ContExactPointsofMatch=0
For r=0 to RightGridArray.Count
For l=0 to LeftGridArray.Count
LeftGridArray[l]=RightGridArray[r] then
Temp_ContExactPointsofMatch=Temp_ContExact
PointsofMatch+1
Else
If Temp_ContExactPointsofMatch>ContExact
PointsofMatch
ContExactPointsofMatch=Temp_ContExact
PointsofMatch
End If
Temp_ContExactPointsofMatch=0
End If
Loop
If Temp_ContExactPointsofMatch>ContExact Point-
sofMatch
ContExactPointsofMatch=
Temp_ContExactPointsofMatch
End If
Loop
Temp_ TotalContinousPointsofVariableMatch=0
For r=0 to RightGridArray.Count
For l=0 to LeftGridArray.Count
CheckValue=(LeftGridArray[l]-RightGridArray[r])
If CheckValue<=PointVarianceThreshold then
Temp_ TotalContinousPointsofVariableMatch=
Temp_ TotalContinousPointsofVariableMatch+1
Else
If Temp_ TotalContinousPointsofVariableMatch>
TotalContinousPointsofVariableMatch Then
TotalContinousPointsofVariableMatch=
Temp_ TotalContinousPointsofVariableMatch
End If
Temp_ TotalContinousPointsofVariableMatch=0
End If
Loop
If Temp_ TotalContinousPointsofVariableMatch>
TotalContinousPointsofVariableMatch Then
TotalContinousPointsofVariableMatch=
Temp_ TotalContinousPointsofVariableMatch
End If
Loop
// Set values of return object
CompareResults.ContExactPointsofMatch=ContExact
PointsofMatch

```

32

```

CompareResults.TotalExactPointsofMatch=TotalExact
PointsofMatch
CompareResults.TotalContinousPointsofVariableMatch=
TotalContinousPointsofVariableMatch
5 CompareResults.TotalPointsofVariableMatch=Total
PointsofVariableMatch
Return CompareResults
End Function
Start Function DetermineDisturbance (AnalysisBuffer[])
Returns DisturbanceResult
// This function determines disturbance based on multiple
factors
// This example utilizes only wavelength and power vari-
ance, however, multiple reading types
DisturbanceStart=0
DisturbanceStarted=False
DisturbanceEnd=0
For b=0 to AnalysisBuffer.Count
20 If ((AnalysisBuffer[b].Wavelength-_BaselineWave-
length)>
_WavelengthVariance)
OR ((AnalysisBuffer[b].DB-_BaselineDB)>_DBVariance)
Then
25 If DisturbanceStarted=False then
DisturbanceStart=b
DisturbanceStarted=True
End If
Else
30 If DisturbanceStarted=True Then
DisturbanceEnd=b
Exit Loop
End If
End If
35 Loop
DisturbanceResult.DisturbanceStart=DisturbanceStart
DisturbanceResult.DisturbanceEnd=DisturbanceEnd
DisturbanceResult.DisturbanceLength=DisturbanceEnd-
DisturbanceStart
40 Return DisturbanceResult
End Function
Start Function ReturnDistance(Time1, TimeValue2) Returns
Number
DistancePer=_SpeedOfWave/ _DeviceOutputFrequency
45 DistanceDifference=TimeValue2-TimeValue1
SideDistance=DistanceDifference*DistancePer
Return (_CenterDistance+SideDistance)
End Function
Start Function CalculateSpeedofWave(TimeDifference,
50 TotalLength,
KnownDisturbanceDistance) as Number
CenterDistance=TotalLength/2
_CenterDistance=CenterDistance
CenterDifference=DisturbanceDistance-CenterDistance
55 For t=40 to 13000
If ((t/_DeviceOutputFrequency)*TimeDifference)=Center
Difference Then
Return t
Exit Loop
60 End If
Next
End Function
// Calibration of Sensor Data
Start Function CalibrateTimeOffFlight ( ) Returns Boolean
65 *Read Device Information
*Populate Sensor1ReadBuffer[] with Device Information
(Wavelength, Amplitude, etc)

```

US 11,388,181 B2

33

```

*Populate Sensor2ReadBuffer[] with Device Information
(Wavelength, Amplitude, etc)
EstimatedDistance=Prompt User for Estimated Distance
of Disturbance
TotalKnownDistance=Prompt User for Known Distance of Section
// Method One: Sensor Data Time of Flight for Two Sensors
Sensor1DisturbanceResult=DetermineDisturbance
(Sensor1ReadBuffer[])
Sensor2DisturbanceResult=DetermineDisturbance
(Sensor2ReadBuffer[])
// Verify that disturbance is the same
SensorDisturbance1=CopyFromArray
(Sensor1ReadBuffer[]),
Sensor1DisturbanceResult.DisturbanceStart,
Sensor1DisturbanceResult.DisturbanceLength)
SensorDisturbance2=CopyFromArray
(Sensor2ReadBuffer[]),
Sensor2DisturbanceResult.DisturbanceStart,
Sensor2DisturbanceResult.DisturbanceLength)
SensorCompareResults=GridMatch(SensorDisturbance1
[], SensorDisturbance2[],
_MatchVariance)
If ((SensorCompareResults.ContExactPointsofMatch/
SensorDisturbance1.Count)>=
_CompareResultThresholdCEPoM) OR
(SensorCompareResults.TotalExactPointsofMatch/
SensorDisturbance1.Count)>=
_CompareResultThresholdTEPoM) OR
(SensorCompareResults.TotalContinousPointsofVari-
ableMatch/SensorDisturbance1.Count)>=
_CompareResultThresholdCPoVM) OR
(SensorCompareResults.TotalPointsofVariableMatch/
SensorDisturbance1.Count)>=
_CompareResultThresholdTPoVM) Then
// Determine the speed of wave through the material
_SpeedOfWave=CalculateSpeedofWave(
(SensorDisturbance2.DisturbanceStart-
SensorDisturbance1.DisturbanceStart), TotalKnownDis-
tance, EstimatedDistance)
Return True
Else
Return False
End If
End Function
Start Function CalculateTimingSpeed(DisturbanceTime1,
DisturbanceTime2,
TotalKnownDistance)
DisturbanceTimeDiff=DisturbanceTime2-Disturbance-
Time1
DisturbanceDistanceDiff=DisturbanceDistance2-Distur-
banceDistance1
DistancePerTime=DisturbanceDistanceDiff/Disturbance-
TimeDiff
_DistanceTimingValue=DistancePerTime
End Function
// Starlight
Start Function CalibrateTimingValue( ) Returns Boolean
// Method Two & Three: Timestamp Distance Calculation
TotalKnownDistance=Prompt User for Known Distance
of Section
*Prompt User to Create Disturbance at the Beginning of
the Section
KnownDistance1=Prompt User for Known Distance of
Section Disturbance
*Read Device Information

```

34

```

*Populate Sensor1ReadBuffer[] with Device Information
(Wavelength, Amplitutde, etc)
and Timestamp Information
SensorBeginDisturbanceResult=DetermineDisturbance
(Sensor1ReadBuffer[])
*Set Known KnowDistance1TimeStamp from
SensorBeginDisturbanceResult.DisturbanceStart
*Prompt User to Create Disturbance at the End of the
Section
KnownDistance=Prompt User for Known Distance of
Section Disturbance
*Read Device Information
*Populate Sensor1ReadBuffer[] with Device Information
(Wavelength, Amplitude, etc)
and Timestamp Information
SensorEndDisturbanceResult=DetermineDisturbance
(Sensor1ReadBuffer[])
CalculateTimingSpeed(KnowDistance1TimeStamp,
KnowDistance2TimeStamp,
TotalKnownDistance)
_CompleteTimeCycle=TotalKnownDistance*_Distance
TimingValue
_StartingTimeStampValue=KnowDistance1TimeStamp-
(KnownDistance1*_
_DistanceTimingValue
Return True
End Function
Start Function EstimatedDisturbanceLocationByTime(Dis-
turbanceTimeStamp) Returns Number
TickDisturbanceDiff=DisturbanceTimeStamp-_Starting-
TimeStampValue
CompletedCycles=Math.RoundDown(TickDisturbanc-
eDiff/ _CompleteTimeCycle)
Return (TickDisturbanceDiff-
(_CompleteTimeCycle*CompletedCycles))*
_DistanceTimingValue
End Function
Cable Assembly
FIGS. 29A and 29B show a cable assembly that illumi-
nates using, for example, light emitting diodes (LEDs) (see
also visual indication 1528 in FIG. 15) to provide an
inspection personnel with real-time information regarding
the state of the cable assembly. The inner and outer jackets
(or sheaths) of the cable assembly may be utilized for new
or existing optical fiber cable designs as well as armored
optical fiber assemblies that utilize metal or non-metallic
tubing (spiral, inter-locking, or non-interlocking) with
aramid and/or other strengthening materials.
FIGS. 29A and 29B show a cable assembly 2900 that
includes an outer jacket 2901 (or outer sheath), a printed
circuit board (PCB) 2902 (including a plurality of LEDs
2905), an optional inner jacket 2903 (or inner sheath), and
a core 2904 (e.g., a fiber optic cable or optical fiber assembly
which comprises at least one optical fiber enclosed in a
tubular member). The PCB 2902 may include circuitry to
communicate with the server 1502 to receive instructions to
turn on/off one or more LEDs 2905 and may include control
circuitry to turn on/off the LEDs 2905 based on such
instructions. The outer jacket 2901 may have an inner
diameter than is slightly larger than an outer diameter of the
core 2904. The outer jacket 2901 may be composed of
Polyvinly Chloride (PVC), Low smoke Zero Halogen
(LSZH), Thermoplastic polyurethane (TPU), Ethylene Tet-
rafluoroethylene (ETFE), Optical Fiber Nonconductive Ple-
num (OFNP), or other types of plastic or rubber compounds.
The outer jacket 2901 may or may not be flame retardant and
the outer jacket 2901 may either be translucent in color or
may be a colored jacket with transitions of translucent

```


US 11,388,181 B2

35

material at the location of the LEDs **2905** to allow emitted light to pass through. The PCB **2902** may include LEDs **2905** and additional circuitry for control. The thickness of the PCB **2902** may range from 0.50-2.50 mm, the width of the PCB **2902** may vary, but is typically between 6 and 12 mm, and the length of the PCB **2902** may be consistent with the length of the cable assembly. An example of the circuitry for the PCB **2902** is illustrated in FIG. **30**. FIG. **30** shows an SMD5050 design for analog control of Red Green Blue (RGB) LEDs. However alternate LED control circuits such as an LPD8806 can be utilized to provide individually accessible RGB LED control. The PCB **2902** may include connections at the beginning and/or end of the assembly for connecting to an external power source and additional control circuits for signal processing. The relative thickness of the PCB **2902** allows for contouring around the inner jacket **2903** and/or core **2904**.

The inner jacket **2903** may have an inner diameter than is slightly larger than the outer diameter of the core **2904**. The inner jacket **2903** may be composed of PVC, LSZH, TPU, ETFE, OFNP, or other types of plastic or rubber compounds that can be utilized to color the inner jacket **3** when utilizing a translucent outer jacket **2901**. The core **2904** (e.g., a fiber optic cable or optical fiber assembly which may comprise at least one optical fiber enclosed in a tubular member) may be composed of PVC, High-density Polyethylene (HDPE) or Silicone. Optionally, the core **2904** may be an armored assembly composed of a metallic or non-metallic spiral, inter-locking or non-interlocking tube. Core **2904** may include optional strengthening materials, such as aramid or glass fibers, plastic or metal wiring or similar strength and rigidity increasing materials.

The PCB **2902** can be integrated into the cable assembly **2900** using multiple methods based on the outer and inner jacket materials and the environmental and performance requirements of the cable assembly **2900**.

FIG. **29A** shows a cable assembly **2900** without channels (or channel openings). In FIG. **29**, the PCB **2902** (which includes a plurality of LEDs **2905**) is placed between the outer jacket **2901** and core **2904**. For example, the PCB **2902** may be placed on top of the core **2904** using an adhesive to ensure proper alignment of the PCB **2902** with the overall cable assembly **2900**. Alternatively, as illustrated in FIG. **29B**, the PCB **2902** may be placed between the inner jacket **2903** and outer jacket **2901**. For example, the PCB **2902** may be placed on top of the inner jacket **2903** using an adhesive to ensure proper alignment of the PCB **2902** with the overall cable assembly **2900**. FIG. **29B** shows a YZ plane view of the cable **2900** assembly illustrated in FIG. **29A**.

The spacing between the outer jacket **2901** and the core **2904** (or between the outer jacket **2901** and the inner jacket **2903**) may be approximately 0.50-2.50 mm depending upon the thicknesses of the PCB **2902** and the material of the outer jacket **2901**. For example, a rigid PVC material for the outer jacket **2901** may require spacing equivalent to the full PCB thickness, whereas a rubber or rubber type compound would allow inherent contouring/molding around the PCB **2902**. Utilizing no channels (or channel openings) for the outer jacket **2901** may ensure that the inherent durability of the outer jacket **2901** is unaffected.

The outer jacket **2901** may be translucent, thereby, allowing light from the LEDs **2905** to be seen. When a location of a disturbance event (e.g., a location of an intrusion attempt) on the cable assembly **2900** is identified, the system **1500** may be configured to supply a signal via network **1550** to the cable assembly **2900** so that the LEDs **2905** that are located at or near the location of the disturbance event can

36

be illuminated. Additionally, the system **1500** may be configured to supply a signal via network **1550** to the cable assembly **2900** so that the LEDs **2905** can be illuminated to indicate a type of disturbance event. For example, different LEDs can be illuminated (different patterns) to identify different types of disturbance events. Additionally, or alternatively, different colors can be illuminated to identify different types of disturbance events. Further, the LEDs can also be illuminated to show specific status information such as warning conditions and maintenance activity. Although only one strip of LEDs **2905** is illustrated in FIGS. **29A** and **29B**, it should be understood that a plurality of PCBs **2902** can be included between the core **2904** and outer jacket **2901** (or between the inner jacket **2903** and the outer jacket **2901**) such that the LEDs **2905** on the PCB **2902** can be viewed from different angles and directions.

FIG. **31A** shows a cable assembly **3100** that includes a core **3104**, PCB **3102** (including a plurality of LEDs **3105**), and an outer jacket **3101**. The outer jacket **3101** includes a channel (or channel opening) **3106** that allows the PCB **3102** to be positioned within the channel opening **3106**. The channel may be molded, cut, or otherwise imparted on the inside of the outer jacket **3101**. The PCB **3102** may include circuitry to communicate with the server **1502** to receive instructions to turn on/off one or more LEDs **3105** and may include control circuitry to turn on/off the LEDs **3105** based on such instructions. FIG. **31B** shows another view of the cable assembly **3100** (view of the YZ plane). In FIG. **31B**, the outer jacket **3101** is illustrated to include a plurality of channel openings **3106A-D** (within which a plurality of PCBs **3102** may be positioned). Further, FIG. **31B** illustrates core **3104**. Although the cable assembly **3100** does not illustrate an inner jacket, it should be understood that an inner jacket may be included in the cable assembly **3100** such that the inner assembly surrounds the core **3104** and the PCB **3102** may be positioned between the inner jacket and the outer jacket **3101**.

FIG. **31B** also illustrates an outer layer **3101A** of the outer jacket **3101**, a first inner layer **3101B** of the outer jacket **3101**, and a second inner layer **3101C** of the outer jacket **3101**. Here, the first inner layer **3101B** corresponds to a top portion of the channel **3106A**. The first inner layer **3101B** is formed in a section of the outer jacket **3101** that includes the channel opening **3106A** and the second inner layer **3101C** is formed in a section of the outer jacket **3101** that does not include the channel opening **3106A**. The first thickness between the outer layer **3101A** and the first inner layer **3101B** is smaller than the second thickness between the outer layer **3101A** and the second inner layer **3101C**. The shape of the channel opening **3106** can be rectangular, square, circular, trapezoidal, or any other shape that can allow the PCB **3102** to be positioned within the channel opening **3106**.

FIG. **31C** illustrates another view of the channel assembly **3100** (view of the YX plane). In FIG. **31C**, a PCB **3102** is illustrated to be positioned within the channel opening **3106A** and between the outer jacket **3101** and the core **3104**. Here, a depth of the channel opening is illustrated as being consistent throughout a length of the outer jacket in the X direction. This allows the PCB **3102** to stay in a specific orientation and position within the channel **3106A**, while also allowing for removal of the PCB **3102** for activities such as repair, by allowing the PCB **3102** to slide out of the channel **3106A** when adhesives have not been utilized during the manufacturing process. The depth of the channel opening **3106A** may be measured based on a difference between the second thickness (e.g., the second thickness

US 11,388,181 B2

37

between the outer layer **3101A** and the second inner layer **3101C**) and the first thickness (e.g., the first thickness between the outer layer **3101A** and the first inner layer **3101B**). Alternatively, the depth of the channel opening **3106A** may be measured as the difference between the second thickness and the first thickness plus a spacing between the core **3104** and the second inner layer **3101C**. The spacing between the core **3104** and the second inner layer **3101C** (e.g., the spacing between the core **3104** and the outer jacket **3101**) may be less than 1 mm. The channel opening **3106** may have a depth of approximately 0.50-2.50 mm dependent on the type and size of the PCB **3102** that is embedded within the channel opening **3106**.

FIG. **31D** illustrates another view of the channel assembly **3100** (view of the YX plane) and is an alternate to the configuration described and illustrated with regard to FIG. **31C**. For example, FIG. **31D** illustrates a molded channel opening **3106A** (that may contour around each PCB **3102** component) such that a depth of the channel opening **3106A** varies along a length of the outer jacket **3101**. The depth of the channel opening **3106A** may vary by 1 mm because of the varied depth of the channel opening **3106A**. This varied depth allows strict control of the PCB **3102** and may prevent removal or movement under normal and adverse operating circumstances. Adhesives between the core **3104** and the PCB **3102** may be utilized. However, an adhesive is not required.

FIG. **32A** shows a cable assembly **3200** that includes a core **3204**, PCB **3202** (including a plurality of LEDs **3205**), an outer jacket **3201**, and an inner jacket **3203**. The inner jacket **3203** includes a channel (or channel opening or depression) **3208** that allows the PCB **3202** to be positioned within the channel opening **3208**. The channel may be molded, cut, or otherwise imparted on the outside of the inner jacket **3203**. FIG. **32B** shows another view of the cable assembly **3200** (view of the YZ plane). In FIG. **32B**, the inner jacket **3203** is illustrated to include a plurality of channel openings **3208A-D** (within which a plurality of PCBs **3202** may be positioned). Further, FIG. **32B** also illustrates the outer jacket **3201** and core **3204**.

FIG. **32B** also illustrates an inner layer **3203A** of the inner jacket **3203**, a first outer layer **3203B** of the inner jacket **3203**, and a second outer layer **3203C** of the inner jacket **3203**. Here, the second inner layer **3203C** corresponds to a bottom portion of the channel opening **3208A**. The second outer layer **3203C** is formed in a section of the inner jacket **3203** that includes the channel opening **3208A** and the first outer layer **3203B** is formed in a section of the inner jacket **3203** that does not include the channel opening **3208A**. The first thickness between first outer layer **3203B** and the inner layer **3203A** is larger than the second thickness between the second outer layer **3203C** and the inner layer **3203A**. The shape of the channel opening **3208** can be rectangular, square, circular, trapezoidal, or any other shape that can allow the PCB **3202** to be positioned within the channel opening **3208**.

A depth of the channel opening **3208** may be consistent throughout a length of the outer jacket **3201** in the X direction. The depth of the channel opening **3208** may be measured based on a difference between the first thickness (e.g., the first thickness between first outer layer **3203B** and the inner layer **3203A**) and the second thickness (e.g., the second thickness between the second outer layer **3203C** and the inner layer **3203A**). Alternatively, the depth of the channel opening **3208A** may be measured as the difference between the first thickness and the second thickness plus a spacing between the first outer layer **3203B** and the outer

38

jacket **3201**. The spacing between the first outer layer **3203B** and the outer jacket **3201** (e.g., the spacing between the inner jacket **3203** and the outer jacket **3201**) may be less than 1 mm. The channel opening **3208** may have a depth of approximately 0.50-2.50 mm dependent on the type and size of the PCB **3202** that is embedded within the channel opening **3208**.

The channel opening **3208** may be included within the inner jacket **3203** in situations where the durability, rigidity or performance of the material of the outer jacket **3201** could be negatively affected by the varying diameter/thickness of the channel within the outer jacket **3201**. Such a configuration in FIGS. **32A** and **32B** may ensure that environmental durability, bending radius, and other stress factors do not affect the integrity of the outer jacket **3201**.

The channel opening **3208** within the inner jacket **3203** ensures that the PCB **3202** stays within a fixed position relative to the rest of the cable assembly **3200**. This configuration in FIGS. **32A** and **32B** allows the PCB **3202** to stay in a specific orientation and position, while allowing for removal of the PCB **3202** for activities such as repair, by allowing the PCB **3202** to slide out of the channel **3208** when adhesives have not been used during the manufacturing process.

The LEDs described above may provide alarm response personnel with visual indicators attached to transmission lines (or their enclosures) that provide specific status information such as warning conditions, maintenance activity, intrusion information, and/or location information. The spacing between LEDs may be varied based on several factors. Some of the factors may include length, width, and/or diameter of the cable assembly. For example, a shorter cable assembly may have less spacing between the LEDs compared to a longer cable.

Further, a number of LEDs that are lit may depend on a length of the disturbance event on the physical transmission line. For example, if the disturbance event spans a large portion of the transmission line, then several LEDs (that span the portion of the physical transmission line that has been disturbed) may be lit. Alternatively, only two LEDs may be lit (e.g., an LED at a start location of the disturbance event on the physical transmission line and at an end location of the disturbance event on the physical transmission line). Alternatively, only one LED may be lit that is closest to the identified location of the disturbance event on the physical transmission line. By lighting few number of LEDs, power can be saved. Long distances of continuously lit LEDs require large amounts of power. For that reason, the number of LEDs that are simultaneously lit may be limited to ensure that usage of power by the LEDs is below a predetermined threshold. The server **1502** may determine a number of LEDs to be lit and/or the pattern of the LEDs to be lit based on the length of the disturbance event on the physical transmission line (in other words, a length of the portion of the physical transmission line that has been disturbed), amount of power supply required for each of the LEDs, and/or color of the LEDs to be visually displayed so that the power used by the LEDs does not exceed a predetermined threshold. Alternatively, control circuitry of the PCB may determine a number of LEDs to be lit and/or the pattern of the LEDs to be lit based on the length of the disturbance event on the physical transmission line (in other words, a length of the portion of the physical transmission line that has been disturbed), amount of power supply required for each of the LEDs, and/or color of the LEDs to be visually displayed so that the power used by the LEDs does not exceed a predetermined threshold.

US 11,388,181 B2

39

In addition to visually indicating that there is a disturbance event at a specific location of the physical transmission line, the LEDs may be lit based on one or more patterns. For example, one LED may be made to blink (e.g., an LED closest to the identified location of the disturbance event on the physical transmission line), thereby, providing a network personnel better visibility of the exact location of the disturbance event on the physical transmission line. Alternatively, a series of LEDs may be lit one after another (a “chase” effect) that located between a start location of the disturbance event on the physical transmission line and an end location of the disturbance event on the physical transmission line. Such a chase effect may allow very long sections of the physical transmission line to be illuminated without exceeding a power level beyond a predetermined threshold. Further, different color LEDs may be lit to indicate different information to a network personnel. For example, a red LED may indicate that there is a disturbance event on the physical transmission line, a green LED may indicate that there is no disturbance event on the physical transmission line, and a blue LED may indicate that maintenance is being conducted on the physical transmission line. It should be understood that these are merely some examples, and various combinations of patterns and colors may be used to provide alarm response personnel with specific status information such as warning conditions, maintenance activity, intrusion information, and/or location information.

FIG. 33 shows an architecture and operation of a visual indication system 3300 in conjunction with a PDS manager architecture. One or more components of the visual indication system 3300 illustrated in FIG. 33 may correspond to one or more components of the system 1500 in FIG. 15.

FIG. 33 shows alarm monitoring devices 3307 that detect disturbances to a transmission line 3306. The transmission line 3306 may be affixed with a visual indication collar 3304, which includes a series of LED lights managed and controlled by an electronic controller 3305. As the alarm monitoring devices 3307 detect disturbances on the transmission line 3306, data is sent to the PDS manager architecture (see 3301 and 3302 in FIG. 33) and this data is processed by the PDS manager system and state information (such as “no issue,” “alarm,” “warning,” or “maintenance” conditions) may be produced.

The PDS Manager Web Server may provide real-time data feed in the form of a web service that the visual indicator system controller 3305 may request via Ethernet, WiFi or other wireless radio communication (see 3303 in FIG. 33). Sensor data status information may be processed by the visual indicator system controller 3305 and based on user configuration within the controller, visual indicators (such as LED lights) may display on the transmission line 3306. For example, “no issue” conditions may light the LEDs on the “visual indicator collar” as green, “warning” conditions as yellow, “maintenance” conditions in blue and “alarm” conditions in red. As the PDS Manager continues to update transmission line state information, the visual indication system 3300 may update visual indicators in real-time so that response personnel know current transmission line status.

The visual indication system 3300 can utilize multiple form factors, including a “visual indicator collar” as shown in FIG. 33, a visual indicator “strip” as shown in FIG. 34 which uses a series of connected lights that affix to the transmission line or one or more indicators as a visual indicator “box” affixed to the transmission line. When the system 3400 is utilized with a “visual indicator strip” 3401,

40

location information provided by the PDS Manager is utilized by the visual indicator system controller 3404 to visually indicate the location of the disturbance (e.g., 3403 in FIG. 34 shows a series lights illuminated after a disturbance at location 3402 is detected). This provides response personnel the ability to pinpoint the exact location of a disturbance.

In some embodiments, the various computers and subsystems illustrated in FIG. 15 may include one or more computing devices that are programmed to perform the functions described herein. The computing devices may include one or more electronic storages (e.g., database(s) 1532, which may include signature database 1534, sensor database 1536, etc., or other electric storages), one or more physical processors programmed with one or more computer program instructions, and/or other components. The computing devices may include communication lines or ports to enable the exchange of information with a network (e.g., network 1550) or other computing platforms via wired or wireless techniques (e.g., Ethernet, fiber optics, coaxial cable, WiFi, Bluetooth, near field communication, or other technologies). The computing devices may include a plurality of hardware, software, and/or firmware components operating together. For example, the computing devices may be implemented by a cloud of computing platforms operating together as the computing devices.

The electronic storages may include non-transitory storage media that electronically stores information. The electronic storage media of the electronic storages may include one or both of (i) system storage that is provided integrally (e.g., substantially non-removable) with servers or client devices or (ii) removable storage that is removably connectable to the servers or client devices via, for example, a port (e.g., a USB port, a firewire port, etc.) or a drive (e.g., a disk drive, etc.). The electronic storages may include one or more of optically readable storage media (e.g., optical disks, etc.), magnetically readable storage media (e.g., magnetic tape, magnetic hard drive, floppy drive, etc.), electrical charge-based storage media (e.g., EEPROM, RAM, etc.), solid-state storage media (e.g., flash drive, etc.), and/or other electronically readable storage media. The electronic storages may include one or more virtual storage resources (e.g., cloud storage, a virtual private network, and/or other virtual storage resources). The electronic storage may store software algorithms, information determined by the processors, information obtained from servers, information obtained from client devices, or other information that enables the functionality as described herein.

The processors may be programmed to provide information processing capabilities in the computing devices. As such, the processors may include one or more of a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information. In some embodiments, the processors may include a plurality of processing units. These processing units may be physically located within the same device, or the processors may represent processing functionality of a plurality of devices operating in coordination. The processors may be programmed to execute computer program instructions to perform functions described herein of subsystems 1512-1518 or other subsystems. The processors may be programmed to execute computer program instructions by software; hardware; firmware; some combination of software, hardware, or firmware; and/or other mechanisms for configuring processing capabilities on the processors.

US 11,388,181 B2

41

It should be appreciated that the description of the functionality provided by the different subsystems **1512-1518** described herein is for illustrative purposes, and is not intended to be limiting, as any of subsystems **1512-1518** may provide more or less functionality than is described. For example, one or more of subsystems **1512-1518** may be eliminated, and some or all of its functionality may be provided by other ones of subsystems **1512-1518**. As another example, additional subsystems may be programmed to perform some or all of the functionality attributed herein to one of subsystems **1512-1518**.

Although the present invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the scope of the appended claims. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment may be combined with one or more features of any other embodiment.

The present techniques will be better understood with reference to the following enumerated embodiments:

A1. A method for identifying a location of a disturbance event on a physical transmission line, the method comprising: obtaining, from a first sensor among sensors on a physical transmission line, first sensor data, the first sensor data including first measured values of the disturbance event over a length of time; obtaining, from a second sensor among the sensors on the physical transmission line, second sensor data, the second sensor data including second measured values of the disturbance event over the length of time; determining a first initial detection time of the first measured values and a second initial detection time of the second measured values; determining a time difference between the first initial detection time and the second initial detection time; approximating a first distance of the disturbance event from the first sensor based on the time difference and a known constant and a second distance of the disturbance event from the second sensor based on the time difference and the known constant; and identifying a location of the disturbance event on the physical transmission line based on the approximated first and second distances.

A2. The method of embodiment A1, wherein the location of the disturbance event on the physical transmission line is identified further based on locations of the first and second sensors on the physical transmission line.

A3. The method of any of embodiments A1-2, further comprising: obtaining, from a sensing device located on the physical transmission line, sensing data, the sensing data including information regarding timestamp values of a light beam emitted by the sensing device and reflected back to the sensing device by one of the sensors and information regarding a property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors; determining, based on the sensing data, (i) a roundtrip time of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors and (ii) a change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors; and identifying the location of the disturbance event on the physical transmission line further based on (i) the roundtrip time of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors and (ii) the change

42

in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors.

A4. The method of any of embodiments A1-3, wherein the location of the disturbance event on the physical transmission line is identified further based on a location of the sensing device on the physical transmission line.

A5. The method of any of embodiments A1-4, further comprising: obtaining, from a sensing device located on the physical transmission line, sensing data, the sensing data including information regarding a property of a light beam emitted by the sensing device and reflected back to the sensing device by one of the sensors and information regarding timestamp values of another light beam emitted by the sensing device and reflected back to the sensing device by another one of the sensors; determining, based on the sensing data, (i) a change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors and (ii) a roundtrip time of the other light beam emitted by the sensing device and reflected back to the sensing device by the other one of the sensors; and identifying the location of the disturbance event on the physical transmission line further based on (i) the change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the one of the sensors and (ii) the roundtrip time of the other light beam emitted by the sensing device and reflected back to the sensing device by the other one of the sensors.

A6. The method of any of embodiments A1-5, wherein the known constant is at least one of speed of sound or speed of light.

A7. The method of any of embodiments A1-6, further comprising: presenting, via a user interface, the location of the disturbance event on the physical transmission line.

A8. The method of any of embodiments A1-7, further comprising: determining whether the first measured values and the second measured values correspond to a single disturbance event or multiple disturbance events based on (i) a comparison of time durations of the first and second measured values and (ii) a comparison of peak/valley magnitudes of the first and second measured values.

A9. The method of any of embodiments A1-8, wherein the property of the light beam includes at least one of wavelength or amplitude.

A10. The method of any of embodiments A1-9, wherein the light beam is emitted by the sensing device via the physical transmission line and reflected back to the sensing device via the physical transmission line.

A11. The method of any of embodiments A1-10, wherein the property of the light beam includes at least one of wavelength or amplitude.

A12. The method of any of embodiments A1-11, wherein the light beam is emitted by the sensing device via the physical transmission line and reflected back to the sensing device via the physical transmission line, and wherein the other light beam is emitted by the sensing device via the physical transmission line and reflected back to the sensing device via the physical transmission line.

A13. The method of any of embodiments A1-12, wherein the sensors include optical sensors, electrical sensors, acoustical sensors, or fiber bragg grating sensors.

A14. The method of any of embodiments A1-13, further comprising: obtaining signature files corresponding to previous disturbance events, each of the signature files including signature data including previously measured values of the previous disturbance events over the length of time; comparing the first and second sensor data with the signature

US 11,388,181 B2

43

data of the signature files; determining a first confidence value and a second confidence value for each of the signature files based on the comparison of the first and second sensor data with the signature data of the signature files; identifying one or more signature files whose said first confidence value or said second confidence value exceeds a predetermined confidence threshold; and identifying a type of the disturbance event on the physical transmission line based on the identified one or more signature files.

A15. The method of any of embodiments A1-14, wherein comparing the first and second sensor data with the signature data of the signature files comprises: determining, for each of the signature files, a first total number of overlapping values between the first sensor data and the signature data of the signature file, determining, for each of the signature files, a second total number of overlapping values between the second sensor data and the signature data of the signature file, determining, for each of the signature files, a first total number of continuously overlapping values between the first sensor data and the signature data of the signature file, and determining, for each of the signature files, a second total number of continuously overlapping values between the second sensor data and the signature data of the signature file, and wherein the first confidence value and the second confidence value for each of the signature files are based on the first and second total number of overlapping values and the first and second total number of continuously overlapping values.

A16. The method of any of embodiments A1-15, wherein comparing the first and second sensor data with the signature data of the signature files comprises: determining, for each of the signature files, a first total number of values of the signature data of the signature file that are within a predetermined threshold from the first sensor data, determining, for each of the signature files, a second total number of values of the signature data of the signature file that are within a predetermined threshold from the second sensor data, determining, for each of the signature files, a first total number of continuous values of the signature data of the signature file that are within the predetermined threshold from the first sensor data, and determining, for each of the signature files, a second total number of continuous values of the signature data of the signature file that are within the predetermined threshold from the second sensor data, and wherein the first confidence value and the second confidence value for each of the signature files are based on the first and second total number of values and the first and second total number of continuous values.

A17. The method of any of embodiments A1-16, wherein the first and second sensor data are compared with the signature data of the signature files when at least a portion of the first and second measured values exceeds a predetermined threshold.

A18. The method of any of embodiments A1-17, further comprising: presenting, via a user interface, the identified type of the disturbance event; requesting, via the user interface, a user to confirm accuracy of the identified type of disturbance event; retrieving, from a memory, the one or more signature files when the user confirms the accuracy of the identified type of the disturbance event; comparing the first and second sensor data with the signature data of the one or more signature files to determine differences between the first sensor data and the signature data of the one or more signature files and between the second sensor data and the signature data of the one or more signature files; and updating the signature data of the one or more signature files based on the determined differences.

44

A19. The method of any of embodiments A1-18, further comprising: identifying the disturbance event on the physical transmission line as an unknown event when the first confidence value and the second confidence value for each of the signature files does not exceed the predetermined confidence threshold; presenting, via a user interface, the disturbance event as the unknown event; requesting, via the user interface, information about the unknown event; and generating one or more new signature files based on the first sensor data, the second sensor data, and the information about the unknown event.

A20. The method of any of embodiments A1-19, further comprising: obtaining signature files corresponding to previous disturbance events, each of the signature files including signature data including previously measured values of the previous disturbance events over the length of time; comparing the first sensor data with the signature data of the signature files; determining a first confidence value for each of the signature files based on the comparison of the first sensor data with the signature data of the signature files; identifying one or more signature files whose said first confidence value exceeds a predetermined confidence threshold; and identifying a type of the disturbance event on the physical transmission line based on the identified one or more signature files.

A21. A method for identifying a location of a disturbance event on a physical transmission line, the method comprising: obtaining, from a sensing device located on the physical transmission line, sensing data, the sensing data including information regarding timestamp values of a light beam emitted by the sensing device and reflected back to the sensing device by a sensor located on the physical transmission line and information regarding a property of the light beam emitted by the sensing device and reflected back to the sensing device by the sensor; determining, based on the sensing data, (i) a roundtrip time of the light beam emitted by the sensing device and reflected back to the sensing device by the sensor and (ii) a change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the sensor; and identifying the location of the disturbance event on the physical transmission line based on (i) the roundtrip time of the light beam emitted by the sensing device and reflected back to the sensing device by the sensor and (ii) the change in the property of the light beam emitted by the sensing device and reflected back to the sensing device by the sensor.

A22. A system comprising: one or more processors; and memory storing instructions that when executed by the processors cause the processors to effectuate operations comprising those of any of embodiments A1-21.

A23. A tangible, non-transitory, machine-readable medium storing instructions that when executed by a data processing apparatus cause the data processing apparatus to perform operations comprising those of any of embodiments A1-21.

B1. A cable assembly comprising: an outer jacket; a printed circuit board including light emitting diodes; and a cable configured to transmit information, wherein the outer jacket includes a channel opening, and the printed circuit board is configured to be positioned within the channel opening and between the cable and the outer jacket.

B2. The cable assembly of embodiment B1, further comprising: an inner jacket, wherein the inner jacket surrounds the cable and the outer jacket surrounds the inner jacket.

B3. The cable assembly of any of embodiments B1-2, wherein a first thickness between an outer layer and an inner layer of the outer jacket in a section of the outer jacket that includes the channel opening is less than a second thickness

US 11,388,181 B2

45

between the outer layer and the inner layer of the outer jacket in another section of the outer jacket that does not include the channel opening.

B4. The cable assembly of any of embodiments B1-3, wherein a shape of the channel opening is rectangular, square, circular, or trapezoidal.

B5. The cable assembly of any of embodiments B1-4, wherein the outer jacket includes a plurality of channel openings and wherein a plurality of printed circuit boards are configured to be positioned within the plurality of channel openings between the cable and the outer jacket.

B6. The cable assembly of any of embodiments B1-5, wherein a depth of the channel opening is consistent throughout a length of the outer jacket.

B7. The cable assembly of any of embodiments B1-6, wherein a depth of the channel opening varies along a length of the outer jacket.

B8. The cable assembly of any of embodiments B1-7, wherein the depth of the channel opening corresponds to a difference between a first thickness and a second thickness between an outer layer and an inner layer of the outer jacket, the first thickness is measured between the outer layer and the inner layer of the outer jacket in a section of the outer jacket that includes the channel opening, and the second thickness is measured between the outer layer and the inner layer of the outer jacket in another section of the outer jacket that does not include the channel opening.

B9. The cable assembly of any of embodiments B1-8, wherein the printed circuit board is configured to be positioned within the channel opening between the inner jacket and the outer jacket.

B10. The cable assembly of any of embodiments B1-9, wherein the depth of the channel opening varies along the length of the outer jacket based on a size of the light emitting diodes.

B11. The cable assembly of any of embodiments B1-10, wherein the outer jacket is translucent.

B12. A cable assembly comprising: an inner jacket; an outer jacket; a printed circuit board including light emitting diodes; and a cable configured to transmit information, wherein the inner jacket includes a channel opening, and the printed circuit board is configured to be positioned within the channel opening and between the inner jacket and the outer jacket.

B13. The cable assembly of embodiment B12, wherein the inner jacket surrounds the cable and the outer jacket surrounds the inner jacket.

B14. The cable assembly of any of embodiments B12-13, wherein a first thickness between an outer layer and an inner layer of the inner jacket in a section of the inner jacket that includes the channel opening is less than a second thickness between the outer layer and the inner layer of the inner jacket in another section of the inner jacket that does not include the channel opening.

B15. The cable assembly of any of embodiments B12-14, wherein the inner jacket includes a plurality of channel openings and wherein a plurality of printed circuit boards are configured to be positioned within the plurality of channel openings between the inner jacket and the outer jacket.

B16. The cable assembly of any of embodiments B12-15, wherein a depth of the channel opening is consistent throughout a length of the outer jacket.

B17. The cable assembly of any of embodiments B12-16, wherein the depth of the channel opening corresponds to a difference between a first thickness and a second thickness between an outer layer and an inner layer of the inner jacket,

46

the first thickness is measured between the outer layer and the inner layer of the inner jacket in a section of the inner jacket that includes the channel opening, and the second thickness is measured between the outer layer and the inner layer of the inner jacket in another section of the inner jacket that does not include the channel opening.

B18. The cable assembly of any of embodiments B12-17, wherein the outer jacket is translucent.

B19. An outer jacket for a cable that transmits information, the outer jacket comprising: an outer layer; and an inner layer, wherein the inner layer comprises a channel opening to allow a plurality of light emitting diodes to be housed within the channel opening.

B20. An inner jacket for a cable that transmits information, the inner jacket comprising: an inner layer; and an outer layer, wherein the outer layer comprises a channel opening to allow a plurality of light emitting diodes to be housed within the channel opening.

What is claimed is:

1. A method for using a LED-embedded cable assembly to indicate a disturbance event, the method comprising:

providing one or more cable assemblies as part of a physical transmission line, wherein the one or more cable assemblies comprises a cable assembly having an outer jacket, light emitting diodes, and a core, wherein the outer jacket includes a channel opening, and the light emitting diode is positioned within the channel opening and between the core and the outer jacket;

obtaining, from multiple sensors distributed across the physical transmission line, sensor data related to a mechanical disturbance event on the physical transmission line;

determining a type of the mechanical disturbance event on the physical transmission line based on one or more mechanical disturbance event signatures, the one or more mechanical disturbance event signatures being derived from one or more prior mechanical disturbance events, wherein the mechanical disturbance event is determined to be (i) a first event type in response to the sensor data being similar to a first signature and (ii) a second event type in response to the sensor data being similar to a second signature; and

causing an action to be performed via the light emitting diodes of the cable assembly such that (ii) the action is a first visual display in response to the mechanical disturbance event being the first event type and (ii) the action is a second visual display in response to the mechanical disturbance event being the second event type.

2. The method of claim 1, wherein the cable assembly comprises circuitry configured to control the light emitting diodes, and wherein causing the action comprises providing signals to the circuitry to control the light emitting diodes to produce the first or second visual display.

3. The method of claim 2, wherein the circuitry is positioned between the core and the outer jacket.

4. The method of claim 1, wherein the core is a cable configured to transmit information.

5. The method of claim 1, wherein the outer jacket is translucent.

6. A method comprising:

providing one or more cable assemblies as part of a physical transmission line, wherein the one or more cable assemblies comprises a cable assembly having an outer jacket, one or more light emitting diodes, and a core;

US 11,388,181 B2

47

obtaining, from multiple sensors associated with the physical transmission line, sensor data related to a mechanical disturbance event on the physical transmission line;

determining a type of the mechanical disturbance event on the physical transmission line based on one or more mechanical disturbance event signatures, the one or more mechanical disturbance event signatures being derived from one or more prior mechanical disturbance events, wherein the mechanical disturbance event is determined to be (i) a first event type in response to the first and second sensor data being similar to a first signature and (ii) a second event type in response to the first and second sensor data being similar to a second signature; and

causing an action to be performed via the one or more light emitting diodes of the cable assembly such that (ii) the action is a first action in response to the mechanical disturbance event being the first event type and (ii) the action is a second action in response to the mechanical disturbance event being the second event type.

7. The method of claim 6, wherein the cable assembly comprises circuitry configured to control the one or more light emitting diodes, and wherein causing the action comprises providing signals to the circuitry to control the one or more light emitting diodes to produce a visual indication corresponding to the first or second action.

8. The method of claim 7, wherein the circuitry is positioned between the core and the outer jacket.

9. The method of claim 6, wherein the core is a cable configured to transmit information.

10. The method of claim 6, wherein the outer jacket is translucent.

11. The method of claim 6, wherein causing the action to be performed comprises causing the action to be performed via the one or more light emitting diodes such that (ii) the action is a first visual display in response to the mechanical disturbance event being the first event type and (ii) the action is a second visual display in response to the mechanical disturbance event being the second event type, the second visual display being different from the first visual display.

12. The method of claim 6, further comprising:

determining a set of light emitting diodes corresponding to a detected location of the mechanical disturbance event on the physical transmission line,

wherein causing the action to be performed comprises causing the action to be performed via the set of light emitting diodes corresponding to the detected location such that (ii) the action is a first visual display using the set of light emitting diodes in response to the mechanical disturbance event being the first event type and (ii) the action is a second visual display using the set of light emitting diodes in response to the mechanical disturbance event being the second event type, the second visual display being different from the first visual display.

13. The method of claim 12, further comprising:

causing, via a user interface, display of a disturbance type indication corresponding to the type of the mechanical disturbance event at an interface location corresponding to the detected location of the mechanical disturbance event on the physical transmission line.

14. One or more non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause operations comprising:

48

obtaining, from multiple sensors associated with a physical transmission line, sensor data related to a mechanical disturbance event on the physical transmission line, wherein the physical transmission line comprises one or more cable assemblies, the one or more cable assemblies comprising a cable assembly having an outer jacket and a core;

determining a type of the mechanical disturbance event on the physical transmission line based on one or more mechanical disturbance event signatures, the one or more mechanical disturbance event signatures being derived from one or more prior mechanical disturbance events, wherein the mechanical disturbance event is determined to be (i) a first event type in response to the first and second sensor data being similar to a first signature and (ii) a second event type in response to the first and second sensor data being similar to a second signature; and

causing an action to be performed such that (ii) the action is a first action in response to the mechanical disturbance event being the first event type and (ii) the action is a second action in response to the mechanical disturbance event being the second event type.

15. The media of claim 14, wherein causing the action to be performed comprises causing the action to be performed via one or more light emitting diodes of the cable assembly such that (ii) the action is a first action related to the one or more light emitting diodes of the cable assembly in response to the mechanical disturbance event being the first event type and (ii) the action is a second action related to the one or more light emitting diodes of the cable assembly in response to the mechanical disturbance event being the second event type, the second action being different from the first action.

16. The media of claim 14, the operations further comprising:

determining a set of light emitting diodes corresponding to a detected location of the mechanical disturbance event on the physical transmission line,

wherein causing the action to be performed comprises causing the action to be performed via the set of light emitting diodes corresponding to the detected location such that (ii) the action is a first visual display using the set of light emitting diodes in response to the mechanical disturbance event being the first event type and (ii) the action is a second visual display using the set of light emitting diodes in response to the mechanical disturbance event being the second event type, the second visual display being different from the first visual display.

17. The media of claim 14, the operations further comprising:

causing, via a user interface, display of a disturbance type indication corresponding to the type of the mechanical disturbance event at an interface location corresponding to the detected location of the mechanical disturbance event on the physical transmission line.

18. The media of claim 14, wherein the cable assembly comprises circuitry configured to control one or more light emitting diodes, and wherein causing the action comprises providing signals to the circuitry to control the one or more light emitting diodes to produce a visual indication corresponding to the first or second action.

19. The media of claim 18, wherein the circuitry is positioned between the core and the outer jacket.

US 11,388,181 B2

49

50

20. The media of claim **14**, wherein the outer jacket is translucent.

* * * * *

Exhibit 3

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

(10) **Patent No.:** **US 9,455,999 B2**
(45) **Date of Patent:** ***Sep. 27, 2016**

(54) **METHOD AND SYSTEM FOR PROTECTIVE DISTRIBUTION SYSTEM (PDS) AND INFRASTRUCTURE PROTECTION AND MANAGEMENT**

(71) Applicants: **Stephen Sohn**, Clarksburg, MD (US);
Scott Rye, La Plata, MD (US)

(72) Inventors: **Stephen Sohn**, Clarksburg, MD (US);
Scott Rye, La Plata, MD (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.
This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/849,746**

(22) Filed: **Sep. 10, 2015**

(65) **Prior Publication Data**

US 2015/0381640 A1 Dec. 31, 2015

Related U.S. Application Data

(63) Continuation of application No. 14/217,259, filed on Mar. 17, 2014, now Pat. No. 9,160,758.

(60) Provisional application No. 61/786,460, filed on Mar. 15, 2013.

(51) **Int. Cl.**
G06F 21/62 (2013.01)
G08B 13/18 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC **H04L 63/1416** (2013.01); **H04L 63/1408** (2013.01); **H04L 63/1425** (2013.01); **H04L 63/1433** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1408; H04L 63/1433; H04L 63/1416; H04L 63/1425
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,735,353 A 5/1973 Donovan et al.
4,538,140 A * 8/1985 Prestel G08B 13/126
340/556

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 2006053273 A2 5/2006

OTHER PUBLICATIONS

International Preliminary Report on Patentability dated Sep. 15 2015 for Appln. No. PCT/US2014/030330.

(Continued)

Primary Examiner — Jung Kim

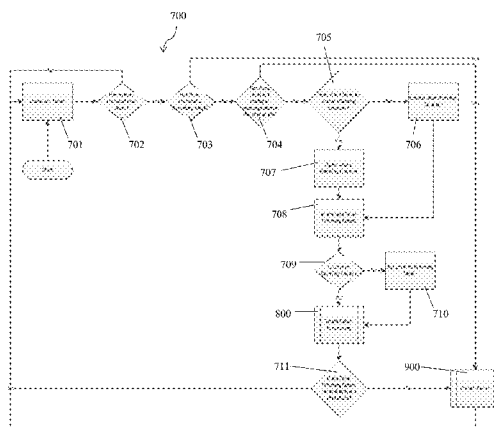
Assistant Examiner — James J Wilcox

(74) *Attorney, Agent, or Firm* — Pillsbury Winthrop Shaw Pittman, LLP

(57) **ABSTRACT**

A method and system for managing a protective distribution system is disclosed. In some embodiments, an information transmission line may be monitored. A disturbance on the information transmission line may be detected. The detected disturbance may not exceed a first preset threshold for triggering alerts of a first alert type based on detected disturbances. Responsive to the detection, a count for the number of disturbances within a preset time period that do not exceed the first preset threshold may be determined. A determination of whether the count, for the number of disturbances that do not exceed the first preset threshold, exceeds a second preset threshold may be effectuated. The second preset threshold may correspond to a preset number of allowable disturbances within the preset time period. An alert of the first alert type may be triggered responsive to a determination that the count exceeds the second preset threshold.

20 Claims, 14 Drawing Sheets



US 9,455,999 B2

Page 2

(56)

References Cited

U.S. PATENT DOCUMENTS

4,673,935	A	6/1987	Spencer	
5,194,847	A	3/1993	Taylor et al.	
5,355,208	A *	10/1994	Crawford	G01D 5/35383 250/227.19
5,680,104	A *	10/1997	Slemon	G08B 13/186 340/568.2
6,288,640	B1	9/2001	Gagnon	
6,421,632	B1	7/2002	LeCorney	
6,775,657	B1 *	8/2004	Baker	H04L 63/1408 706/45
6,819,849	B1	11/2004	Tangonan et al.	
6,980,108	B1 *	12/2005	Gebbia	G08B 13/124 340/541
7,092,586	B2	8/2006	Vokey et al.	
7,403,674	B2	7/2008	Murphy et al.	
8,135,278	B2	3/2012	Lee et al.	
8,165,723	B2 *	4/2012	Nasle	G05B 17/02 700/21
8,355,406	B1 *	1/2013	Shimamoto	H04L 41/0816 370/400
8,947,232	B2	2/2015	Strong et al.	
2006/0153491	A1 *	7/2006	Murphy	H04B 10/071 385/13
2007/0253662	A1	11/2007	Patel et al.	
2009/0031426	A1	1/2009	Dal Lago et al.	
2009/0040046	A1	2/2009	Browning, Jr. et al.	
2009/0208212	A1 *	8/2009	Lee	H04B 10/032 398/72
2010/0091676	A1	4/2010	Moran et al.	
2010/0117830	A1	5/2010	Strong et al.	
2010/0209047	A1	8/2010	Cheung et al.	
2011/0241881	A1 *	10/2011	Badinelli	G02B 6/4446 340/541

2013/0312092	A1 *	11/2013	Parker	H04L 63/1408 726/22
2013/0322490	A1 *	12/2013	Bell	G01K 11/3206 374/161
2013/0335219	A1 *	12/2013	Malkowski	G08B 13/22 340/539.22
2014/0056582	A1 *	2/2014	Roberts	H04B 10/07955 398/20
2014/0091929	A1 *	4/2014	Murphy	G08B 13/186 340/541
2014/0167952	A1 *	6/2014	Zhevelev	H04L 63/1408 340/506

OTHER PUBLICATIONS

International Search Report and Written Opinion dated Aug. 28, 2014 for Appln. No. PCT/US14/30330.

Vigil, "An Evaluation of Fiber Optic Intrusion Detection Systems in Interior Applications," Mar. 1994, pp. 1-46.

Mahmoud, "Nuisance Alarm Suppression Techniques for Fibre-Optic Intrusion Detection Systems," Third Asia Pacific Optical Sensors Conference, 2012, pp. 1-8.

NSTISS, "Protective Distribution Systems," Dec. 13, 1996, pp. 1-13.

Accu-tech Guardian, retrieved from <https://web.archive.org/web/20121115040632/http://www.accu-tech.com/protected-distribution-system/>, Nov. 15, 2012, pp. 1-4.

Alcon-Tech ISPY Fiber Optic Intrusion Detection System Data Sheet, retrieved from <http://www.alcon-tech.com/pdf/ISPY.pdf>, Jun. 2006, pp. 1-5.

Allwood, Fibre Optic Acoustic Sensing for Intrusion Detection Systems, Edith Cowan University, Research Online, ECU Publications 2011, pp. 1-7.

* cited by examiner

Figure 1

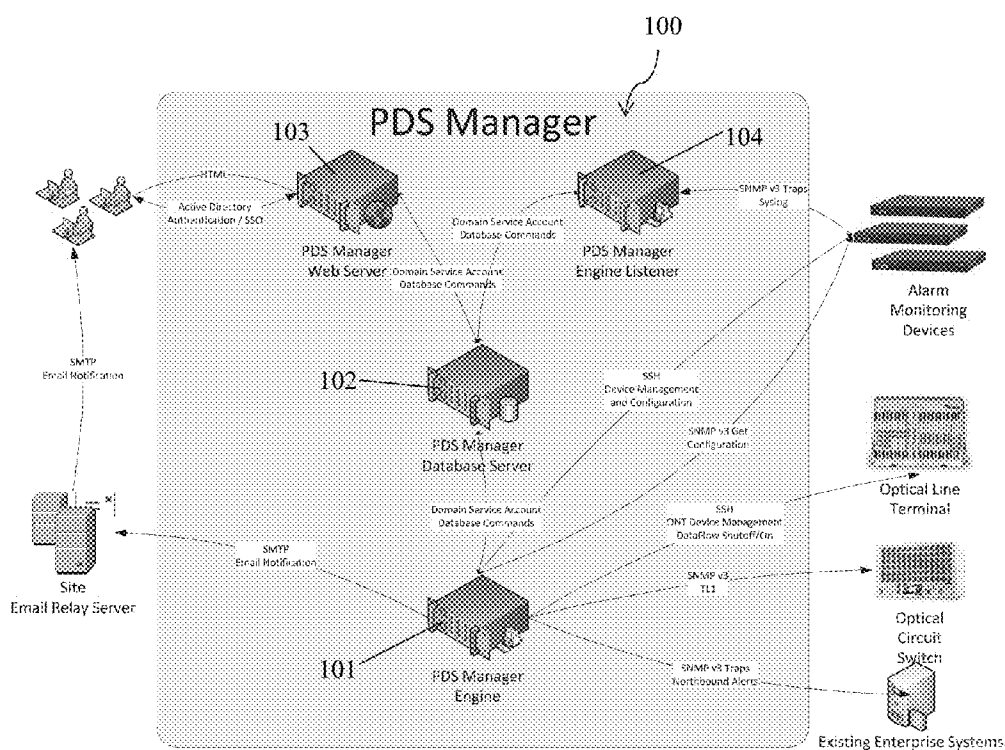


Figure 2

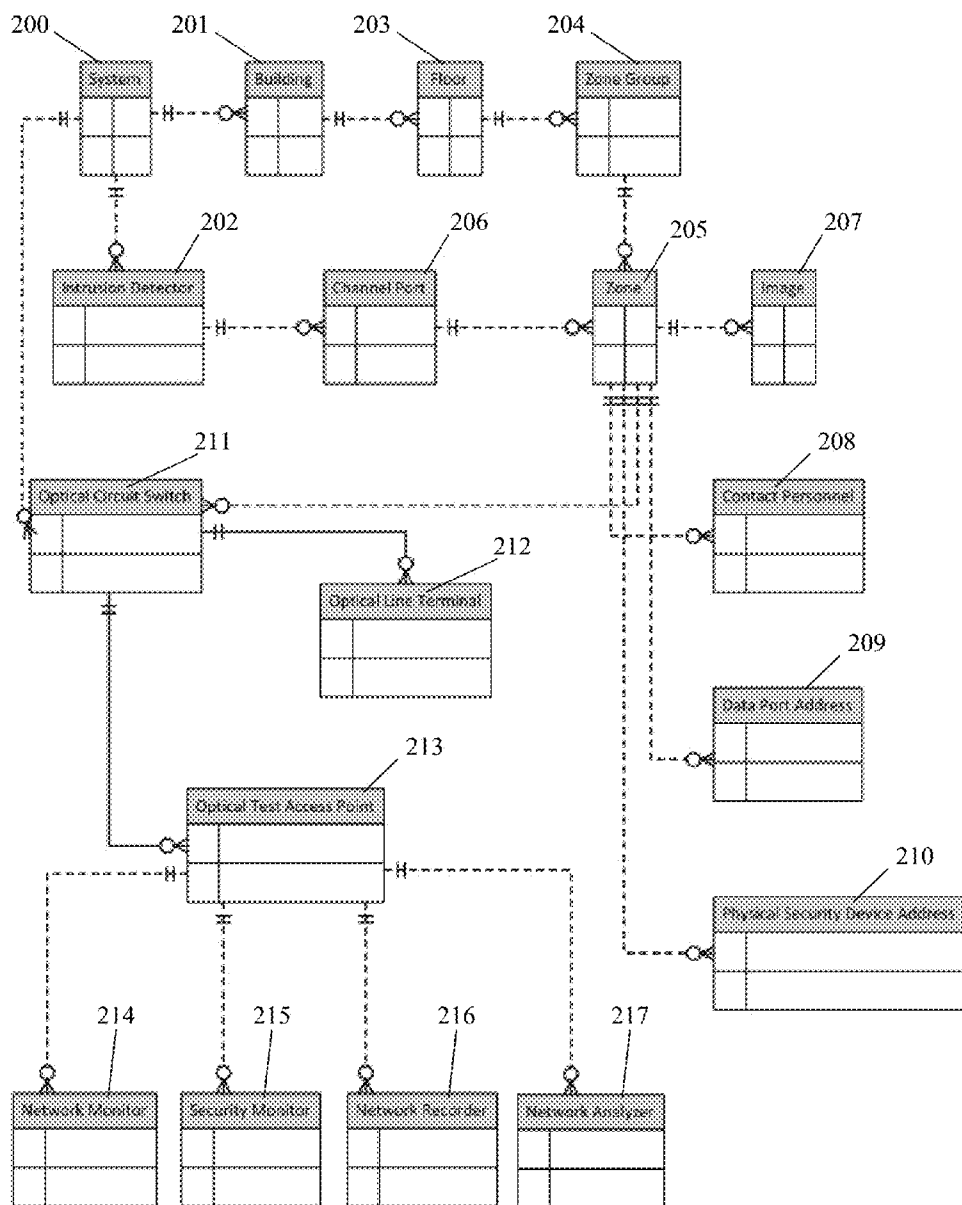
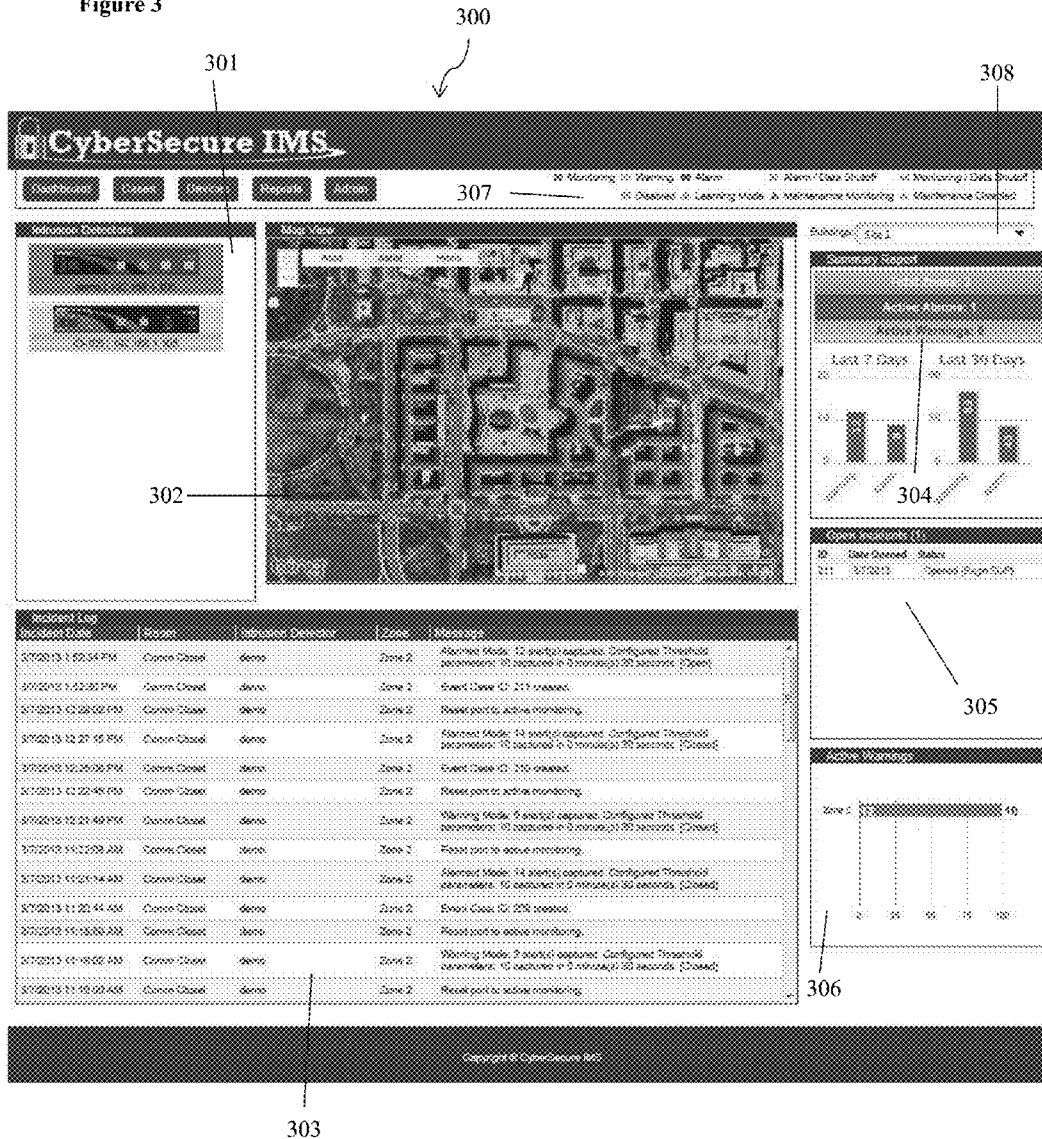


Figure 3



U.S. Patent

Sep. 27, 2016

Sheet 4 of 14

US 9,455,999 B2

Figure 4

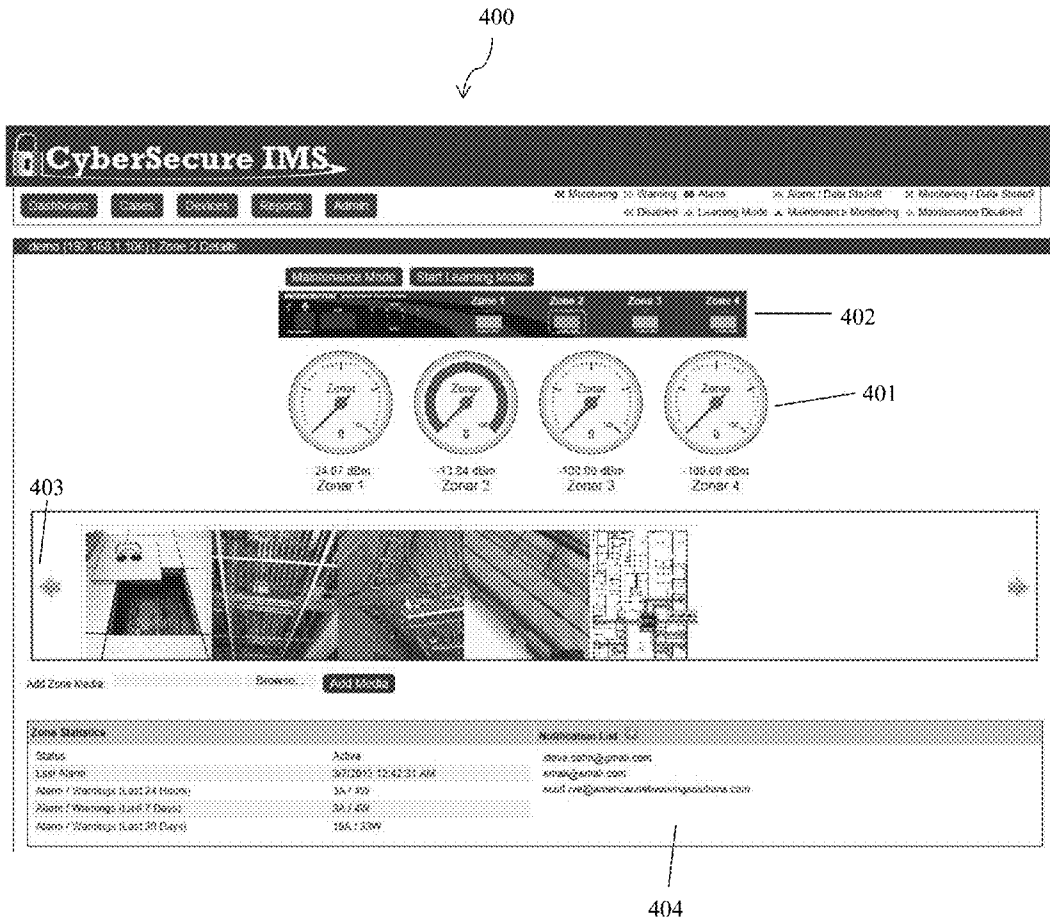


Figure 5

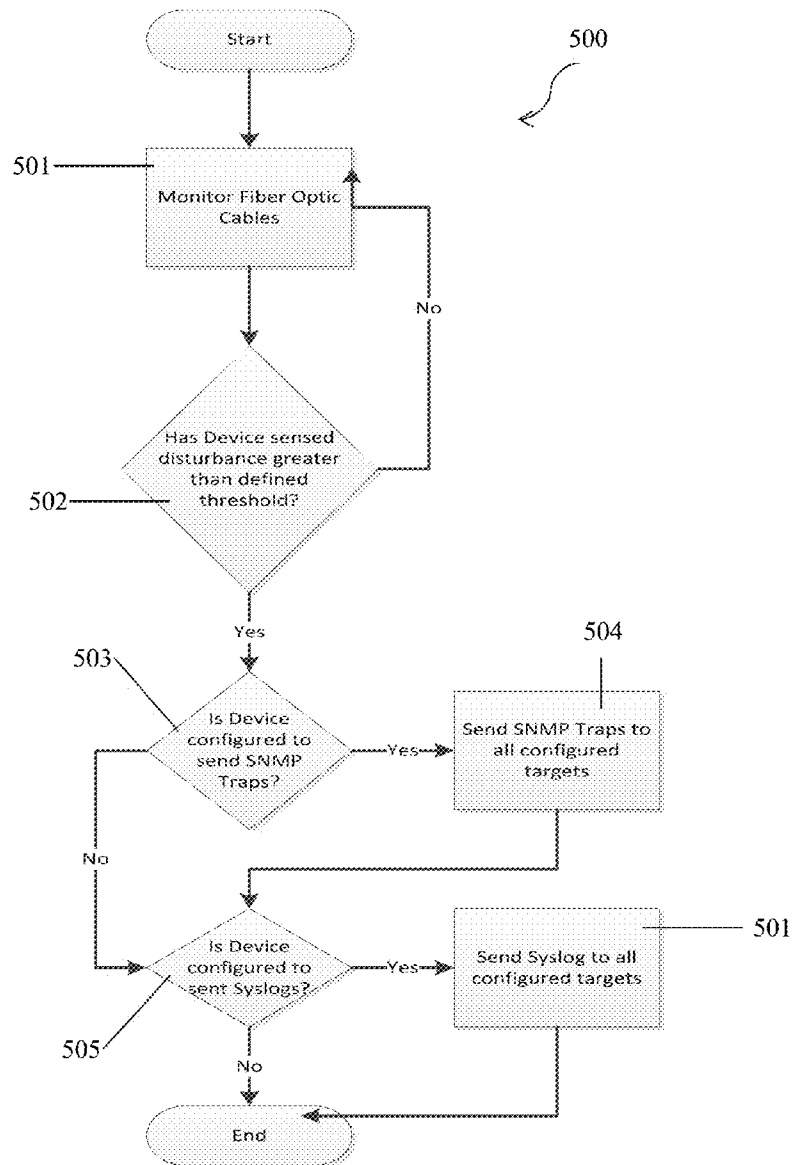
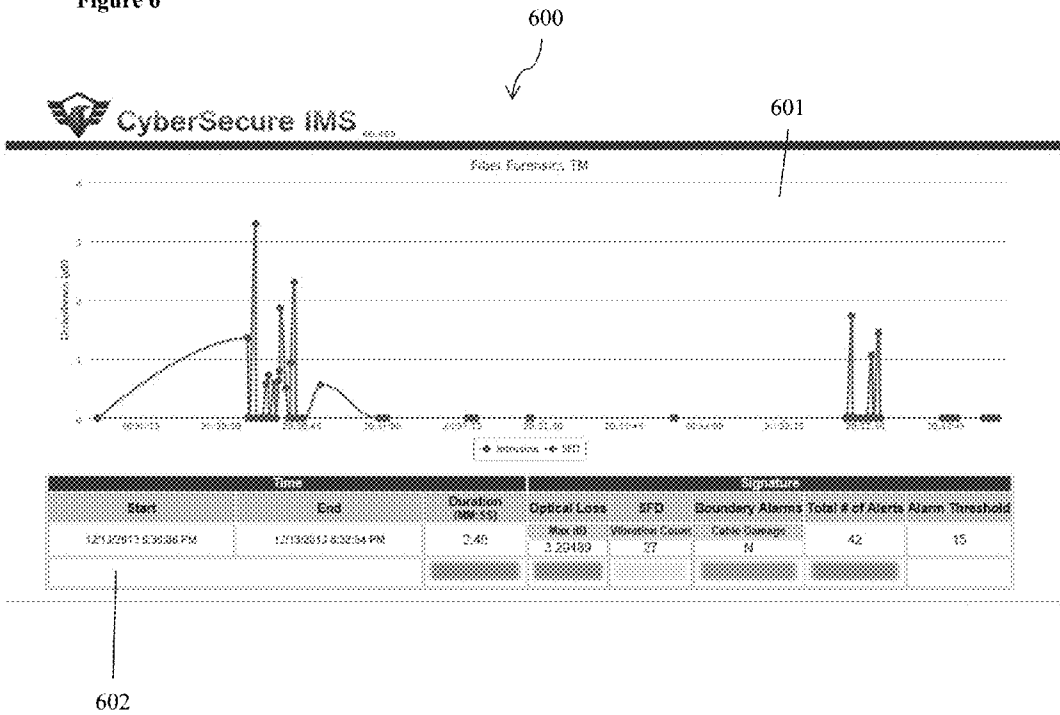


Figure 6



U.S. Patent

Sep. 27, 2016

Sheet 7 of 14

US 9,455,999 B2

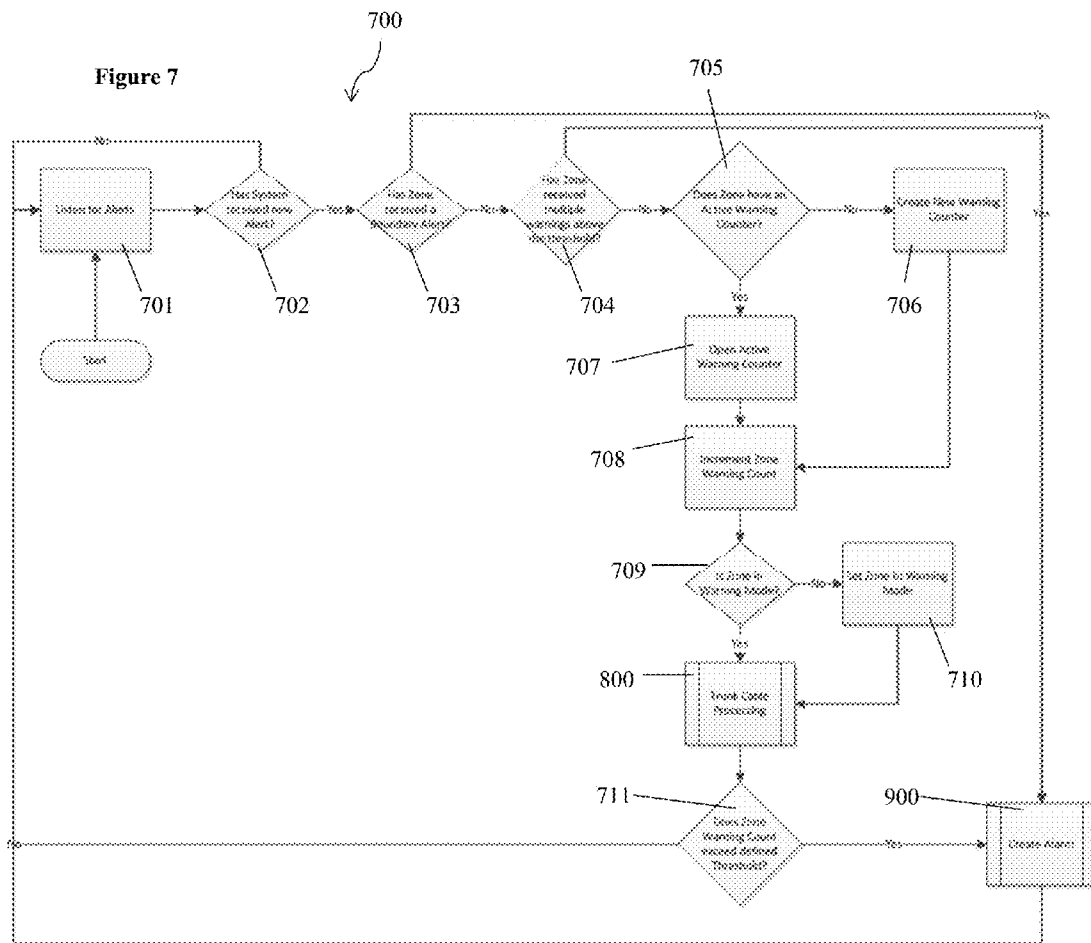


Figure 8

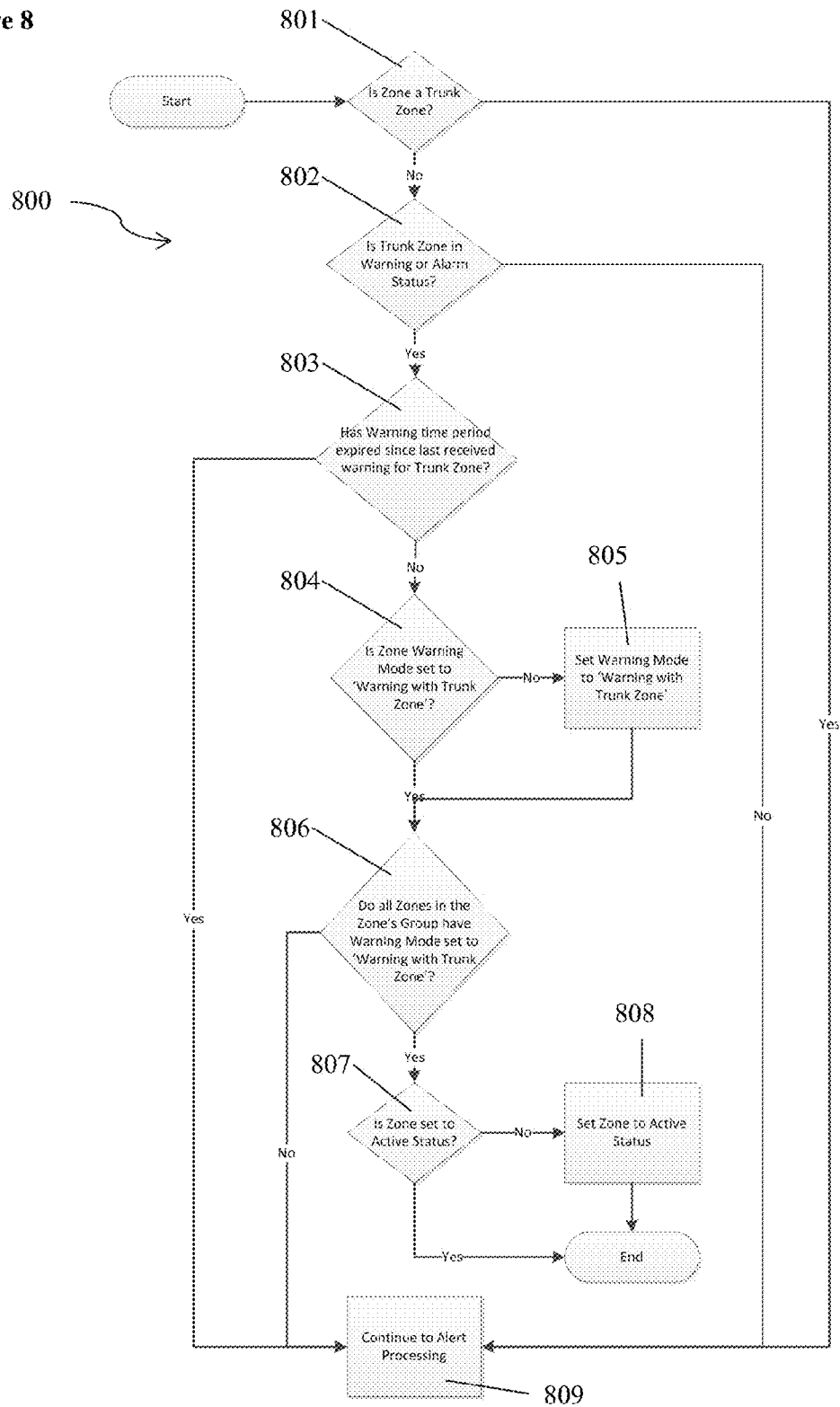


Figure 9

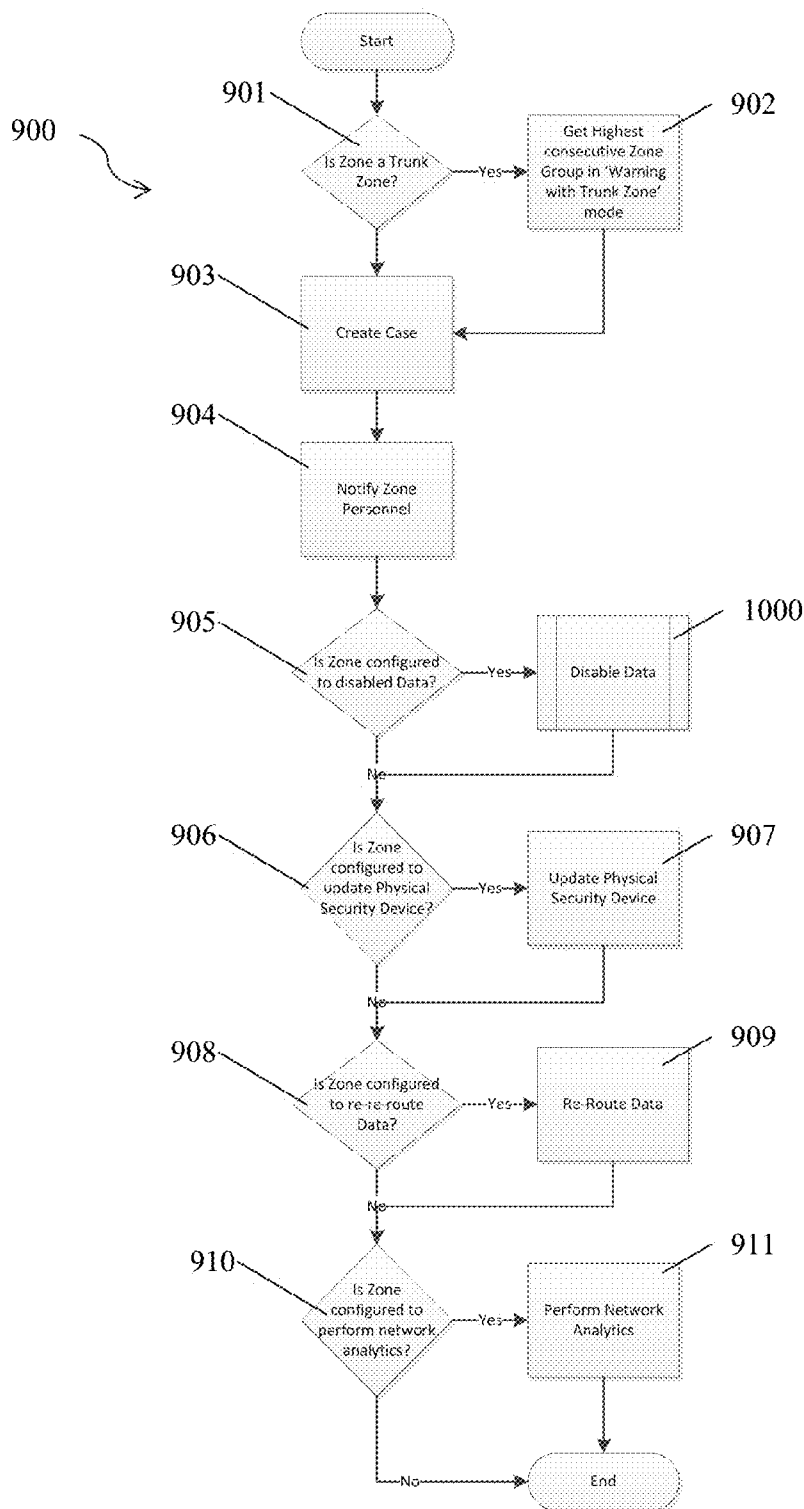


Figure 10

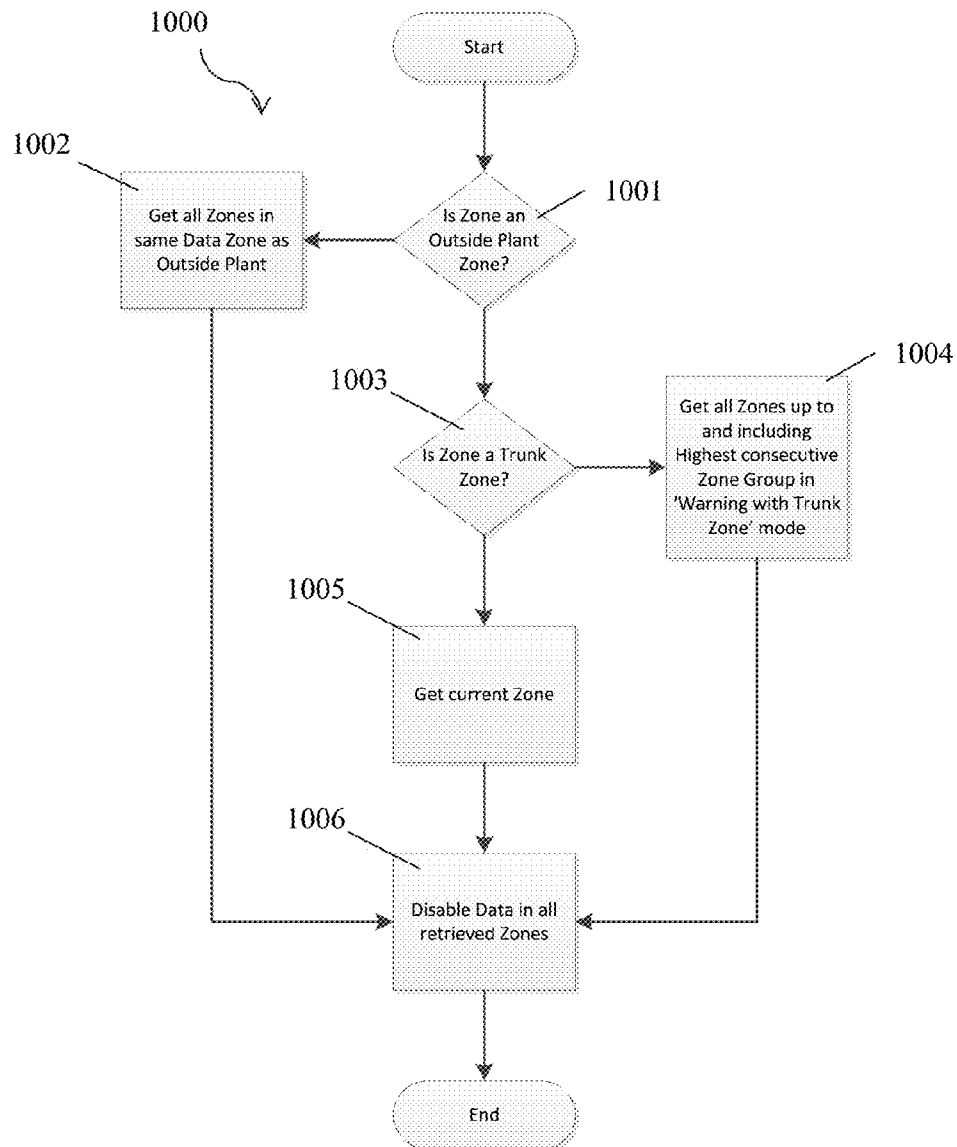


Figure 11

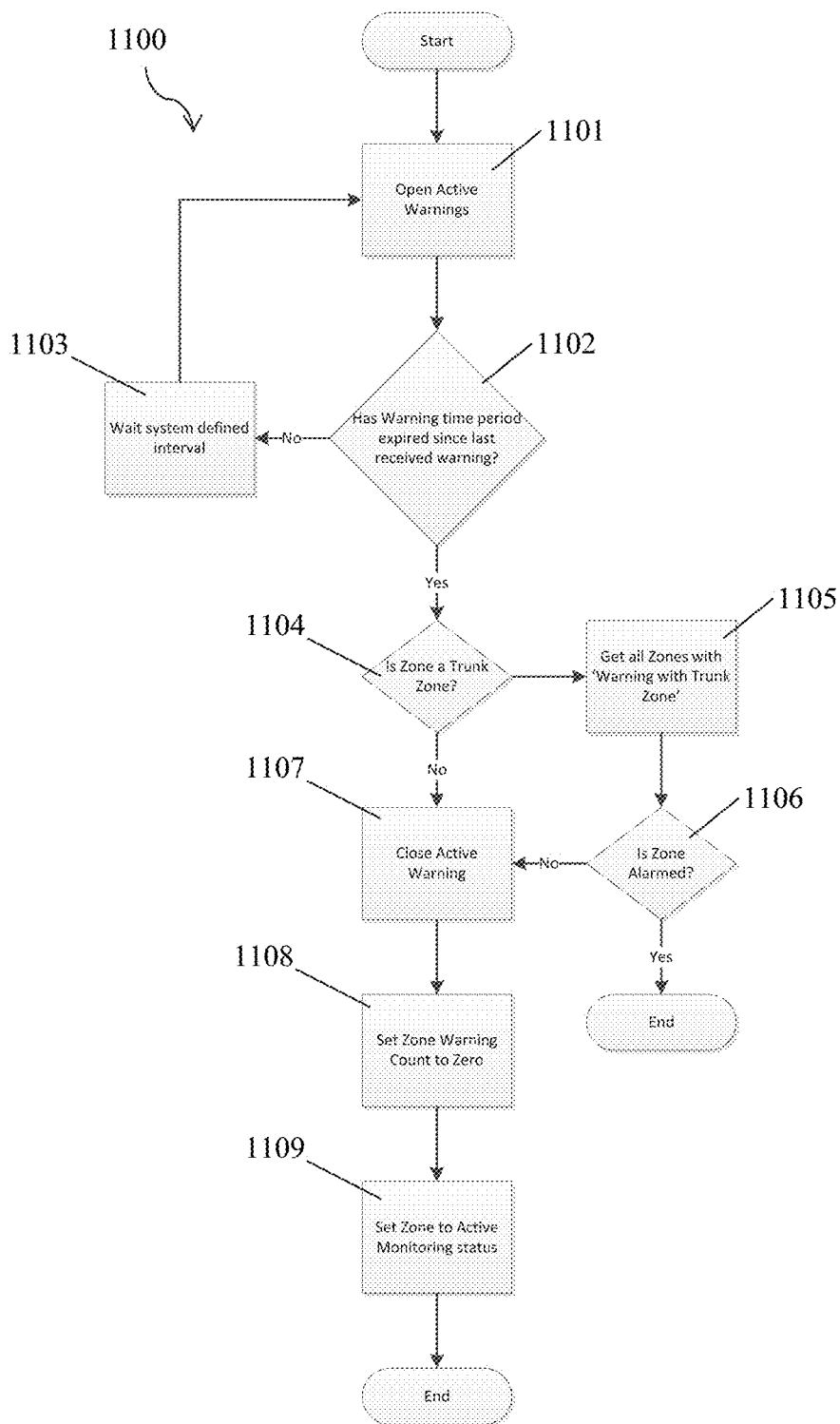


Figure 12

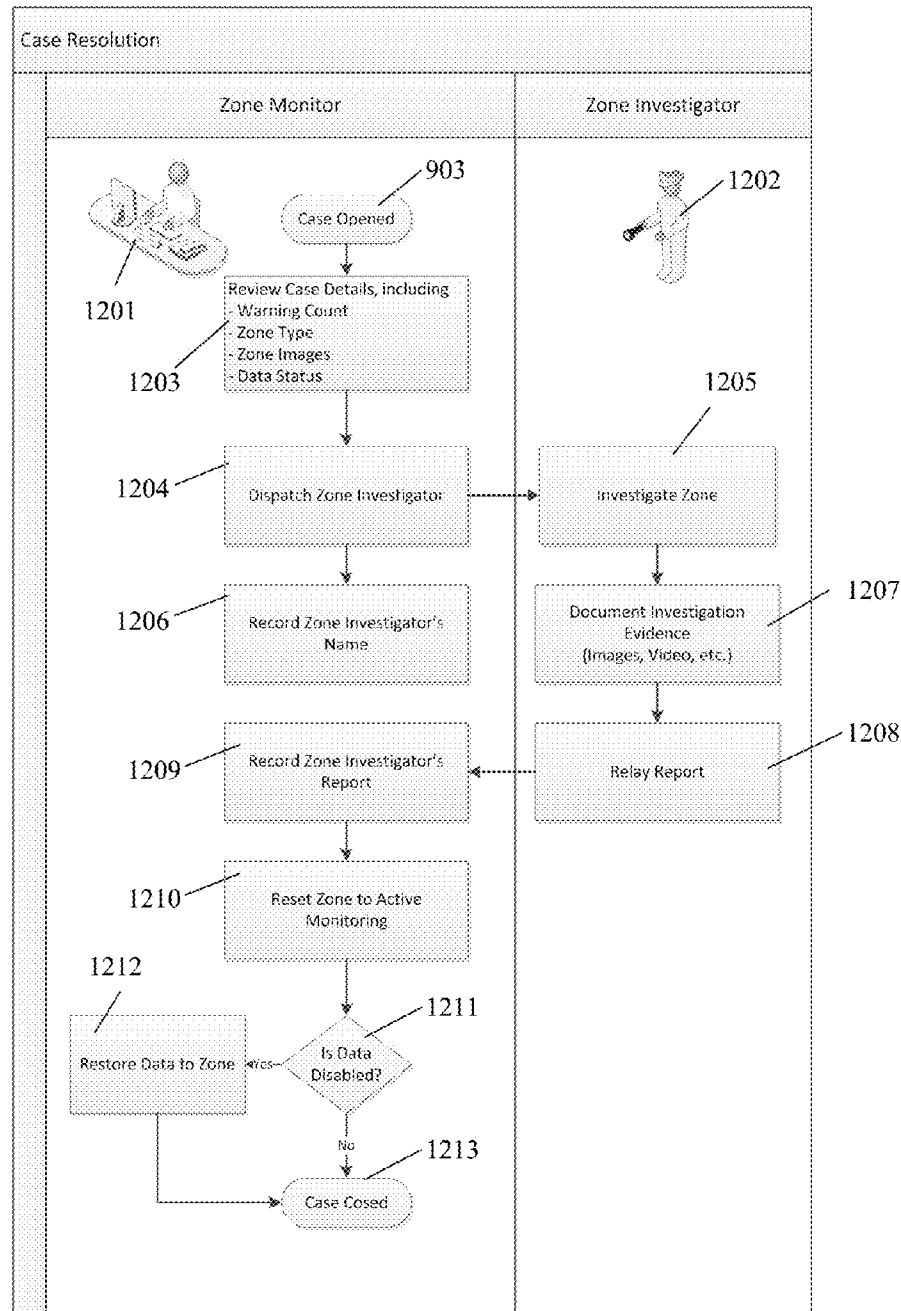
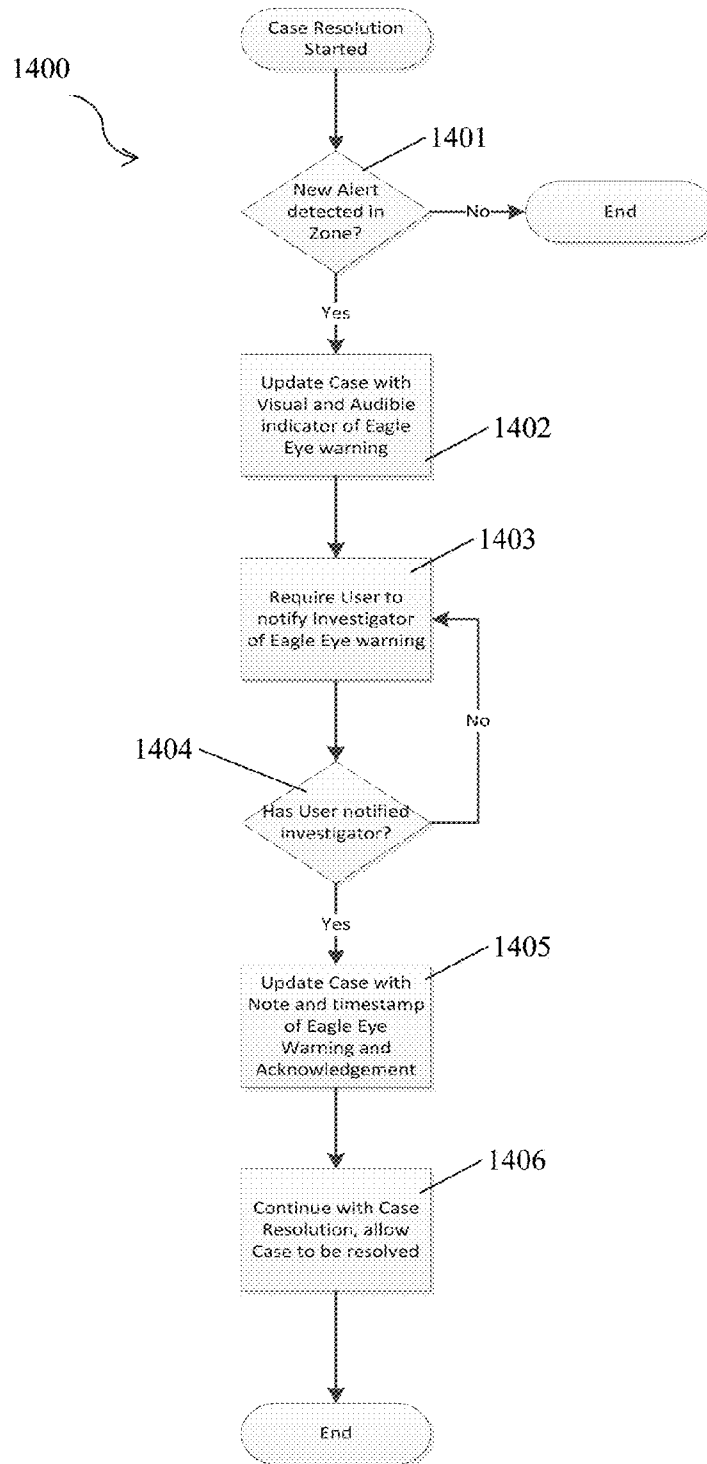


Figure 13

1300



Figure 14



US 9,455,999 B2

1

METHOD AND SYSTEM FOR PROTECTIVE DISTRIBUTION SYSTEM (PDS) AND INFRASTRUCTURE PROTECTION AND MANAGEMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 14/217,259, now U.S. Pat. No. 9,160,758 B2, filed Mar. 17, 2014, which claims the benefit of U.S. Provisional Application Ser. No. 61/786,460 filed on Mar. 15, 2013, each of which is incorporated by reference herein in its entirety.

FIELD OF INVENTION

The present invention relates to monitoring an information transmission line and, more particularly, to a method and system for managing a protective distribution system.

BACKGROUND

The protection of sensitive data has traditionally been focused on data encryption and physical security carriers (conduits) that house IT infrastructure cabling. An example of an encryption device is a TACLANE (short for "Tactical FASTLANE" or Tactical Local Area Network Encryption). A TACLANE is a network encryption device developed by the National Security Agency (NSA) to provide network communications security on Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) networks for the individual user or for enclaves of users at the same security level. An example of a physical security carrier is a Protective Distribution System (PDS). A PDS is a wireline or fiber-optics telecommunication system that includes terminals and adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information. PDS systems are not managed via software, thereby leaving the intrusion detection process and information tracking up to paper logs and human inspections once every 24 hours. When an intrusion is detected it is completely unknown what type of information was taken during the 24 hours between inspections. The lack of software management and the protection of sensitive data infrastructures have been and continue to be vulnerabilities. These and other drawbacks exist.

SUMMARY

Various embodiments as described herein solve these and other problems by providing methods and systems for protective distribution system (PDS) and infrastructure protection and management.

In a first aspect of the invention, a method for managing an information transmission line is disclosed. In one embodiment, the method includes monitoring an information transmission line, detecting a disturbance on the information transmission line, displaying the disturbance as a graphical representation, comparing the disturbance to a preset threshold, and triggering an alert if the disturbance is greater than the preset threshold or the number of disturbances less than the preset threshold meets a preset number within a preset time period.

In a second aspect of the invention, a computer-readable medium for storing computer instructions comprising instructions for managing an information transmission line

2

is disclosed. In one embodiment, the computer-readable medium comprises a set of instructions to perform a method for managing an information transmission line. The method includes monitoring an information transmission line, detecting a disturbance on the information transmission line, displaying the disturbance as a graphical representation, comparing the disturbance to a preset threshold, and triggering an alert if the disturbance is greater than the preset threshold or the number of disturbances less than the preset threshold meets a preset number within a preset time period.

In a third aspect of the invention, a system for managing an information transmission line is disclosed. In one embodiment, the system includes a computer having a set of instructions which when executed causes a processor to perform a method for managing an information transmission line. The method includes monitoring an information transmission line, detecting a disturbance on the information transmission line, displaying the disturbance as a graphical representation, comparing the disturbance to a preset threshold, and triggering an alert if the disturbance is greater than the preset threshold or the number of disturbances less than the preset threshold meets a preset number within a preset time period. The system further includes an intrusion detector, an optical line terminal and/or network switch, an optical circuit switch, an optical test access point device, and a network analytic tool.

These and other aspects of the present patent application, as well as the methods of operation and functions of the related elements of structure and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the present patent application. It shall also be appreciated that the features of one embodiment disclosed herein can be used in other embodiments disclosed herein. As used in the specification and in the claims, the singular form of "a", "an", and "the" include plural referents unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing a system architecture; FIG. 2 is a block diagram showing an overview of an exemplary PDS and IT infrastructure management system; FIG. 3 is a screenshot of a dashboard; FIG. 4 is a screenshot of a zone screen; FIG. 5 is a flowchart for monitoring alerts; FIG. 6 is a screen shot of a fiber forensic graphical display; FIG. 7 is a flowchart for processing alerts; FIG. 8 is a flowchart of a trunk cable processing subprocess; FIG. 9 is a flowchart of a create alarm subprocess; FIG. 10 is a flowchart for a process to disable data; FIG. 11 is a flowchart for processing open warnings; FIG. 12 is a chart showing a process for case resolution; FIG. 13 is a screen shot of a case detail screen; and FIG. 14 is a flowchart for continued monitoring during case management.

DETAILED DESCRIPTION

All publications, patents, and patent applications cited in this specification are hereby incorporated by reference in

US 9,455,999 B2

3

their entirety. The detailed description provided below in connection with the appended drawings is intended as a description of exemplary embodiments and is not intended to represent the only forms in which the invention may be constructed or utilized. The same or equivalent functions and sequences may be accomplished by different embodiments as will be appreciated by those skilled in the art.

FIG. 1 illustrates a block diagram of a system 100 according to an embodiment. System 100 may be used to provide proactive real-time alarm monitoring of dark fiber intrusions and may distribute notification of alarms of suspected tampering to a variety of endpoints. System 100 may include a manager engine 101, a manager database server 102, a manager web server 103, and a manager engine listener 104. In an embodiment, system 100 may include one or more components that functions as any of the manager engine, manager database server, manager web server, and manager engine listener.

System 100 may integrate with a variety of network devices to offer alarm detection and alarm response capabilities in a consolidated system. In an embodiment, system 100 may integrate with Passive Optical Network (PON) equipment, Optical Circuit Switch equipment, Optical Test Access Point equipment, and Network Analyzers to stop and start data flow to network endpoints, re-route data flow, and record or further analyze data when alarms are detected and resolved. Alarm events may be captured in a case management oriented workflow for auditing and analytics.

System 100 may provide the ability for complete network mapping of components starting from a source Optical Line Terminal (OLT) down to an end user Optical Network Terminal (ONT). Network components may be enrolled and maintained in system 100 in a logical and efficient manner. System views and reports may be leveraged to inspect an entire network as well as each data run.

System 100 may handle the coordination of tasks between dark fiber alarm monitoring devices and PON equipment through backend adapters leveraging Simple Network Management Protocol (SNMP) traps and Secure Shell (SSH) protocols. System 100 may be monitored actively and passively to assure events are not missed.

System 100 may offer a secure web user interface to provide network operations center (NOC) oriented dashboards for proactive monitoring. Notification of events may be handled in a guaranteed delivery manner over SMTP and HTTP to assure best effort notification to a targeted endpoint so first responders can focus on the status of the remaining system. Maps and images may be immediately provided with floor plan layouts overlaid with network diagrams for an alarmed area to reduce critical decision times for resolving alarms. System 100 may allow staff to identify a suspected intrusion event, isolate its location, notify responder groups, execute planned remediation, and track its history.

In an embodiment, system 100 offers a warning threshold technology to suppress the occurrence of nuisance alarms. A configurable threshold may allow system 100 to filter out accidental or environmental disturbances from actual intrusion attempts.

System 100 may integrate into an existing enterprise by providing consolidated alerts to 'north-bound' systems over SNMP. System 100 may also integrate with any existing Active Directory authentication system to assure its operation is consistent with pre-established IT security policies and site practices. System 100 may be supported by a relational database to provide redundancy, durability, recovery protection, and tools for data extraction and analysis.

4

In an embodiment, system 100 may provide health reports by providing analytics and reporting on all warnings and alarms captured by system 100. System 100 may provide trend reporting and predictive analysis. System 100 may publish and disseminate the results of the analysis to a configurable group of users at a configurable time period and frequency.

In an embodiment, system 100 may provide infrastructure management for PON Systems. System 100 may provide a graphical and textual depiction of an end to end path for a circuit. For example, one end may start from a port on an optical line terminal and/or network switch joined with a port on an intrusion detector then continue to an optical circuit switch then continue through a trunk cable then continue to a splitter then continue to a zone box then continue to a fiber run to an user area then continue to a user end device, such as an optical network terminal. Each of the devices, passive or active, and each cable run may be represented in the system graphically and textually.

System 100 may provide the ability to add, modify, or delete representative circuit paths. System 100 may track device types, identification numbers, and locations for each device. System 100 may display each circuit path overlaid on a physical diagram, such as a building or floor computer-aided design (CAD) diagram. System 100 may provide querying and reporting capabilities for each device. System 100 may highlight a circuit path when displayed in a graphical view.

Turning to FIG. 2, a schematic diagram showing an overview of a PDS and information technology (IT) infrastructure management system according to an embodiment is shown. In one embodiment, system 200 may be system 100 described above. In one embodiment, system 200 may manage an intrusion detector 202, which monitors a building 201. System 200 may provide the ability to receive alerts when intrusion detector 202 detects intrusion attempts. System 200 may also provide the ability to manage certain features of intrusion detector 202. As will be explained in greater detail below, such features may include learning mode, configuration, enabling and disabling monitoring on a channel port, and reading and updating a threshold setting. Exemplary intrusion detectors that system 200 may integrate with are 'Network Integrity Systems' INTERCEPTOR, VANGUARD, and INTERCEPTOR LD2.

In one embodiment, system 200 tracks a floor 203 of building 201 that is monitored by intrusion detector 202. Each monitored floor 203 may contain one or more zone groups 204. Within each zone group 204 may be a collection of zones 205, each of which may correspond to a single channel port 206 on intrusion detector 202. Though not depicted in the figure, system 200 may also be used to manage a collection of campuses, each of which may contain a collection of buildings.

System 200 may manage a collection of intrusion detectors 202. Intrusion detector 202 may contain a channel port 206, which corresponds to a zone 205. A zone 205 correlates to a physical location that is being monitored by system 200. A zone 205 may have an image 207, which may include computer-aided design drawings, first person perspective images, or video, to aid users in inspections. A zone 105 may also be associated with a contact personnel 208. Contact personnel 208 may be notified in the event of an intrusion attempt.

System 200 may be configured so that a zone 205 has a data port address 209 associated with the zone to integrate with a data providing networking equipment, such as an optical circuit switch or optical line terminal and/or network

US 9,455,999 B2

5

switch. In the event of an intrusion attempt in zone **205**, system **200** may disable or re-route data by sending a command to a networking equipment using data port address **209**. System **200** provides the ability to enable or disable data on a specific port and also provide the ability to read and update details for a port. Some example devices that system **200** may integrate with are Tellabs PON, Zhone PON, and Motorola POL.

Zone **205** may also have a physical security device address **210** associated with the zone. In the event of an intrusion attempt in zone **205**, system **200** may adjust physical security including locking doors, recording on IP based cameras, etc. by sending a command to physical security address **210**.

System **200** may also manage an optical circuit switch **211**. Optical circuit switch **211** may provide the ability to disable, enable, or re-route an optical transmission. Optical circuit switch **211** may have an optical line terminal and/or network switch **212**. Optical line terminal and/or network switch **212** may convert and provide a fiber optical signal to a data network. System **200** may also provide the ability to perform a bulk enrollment of a cross connect defined during initial installation or subsequent reconfiguration. An example device that system **200** may integrate with is the Calient S320 or CyberSecure Cyber Patch Panel.

Optical circuit switch **211** may have an optical test access point **213**. Optical test access point **213** may allow system **200** to provide an ability to route or copy network data. Optical test access point **213** may deliver an identical copy of network traffic to a network analytic tool, such as a network monitor **214**, a security monitor **215**, a network recorder **216**, a network analyzer **217**, and other analytic tools. An example of an optical test access point device that system **200** may integrate with is the Mimetrix OpticalTAP.

Turning to FIG. 3, a dashboard **300** according to an embodiment is shown. Dashboard **300** may provide a consolidate view from a system and allow network personnel to determine the health of a network with multiple visual indicators.

Intrusion detectors panel **301** may display a list of all intrusion detectors managed by a system. Each intrusion detector displays a colored icon for a channel port. The colored icons may correlate to a label provided in legend **307**. Each intrusion detector may be associated with a unique label, which may include information such as a user defined name, IP Address, etc. The background for the intrusion detector as shown in intrusion detector panel **301** may be programmed to change according to the status of the intrusion detector. For example, the background for an intrusion detector with a channel port in an alarmed state may be colored red. The list of intrusion detectors may be filtered to a building specific intrusion detector when a building is selected in a building drop down list **308** or when a building icon is selected in a map view panel **302**.

Map view panel **302** may be configured to display a map image with visual indicators for a building managed by a system. The location of the visual indicators may be based on the geographic coordinates of a building. The color of the visual indicator may provide a combined status for each of the intrusion detector's channel ports managed in a building. According to one embodiment, the background colors may be determined in the following hierarchy:

If one or more channel ports are in an alarmed state, the color will be red.

If one or more channel ports are in a warning state and none are in an alarmed state, the color will be yellow.

6

If no channel ports are in an alarmed or a warning state, the color will be green.

Building list **308** may contain the building names for all of the buildings managed by a system. Building list **308** may be set to a default option, e.g. option 'A1', if there are multiple buildings managed by a system. Otherwise, the list may default to a single building managed by a system. When a user selects a building, a system may filter a list of intrusion detectors in intrusion detector panel **301** to only show the devices managed in the selected building.

An incident log panel **303** may display a list of events captured or enacted by a system in response to an alert. In one embodiment, incident log panel **303** may display Incident Date, Room Name, Intrusion Detector Name, Zone Name, and Incident Message for an incident. An incident log may contain the most recent incidents for a given time parameter which may be configured in a system.

A summary report panel **304** may display a total number of zones monitored by a system. Also included may be the number of active alarms in a system as well as the number of active warnings. Summary report panel **304** may also include a chart of all warnings and alarms captured by a system in a specified time period, such as the last 7 days or the last 30 days.

An open incidents panel **305** may include a list of open cases. Open incidents panel **305** may list the ID, Date Opened, and Status for an open case.

An active warnings panel **306** may include a list of all open and active warnings. As will be described in more detail below, active warnings may be set when a set number of disturbances or alerts are captured in a defined amount of time before reaching a configured alarm threshold. The active warning feature may be known as a Zonar Warning System, a Visual Active Alert Indicator. Active warnings panel **306** may also display a graphical chart to show the number of disturbances or alerts captured by a system for a given zone as well as the alarm threshold level for the given zone. When there are no active incidents, a system may display the last number of warning events on the screen, such as the last 5 warning events.

Turning to FIG. 4, a zone screen display **400** according to an embodiment is shown. Zone screen display **400** may show a live representative view of a zone monitored by an intrusion detector. Zone screen display **400** may show a gauge **401**, which may be known as a Zonar Warning Gauge, which displays a current active warning count received by a zone and a current power level reading for a zone. In the event of receiving an alert, zone screen display **400** may show the current alert count and the numeric alarm threshold value by displaying the values in a gauge **401**. Similarly, in the event of receiving an alert, zone screen display **400** may show the severity of the alert by displaying a disturbance level in a power meter icon **402**.

In one embodiment, power meter icon **402** may display the following levels:

Minor—based on a configurable threshold on a lower end of a disturbance spectrum.

Moderate—based on a configurable threshold in between a Minor and a Major threshold.

Major—based on a configurable threshold on a higher end of a disturbance spectrum.

Critical—indicates a boundary alarm, which may occur when a cable is damaged or removed from an intrusion detector port.

Zone screen display **400** may also show a media **403** related to a zone. Media **403** may be in an image, video, or document format. A system may allow users with the

US 9,455,999 B2

7

appropriate privileges to add or remove a zone media and enter the required descriptive text for each media item. Zone screen display **400** may include additional section **404** to display information such as status of the zone, time of last alarm, alarm/warnings in the past 24 hours/7 days/30 days, and notification list for the zone.

Turning to FIG. **5**, a flowchart for creating an alert **500** according to an embodiment is shown. In **501**, an intrusion detector monitors a fiber optic cable. In one embodiment, monitoring may be performed by comparing a light transmitted to a light received in order to detect if a disturbance has occurred. In other embodiments, monitoring may be performed on vibration readings, frequency readings, changes in dB, optical time-domain reflectometer (OTDR), acoustic readings, distance determination based on reflective sensors, or combinations thereof. When a disturbance is detected, the disturbance may be compared to a defined threshold in **502**. If the disturbance is less than the defined threshold, the intrusion detector may return to monitoring a fiber optic cable in **501**. If the disturbance is greater than a defined threshold, the intrusion detector may send an alert to a target based on a configured setting.

In one embodiment, in **503** and **504**, an intrusion detector configured to send simple network management protocol (SNMP) traps may send SNMP traps to configured targets. In **505** and **506**, an intrusion detector configured to send Syslog entries may send Syslog entries to configured targets.

In one embodiment, a detected disturbance may be presented to a user as a graphical representation. FIG. **6** shows a screen shot of one embodiment of a graphical representation of detected disturbances. Graph **601** shows a detected disturbance as a function of time. The graphical points may be plotted based on the level of dB difference registered on the transmission line during the disturbance and represented accordingly with a unique graphical icon. Additional graphical points may be plotted based on vibration and acoustic calculations registered on the transmission line during the disturbance and represented accordingly with a unique graphical icon. Summary section **602** shows different characteristics of the detected disturbances. The graphical representation may include time characteristics of the detected disturbance including the start time, end time, and total duration of the detected disturbance. The graphical representation may include disturbance characteristics of the detected disturbance including the maximum optical loss measured in dB, the number of registered vibration or acoustic events, the detection of cable damage, and the total number of distinct disturbances. The graphical representation may be used by a user to determine whether an immediate alarm response is required and which alarm response team member would be able to perform the on-site inspection. Similarly, the graphical representation may be used to indicate to the user where to perform the onsite inspection first. The graphical representation showing a short duration with fluctuating dB loss may indicate that inspection starts where the transmission line is readily exposed such as in a telecommunications closet. The graphical representation showing a long duration starting with many vibration or acoustic disturbances followed by multiple fluctuating dB loss disturbances may indicate an injection of an optical tap and that the inspection include a visual inspection of the entire transmission line. The graphical representation showing optical signatures indicative of accidental contact with a low severity would be represented accordingly. Similarly, optical signatures of a sever event such as the insertion of a fiber optic tap would be represented accordingly. While the graphical representation shown in

8

FIG. **6** and described herein depicts an exemplary graphical representation of the detected disturbance, other graphical representations arranged with different plot points may be implemented based on different interfaces with various intrusion detection hardware.

In FIG. **7**, a flowchart for alert processing **700** by a system according to an embodiment is shown. In **701**, a system may keep an open port to listen for an alert. In **702**, the system determines if an alert has been received by a target. If an alert has been received, the system translates the alert to determine a zone number for the alert. In **703**, the system determines if the alert is a boundary alarm. Boundary alarms may be classified as critical severity. If the alert is a boundary alarm, the system creates an alarm as defined in 'create alarm' sub process **900**.

If the system determines that the alert is not a boundary alarm in **703**, the system may check in **704** to see if multiple warnings above a defined threshold or criteria in a have been received in a defined period of time. For example, the system may check to see if there have been 3 other previous warnings occurring within the past 24 hours for the zone. If the zone does have multiple warnings that meet a defined criteria, the system creates an alarm as defined in 'create alarm' sub process **900**.

If the system determines in **704** that the zone has not have multiple warnings that meet a defined criteria, the system may check to see if the zone has an active warning counter in **705**. The system creates a new warning counter for a zone in **706** if the zone does not have an active warning counter. If the zone does have an active warning counter, the system opens the warning counter in **707**. With an active warning counter identified for the zone, the system increments the warning count for the zone in **708**. In **709**, the system determines the status of the zone. If the zone is in a warning mode, the system proceeds to a trunk cable processing sub process **800**. A warning mode may be defined as a warning count of greater than 1. If the zone is not in a warning mode, the system sets the zone to a warning status in **710** and then proceeds to 'trunk cable processing' sub process **800**.

In one embodiment, the system evaluates trunk cable processing in a 'trunk cable processing' sub process **800**. After the trunk cable processing sub process, the system moves on to **711** to determine if the warning count exceeds the defined threshold for the zone. If the warning count exceeds the defined threshold for the zone, the system creates an alarm in 'create alarm' sub process **900** and then returns to **701** to listen for alerts. If the warning count does not exceed the defined threshold for the zone, the system returns to **701** to listen for alerts. While the flowchart shown in FIG. **7** and described herein depicts an exemplary workflow for processing an alert, other workflows arranged in a different order may be implemented.

In FIG. **8**, a flowchart for 'trunk cable processing' sub process **800** according to an embodiment is shown. In **801**, a system determines if the zone is a trunk zone. In one embodiment, a trunk zone may be defined as a zone that includes a trunk cable. A trunk cable may be co-bundled with monitoring cables for each floor. At each floor, the cables dedicated to that floor may distribute out to the floors. A trunk cable and remaining floor cables may continue down a riser closet (e.g. communication network closets that traverse up and down an area of a building). Having a dedicated trunk zone that may be monitored by a system may allow for a logical separation of user zones (e.g. network cables distributing data throughout a floor of a building) from a riser closet and a source closet (e.g. place where network data for a building originates). Without a

US 9,455,999 B2

9

trunk cable, on an intrusion or disturbance, an investigator may be required to inspect an entire user zone and then back up a riser closet and back to a source closet. Logical separation may allow for meeting an inspection requirement, such as an inspection being required within 15 minute of an alert.

If the zone is a trunk zone, the system proceeds to **809** to evaluate the alert as a standard zone and returns to step **711** as described above. If the zone is not a trunk zone, the system continues to **802** to determine if the trunk zone is in a warning or an alarmed status. If the system is not in a warning or alarmed status, the system proceeds to **809** to evaluate the alert as a standard zone and returns to step **711** as described above. If the trunk zone is in a warning or an alarmed status, the system proceeds to **803** and determines if a warning time period has expired since the last received warning for the trunk zone. The warning time period may be configured by a user to a desired length. If the warning time period has expired, this may indicate an intrusion attempt on a separate zone in addition to an intrusion attempt on the trunk zone and the system proceeds to **809** to evaluate the alert as a standard zone and returns to step **711**.

If the system determines in **803** that the warning time period has not expired, this may indicate that there is an alert in a zone in conjunction with the trunk zone and the system proceeds to **804**. In **804**, the system determines if the zone warning mode has been set to a predetermined setting. In one embodiment, the predetermined setting may be 'Warning with Trunk Zone'. In one embodiment, if the zone does not have a warning mode of 'Warning with Trunk Zone' **804**, the system sets the warning mode to 'Warning with Trunk Zone' in **805** prior to moving onto **806**. In **806**, the system evaluates if all zones in the zone's zone group have warning modes set to 'Warning with Trunk Zone'. In one scenario, if a cable in a riser closet is disturbed, the trunk cable and all of the cables that are monitoring the floors below will set off alerts. In this case, the floor cables will have a 'Warning with Trunk Zone' status so the system can separate these from a user zone. If not, the system proceeds to **809** to evaluate the alert as a standard zone and returns to step **711**.

If all zones in the zone's zone group have warning modes set to 'Warning with Trunk Zone', this may indicate that the entire zone group has received alerts in conjunction with the trunk zone. In that instance, the system will not evaluate the alert as a standard zone, but instead the system may suppress it. The system then proceeds to **807** to determine if the zone is set to active status. If not, the system sets the zone to active status in **808** and proceeds to continue to alert processing. While the flowchart shown in FIG. 8 and described herein depicts an exemplary workflow for a trunk cable processing sub process, other workflows arranged in a different order may be implemented.

Turning to FIG. 9, a flowchart for 'create alarm' sub process **900** according to an embodiment is shown. A system may create an alarm according to 'create alarm' sub process **900** when a zone receives a boundary alert, when a zone receives multiple warnings above a criteria, or when a zone warning count exceeds a defined threshold for the zone. In **901**, a system evaluates if a zone is a trunk zone. If the zone is a trunk zone, the system may retrieve the highest consecutive zone group with a warning mode of 'Warning with Trunk Zone' in **902**. A system may indicate this information in a case as described in more detail below.

A system may create and opens a case in **903**. If a case was opened due to a boundary alert, a system may notate the case accordingly. In **904**, a system may notify a personnel related to a zone. If a case was opened due to a boundary alert, a

10

system may notate the notification accordingly. In **905**, a system may determine if a zone is configured to disable data. If yes, the system may perform a disable data sub process **1000**. In **906**, a system may determine if a zone is configured to update a physical security device. If yes, the system may perform the action based on a zone setting by sending a command to the physical security device management platform in **907**. In **908**, a system may determine if a zone is configured to re-route network data. If yes, the system re-routes data based on a zone setting by sending a command to an optical circuit switch in **909**. In **910**, a system may determine if a zone is configured to perform network analysis. If yes, the system performs an action based on a zone setting by sending a command to an optical test access point in **911**. A system may communicate with a network analytic tool based on a defined action. While the flowchart shown in FIG. 9 and described herein depicts an exemplary workflow for a create alarm sub process, other workflows arranged in a different order may be implemented.

In FIG. 10, a flowchart for 'disable data' sub process **1000** according to an embodiment is shown. In **1001**, a system may evaluate a zone type. In **1002**, if a zone is an outside plant zone, the system may collect all zones in a same data zone as the outside plant zone. The system may then proceed to **1006** to disable data in all of these zones.

In **1003**, a system may evaluate if a zone is a trunk zone. If yes, the system collects all zones up to and including the highest consecutive zone group with a warning mode of 'Warning with Trunk Zone' in **1004**. The system may then proceed to **1006** to disable data in all of these zones. In **1003**, if a system determines that a zone is not a trunk zone but is a user zone, the system may retrieve the current zone in **1005** and proceed to disable data in this zone in **1006**.

A system may be configured to disable data by directly communicating with an optical line terminal and/or network switch by sending a command to the optical line terminal and/or network switch. A system may also be configured to disabled data by communicating with an optical circuit switch by sending a command to the optical circuit switch. While the flowchart shown in FIG. 10 and described herein depicts an exemplary workflow for a disable data sub process, other workflows arranged in a different order may be implemented.

Turning to FIG. 11, a work flow for processing open warnings **1100** according to an embodiment is shown. In **1101**, on a defined interval, a system may open all active warnings. In **1102**, a system may determine if a warning time period has elapsed since last receiving a warning timestamp. If the warning time period has not elapse, the system may proceed to **1103** and wait for a defined interval before returning to check all active warnings. If the warning time period has elapsed, the system may proceed to **1104** to determine if a zone is a trunk zone. If the zone is not a trunk zone, the system may proceed to **1107** and close an active warning. If the zone is a trunk zone, the system may collect all zones up to and including the highest consecutive zone group with a warning mode of 'Warning with Trunk Zone' in **1105** and may then proceed to **1106**. In **1106**, a system may check if the trunk zone is alarmed. If not, the system may close the active warning in **1107**. In **1108**, a system may set a zone warning count to zero. In **1109**, a system may set a zone status to active monitoring. While the flowchart shown in FIG. 11 and described herein depicts an exemplary workflow for processing open warnings, other workflows arranged in a different order may be implemented.

FIG. 12 shows a case resolution process according to an embodiment. In **1203**, when a case is created, a zone monitor

US 9,455,999 B2

11

1201 may open the case and review the case details. The case details displayed by a system may include warning count, zone type, zone images, zone inspection guide, notified contact personnel, and status of the data network. A case detail screen according to one embodiment is shown in FIG. 13.

In **1204**, zone monitor **1201** may dispatch an investigator **1202** assigned to a zone. In **1206**, zone monitor **1201** may record zone investigator's **1202** name. In **1205**, zone investigator **1202** may investigate a zone based on a Standard Operating Procedure defined by a system for a zone. In **1207**, zone investigator **1202** may document evidence such as images or videos of the inspection. In **1208**, upon completion of an investigation, zone investigator **1202** may relay a full report in back to zone monitor **1201**, including investigation evidence, a written report, and a final determination. Final determinations may include items such as intrusion, accidental contact, unscheduled maintenance, natural disaster, and other items.

In **1209**, zone monitor **1201** may record zone investigator's **1202** report into a system. In **1210**, a system may enable zone monitor **1201** to reset monitoring on a zone.

In **1211**, when zone monitor **1201** resets monitoring on a zone, a system may check to see if data was disabled in a zone. If so, the system may allow zone monitor **1201** to restore data to the zone in **1212**. Zone monitor **1201** may then restore data to the zone.

In **1213**, a system may then close a case and track a time stamp for each event for audit and reporting purposes. While the workflow for a case resolution process as shown in FIG. 12 and described herein depicts an exemplary workflow, other workflows arranged in a different order may be implemented.

In an embodiment, when a case is open and under review, a system may continue to monitor for new alerts in a zone. FIG. 14 shows a flowchart **1400** of a process for a system to continue monitoring during a case management. In **1401**, a system may determine if a new alert is detected in a zone. In **1402**, if a new alert is detected, the system may update an interface with visual and audible indicators, such as an Eagle Eye Zonar warning. This scenario may occur if an intrusion attempted is continuing. This process may provide an investigator situational awareness and allow for additional safety or response measures.

In **1403**, a system may require a user to notify an investigator of the Eagle Eye Zonar warning. In **1404**, a system may determine if a user has notified an investigator. If not, the system may return to **1403** to require a user to notify an investigator. In **1405**, after a user notifies an investigator, the system may update a case note with information and timestamp for the Eagle Eye warning detection and user acknowledgement. In **1406**, a system may then allow a user to continue with a case resolution process. While the flowchart shown in FIG. 14 and described herein depicts an exemplary workflow for a process to continue monitoring during a case management, other workflows arranged in a different order may be implemented.

According to an embodiment, a system may allow a user with an appropriate privilege the ability to modify a case resolution workflow. A system may allow for adding or removing steps into a workflow. A system may allow for routing and re-routing approval or disapproval functions to a user, collection of users, roles or a collection of roles in a system. Where appropriate, a system may allow for modification of a workflow through a graphically based user interface.

12

In one embodiment, a system may be configured for predictive analysis. A system may calculate the captured alert signatures (duration, count, maximum/minimum/average power, etc.) for a case as well as an associated case resolution status. A system may provide artificial intelligence capabilities in analyzing an alert signature and a resolution to compute likelihood scores for possible causes for an alert.

For a case, a system may use a predictive analysis to offer likelihood scores on the case resolutions status. For each warning, a system may provide a real-time likelihood score for a cause of an alert.

Other features of a system may provide the ability to continuously monitor a given IP address range to discover and enroll unregistered intrusion detectors. A system may allow a user to create a new enrollment task. An enrollment task may include:

Starting IP Address

Ending IP Address

Login ID for Intrusion Detector

Password for Login ID for Intrusion Detector

Frequency at which the Enrollment Task should run (Never, Daily, Weekly)

SNMP Credentials for communication with the Intrusion Detector

Option to All Remote Reset of the Channel Ports of the Intrusion Detector

Option to Disable Data in the Zones when an Alarm occurs

Warning Threshold Count

Warning Threshold Time Period

Alarm Response for Intrusion Alerts (None, Report, Report & Halt, Halt)

Alarm Response for Boundary Alerts (None, Report, Report & Halt, Halt)

Alarm Response for Smart Filter Detect Alerts (None, Report, Report & Halt, Halt)

Device Availability Time Period

During enrollment, a system may query a discovered device and gather device specific information such as the model and the port count of the device. A system may use the information to dynamically enroll the device. A system may provide the ability to discover a variety of device models and types from one enrollment task.

After enrollment completes, a system may read an intrusion detector threshold setting. A system may disable monitoring on channel ports that are determined to not have a fiber cable plugged into it. A system may provide a wizard based workflow to allow a user to provide additional information to configure an enrolled device.

According to another embodiment, a system may provide the ability to set a specific channel port on an intrusion detector into a Learning Mode or Auto Configure. In this mode, an intrusion detector observes a fiber for a channel port for a configurable period of time to determine an optimal monitoring parameter that may be used for monitoring intrusions, excessive optical gains/losses or environmental changes.

A system may be configured to allow a user with an appropriate privilege an option to perform Learning Mode. When the option is selected, the system may present an allowed user with a screen offering various time periods. When a user initiates a task in a system, the system sends an appropriate command to an intrusion detector to begin Learning Mode. A system may set the channel port Report only for any alert and not send Halt alerts. At any time during Learning Mode, a system may allow a user to abort

US 9,455,999 B2

13

Learning Mode. A system may continue to receive a detected alert during Learning Mode and may record the results in the system for further consideration by a user.

When Learning Mode completes, a system may receive a notification from an intrusion detector. A system may read and record a threshold setting determined during Learning Mode and associate the setting to a specific zone. A system may reset a channel port back from Report only to a previous setting.

A system may read and record a current threshold setting of a channel port of an intrusion detector and associate the setting to a specific zone. For a setting, a system may indicate if the setting was Learned, set by Default, or set by a User.

A system may allow a user with an appropriate privilege the ability to sync a setting from a device to a system. A system may allow a user with an appropriate privilege the ability to edit any or all of the settings. When a user initiates a task in a system to update a setting, the system may send an appropriate command to an intrusion detector to update the settings based on the user provided values. Any settings unchanged by a user remain unaffected.

A system may be deployed for various purposes. In one embodiment, a system may be used to verify whether a data infrastructure is suitable for alarmed carrier PDS. This testing process maybe used pre-deployment on existing cables and conduit or during post-deployment testing process to validate new installations of alarmed cables and conduit.

While the invention has been described in detail with reference to particularly preferred embodiments, those skilled in the art will appreciate that various modifications may be made thereto without significantly departing from the spirit and scope of the invention.

What is claimed:

1. A method for managing a protective distribution system, comprising:

monitoring a fiber optic information transmission line; detecting, via one or more sensors, a disturbance on the fiber optic information transmission line, wherein the detected disturbance does not exceed a first preset threshold for triggering alerts of a first alert type based on detected disturbances, and wherein the one or more sensors comprise at least one of a vibration sensor, a frequency sensor, an acoustic sensor, and reflective sensor;

determining, responsive to the detection via the one or more sensors, a count for the number of disturbances within a preset time period that do not exceed the first preset threshold;

determining whether the count, for the number of disturbances that do not exceed the first preset threshold, exceeds a second preset threshold for triggering alerts of the first alert type, wherein the second preset threshold corresponds to a preset number of allowable disturbances, not exceeding the first preset threshold and within the preset time period, before one or more alerts of the first alert type are to be triggered; and

triggering an alert of the first alert type responsive to a determination that the count exceeds the second preset threshold.

2. The method of claim 1, wherein (1) the detected disturbance is of a first disturbance type, (2) the first preset threshold is a threshold for triggering alerts of the first alert type based on detected disturbances of the first disturbance type, and (3) the second preset threshold corresponds to a

14

preset number of allowable disturbances of the first disturbance type within the preset time period.

3. The method of claim 2, wherein the detected disturbance of the first disturbance type comprises at least one of a vibration, a frequency change, an acoustic change, and a change in distance based on reflectometer reading, and a disturbance of a second disturbance type comprises at least a different one of a vibration, a frequency change, an acoustic change, and a change in distance based on reflectometer reading.

4. The method of claim 1, wherein the detected disturbance comprises a vibration-related disturbance, and wherein the first preset threshold is a threshold for triggering alerts based on detected vibration-related disturbances.

5. The method of claim 1, wherein the detected disturbance comprises a frequency-change-related disturbance, and wherein the first preset threshold is a threshold for triggering alerts based on detected frequency-change-related disturbances.

6. The method of claim 1, wherein the detected disturbance comprises an acoustic-change-related disturbance, and wherein the first preset threshold is a threshold for triggering alerts based on detected acoustic-change-related disturbances.

7. The method of claim 1, wherein the detected disturbance comprises a disturbance related to a change in signal propagation distance, and wherein the first preset threshold is a threshold for triggering alerts based on detected disturbances related to a change in signal propagation distance.

8. The method of claim 1, further comprising:

initiating a response to the detected disturbance responsive to the triggering of the alert of the first alert type, wherein the response comprises at least one of opening a case, dispatching an investigator to investigate the detected disturbance, and documenting the investigation in the case.

9. The method of claim 1, further comprising:

initiating a response to the detected disturbance responsive to the triggering of the alert of the first alert type, wherein the response comprises at least one of disabling a data collection, adjusting a physical security device, rerouting a data collection, and performing network analysis.

10. The method of claim 1, further comprising:

causing the detected disturbance to be presented in comparison to the first preset threshold in real-time responsive to the detection of the disturbance.

11. The method of claim 1, wherein the count is for the number of disturbances within the preset time period that do not exceed the first preset threshold, but exceeds a third preset threshold.

12. A system for managing a protective distribution system, comprising:

a computer system comprises one or more processors programmed to execute computer program instructions which, when executed, cause the computer system to: monitor a fiber optic information transmission line; detect, via one or more sensors, a disturbance on the fiber optic information transmission line, wherein the detected disturbance does not exceed a first preset threshold for triggering alerts of a first alert type based on detected disturbances, and wherein the one or more sensors comprise at least one of a vibration sensor, a frequency sensor, an acoustic sensor, and reflective sensor;

US 9,455,999 B2

15

determine, responsive to the detection via the one or more sensors, a count for the number of disturbances within a preset time period that do not exceed the first preset threshold;

determine whether the count, for the number of disturbances that do not exceed the first preset threshold, exceeds a second preset threshold for triggering alerts of the first alert type, wherein the second preset threshold corresponds to a preset number of allowable disturbances, not exceeding the first preset threshold and within the preset time period, before one or more alerts of the first alert type are to be triggered; and

trigger an alert of the first alert type responsive to a determination that the count exceeds the second preset threshold.

13. The system of claim 12, further comprising: an intrusion detector coupled to the computer system, the disturbance is detected by the computer system via the intrusion detector.

14. The system of claim 13, further comprising: an optical line terminal or network switch; an optical circuit switch; an optical test access point device; a network analytic tool; and a video camera.

15. The system of claim 12, wherein (1) the detected disturbance is of a first disturbance type, (2) the first preset threshold is a threshold for triggering alerts of the first alert type based on detected disturbances of the first disturbance type, and (3) the second preset threshold corresponds to a preset number of allowable disturbances of the first disturbance type within the preset time period.

16. The system of claim 15, wherein the detected disturbance of the first disturbance type comprises at least one of a vibration, a frequency change, an acoustic change, and a change in signal propagation distance, and a disturbance of a second disturbance type comprises at least a different one of a vibration, a frequency change, an acoustic change, and a change in signal propagation distance.

17. The system of claim 12, wherein the computer system is further caused to: initiating a response to the detected disturbance responsive to the triggering of the alert of the first alert type, wherein the response comprises at least one of opening

16

a case, dispatching an investigator to investigate the detected disturbance, documenting the investigation in the case, disabling a data collection, adjusting a physical security device, rerouting a data collection, and performing network analysis.

18. The system of claim 12, wherein the computer system is further caused to:

causing the detected disturbance to be presented in comparison to the first preset threshold in real-time responsive to the detection of the disturbance.

19. The system of claim 12, wherein the count is for the number of disturbances within the preset time period that do not exceed the first preset threshold, but exceeds a third preset threshold.

20. A non-transitory computer-readable medium for storing computer instructions therein, the computer-readable medium comprising a set of instructions which when executed causes a processor to perform a method for managing a protective distribution system, the method comprising:

monitoring a fiber optic information transmission line; detecting, via one or more sensors, a disturbance on the fiber optic information transmission line, wherein the detected disturbance does not exceed a first preset threshold for triggering alerts of a first alert type based on detected disturbances, and wherein the one or more sensors comprise at least one of a vibration sensor, a frequency sensor, an acoustic sensor, and reflective sensor;

determining, responsive to the detection via the one or more sensors, a count for the number of disturbances within a preset time period that do not exceed the first preset threshold;

determining whether the count, for the number of disturbances that do not exceed the first preset threshold, exceeds a second preset threshold for triggering alerts of the first alert type, wherein the second preset threshold corresponds to a preset number of allowable disturbances, not exceeding the first preset threshold and within the preset time period, before one or more alerts of the first alert type are to be triggered; and

triggering an alert of the first alert type responsive to a determination that the count exceeds the second preset threshold.

* * * * *

Exhibit 4

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

(10) **Patent No.:** **US 11,367,342 B2**
(45) **Date of Patent:** **Jun. 21, 2022**

(54) **REAL-TIME PLAYBACK MODIFICATION
FOR ACTIVITY EVENT PLAYBACK**

(71) Applicant: **CyberSecure IPS, LLC**, Upper
Marlboro, MD (US)

(72) Inventors: **Bobby Nakanelua**, Elizabethtown, KY
(US); **Scott Rye**, Prince Frederick, MD
(US); **Stephen Sohn**, Cummings, GA
(US)

(73) Assignee: **CyberSecure IPS, LLC**, Upper
Marlboro, MD (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 122 days.

(21) Appl. No.: **17/003,220**

(22) Filed: **Aug. 26, 2020**

(65) **Prior Publication Data**

US 2021/0067590 A1 Mar. 4, 2021

Related U.S. Application Data

(60) Provisional application No. 62/893,112, filed on Aug.
28, 2019, provisional application No. 62/893,121,
filed on Aug. 28, 2019.

(51) **Int. Cl.**

H04L 29/08 (2006.01)
G08B 29/18 (2006.01)
G01V 8/14 (2006.01)
G08B 21/18 (2006.01)
G06K 9/62 (2022.01)
H04L 67/12 (2022.01)

(52) **U.S. Cl.**

CPC **G08B 29/185** (2013.01); **G01V 8/14**
(2013.01); **G06K 9/6277** (2013.01); **G06K**
9/6288 (2013.01); **G08B 21/182** (2013.01);
H04L 67/12 (2013.01)

(58) **Field of Classification Search**

CPC .. **G08B 29/185**; **G08B 21/182**; **G08B 13/186**;
G08B 29/24; **G01V 8/14**; **G06K 9/6277**;
G06K 9/6288; **G06K 9/6271**; **H04L**
67/12; **G06V 10/82**; **G06V 20/52**

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0254356 A1* 10/2012 Kashiwagi G06Q 30/0201
709/217
2017/0031650 A1* 2/2017 Fraga G10L 25/21

* cited by examiner

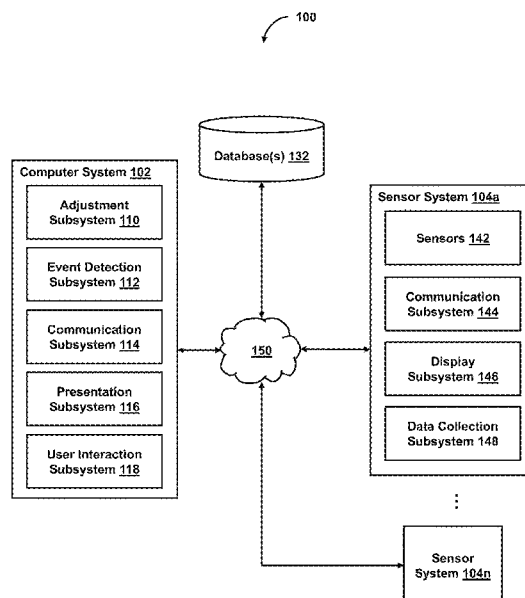
Primary Examiner — Kim T Nguyen

(74) *Attorney, Agent, or Firm* — Perkins Coie LLP

(57) **ABSTRACT**

In certain embodiments, real-time playback modification for activity event playback may be facilitated. In some embodiments, an event list portion and an event playback portion may be provided on a user interface, where the event playback portion is configured to present a playback of events on a location map in accordance with event detection times and a set of event layers for the event playback. While the event playback is occurring, a user selection of events may be obtained via the event list portion of the user interface. While the event playback is occurring, a set of layers for the event playback may be modified based on the user selection. In some embodiments, based on the modification to the set of layers, event layers may be overlaid onto the location map of the event playback portion of the user interface.

20 Claims, 12 Drawing Sheets



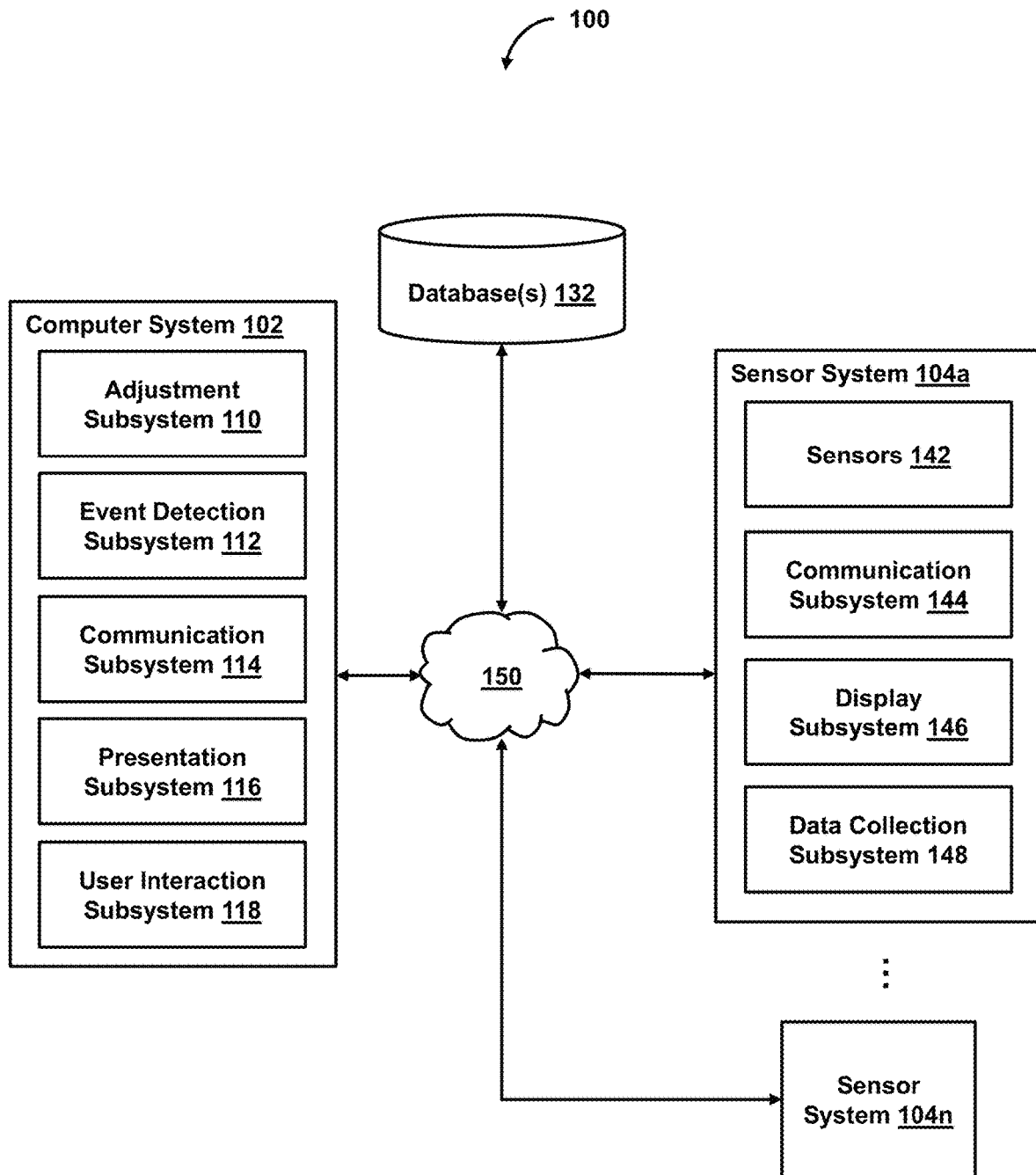


FIG. 1

U.S. Patent

Jun. 21, 2022

Sheet 2 of 12

US 11,367,342 B2

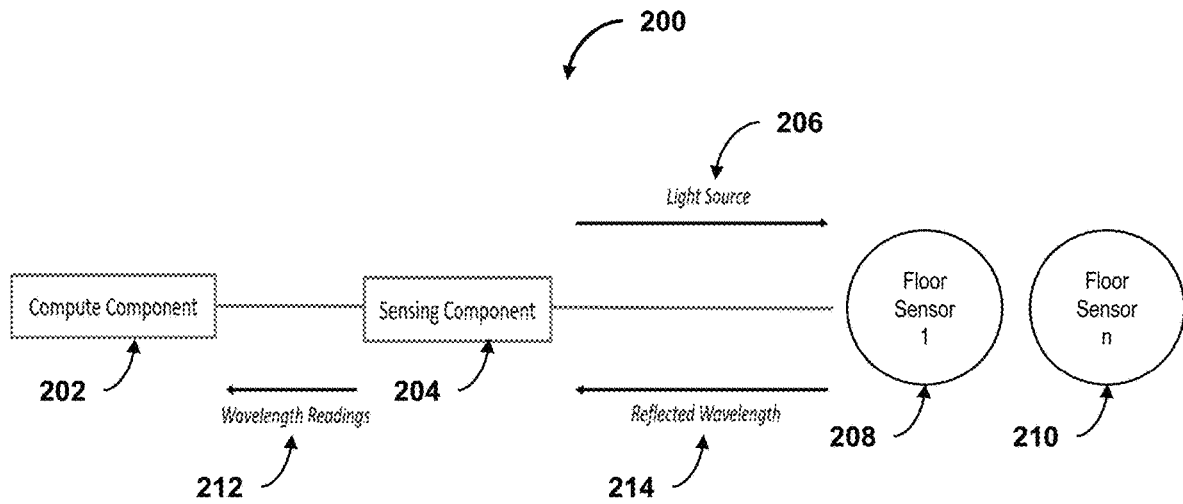


FIG. 2A

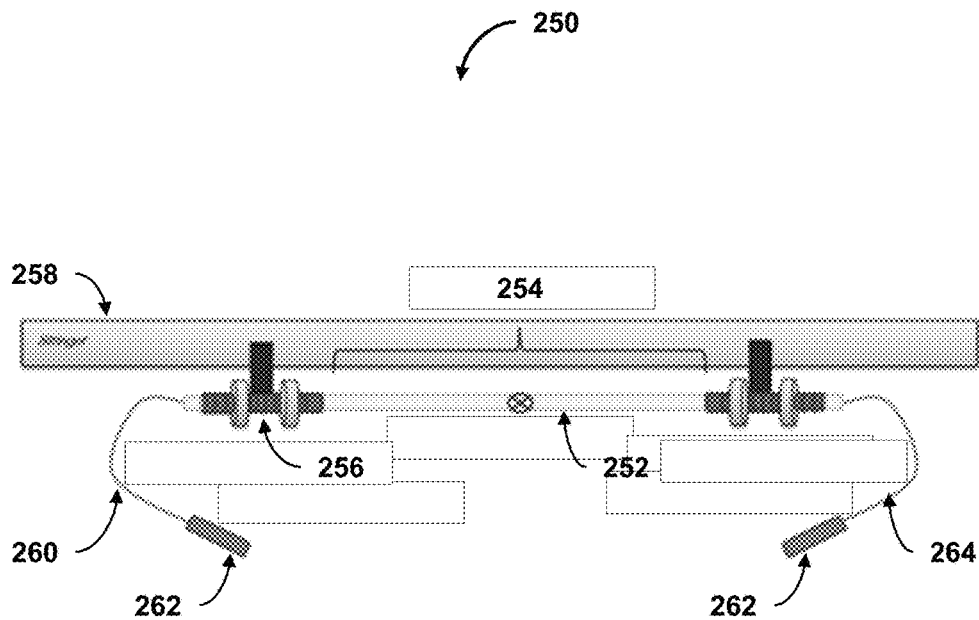


FIG. 2B

U.S. Patent

Jun. 21, 2022

Sheet 3 of 12

US 11,367,342 B2

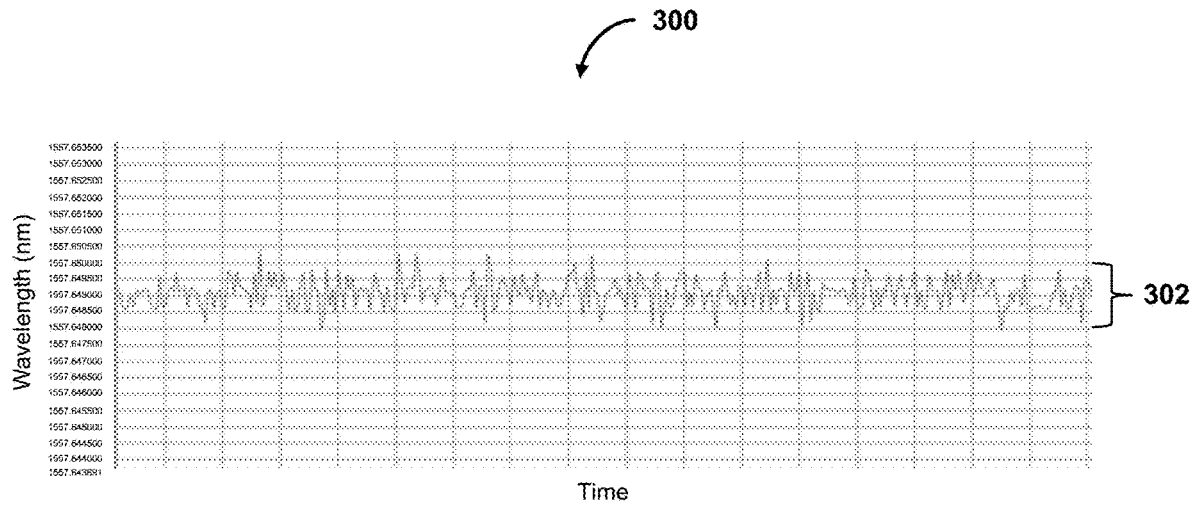


FIG. 3A

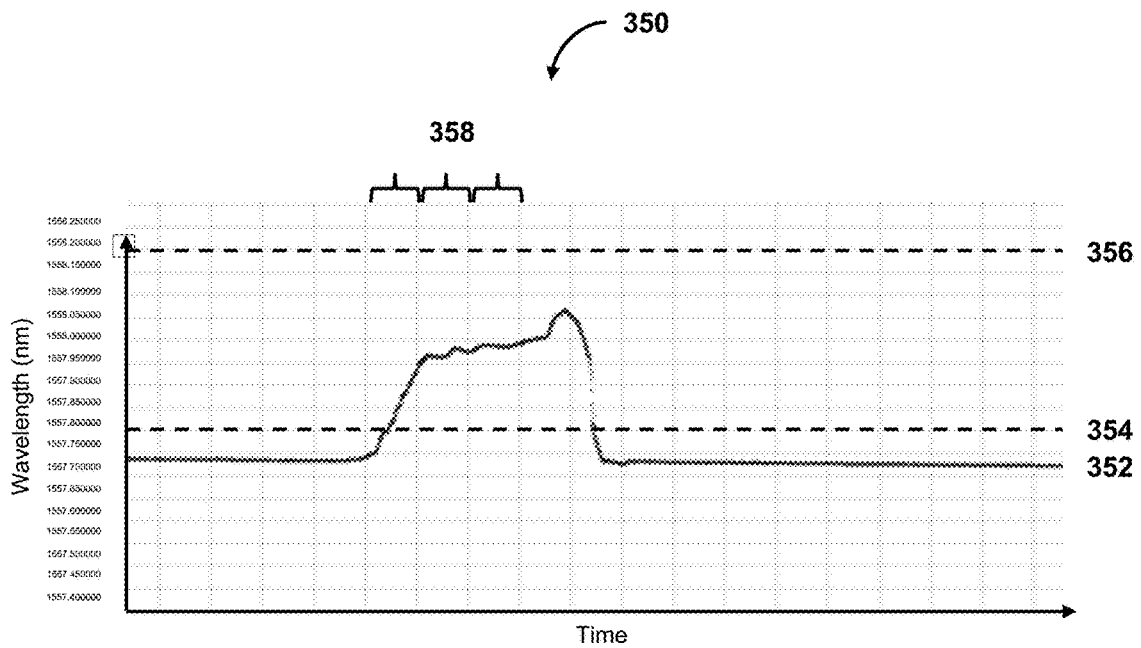


FIG. 3B

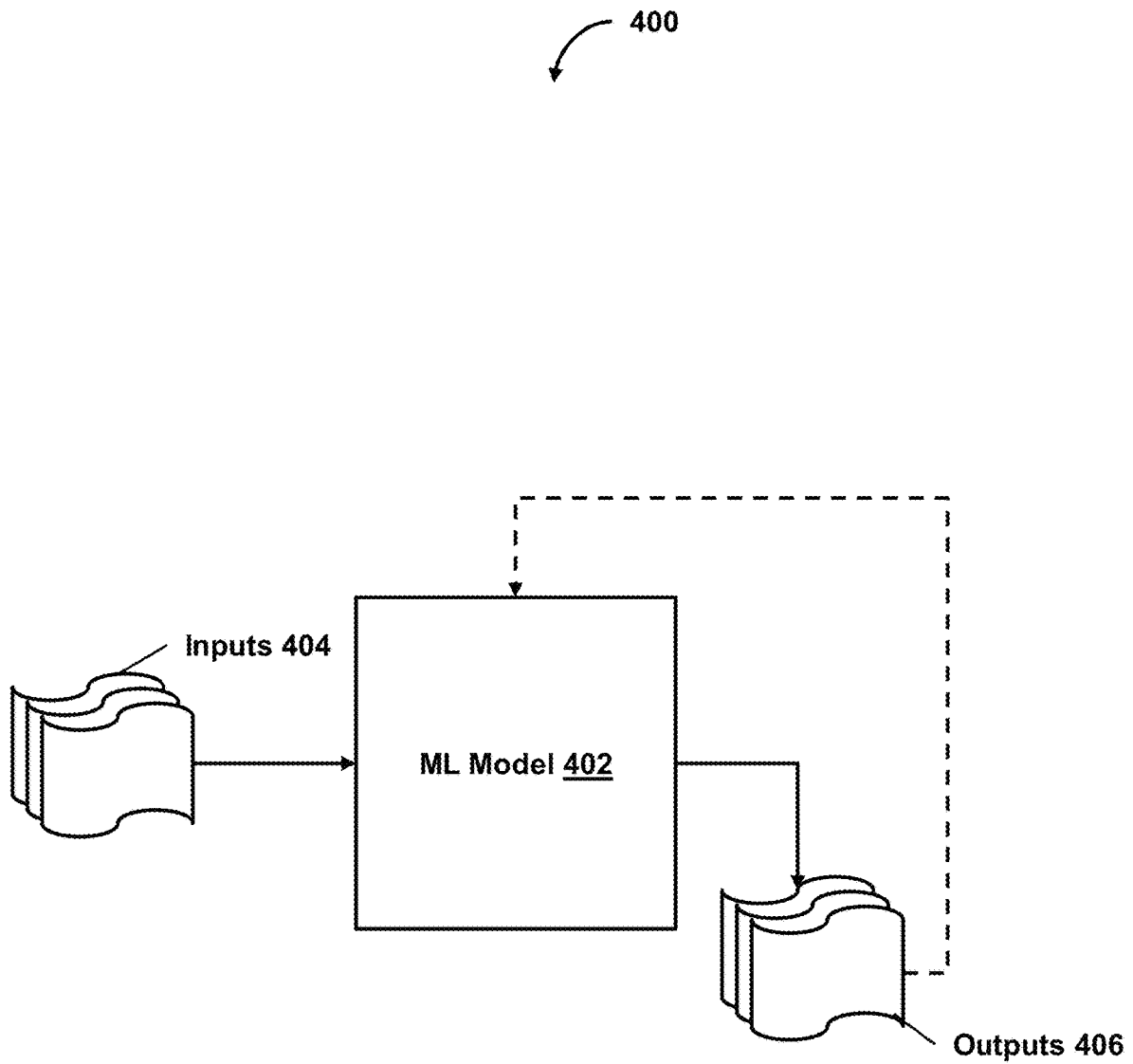


FIG. 4

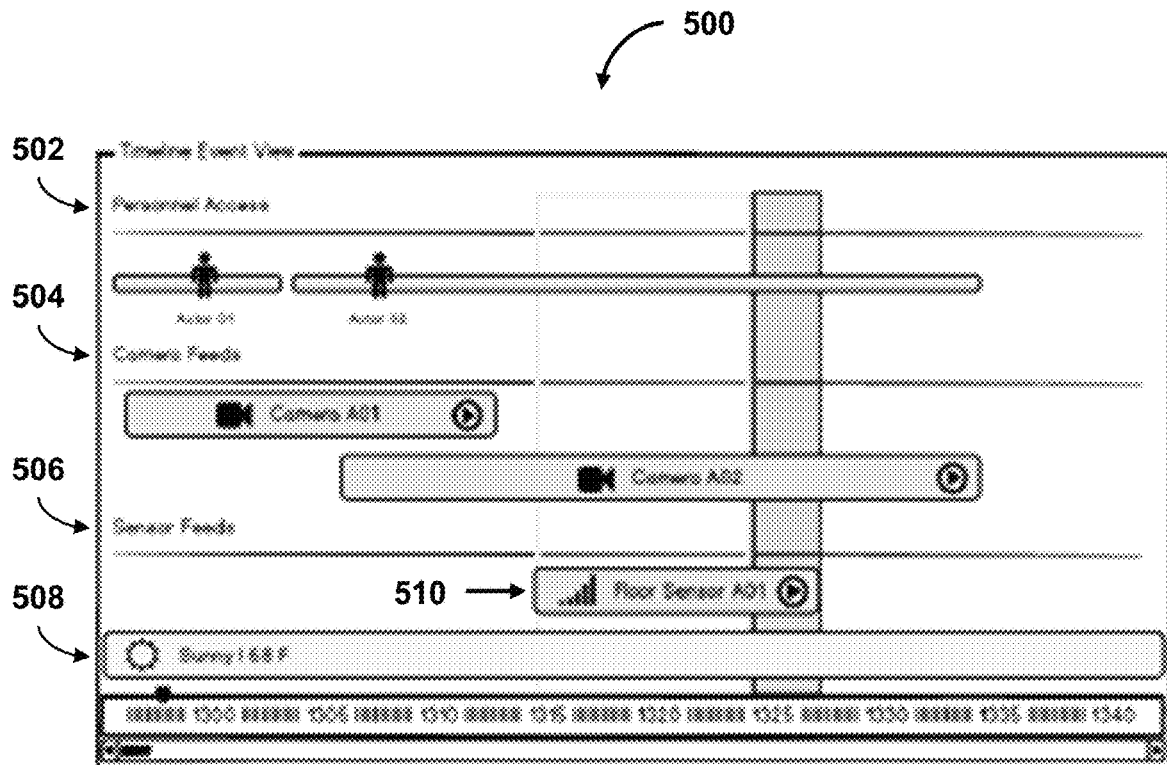


FIG. 5A

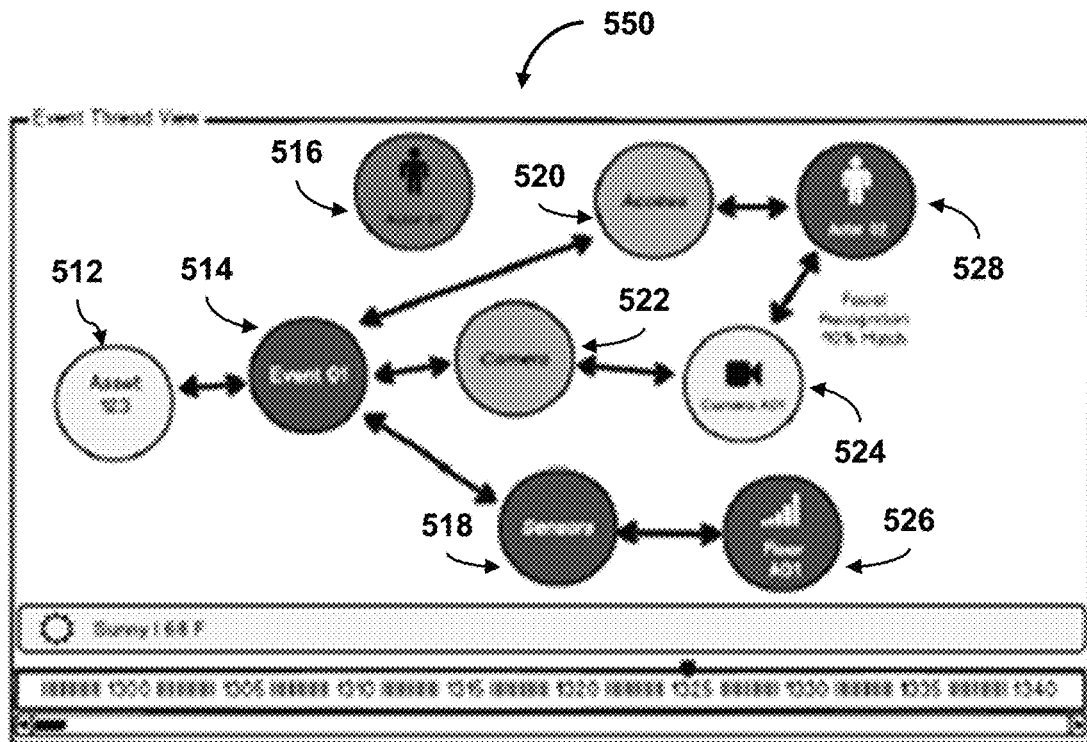


FIG. 5B

U.S. Patent

Jun. 21, 2022

Sheet 6 of 12

US 11,367,342 B2

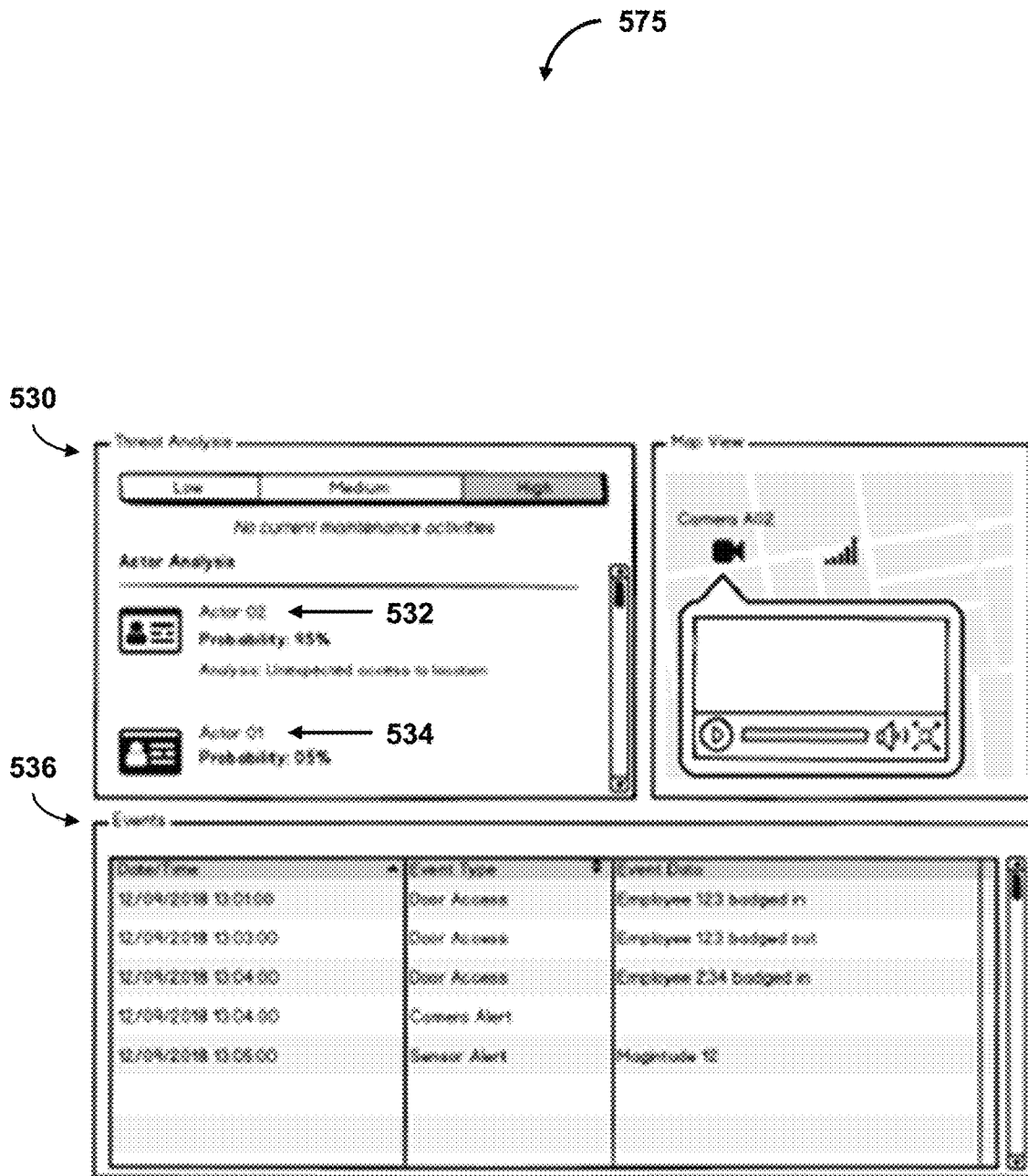


FIG. 5C

U.S. Patent

Jun. 21, 2022

Sheet 7 of 12

US 11,367,342 B2

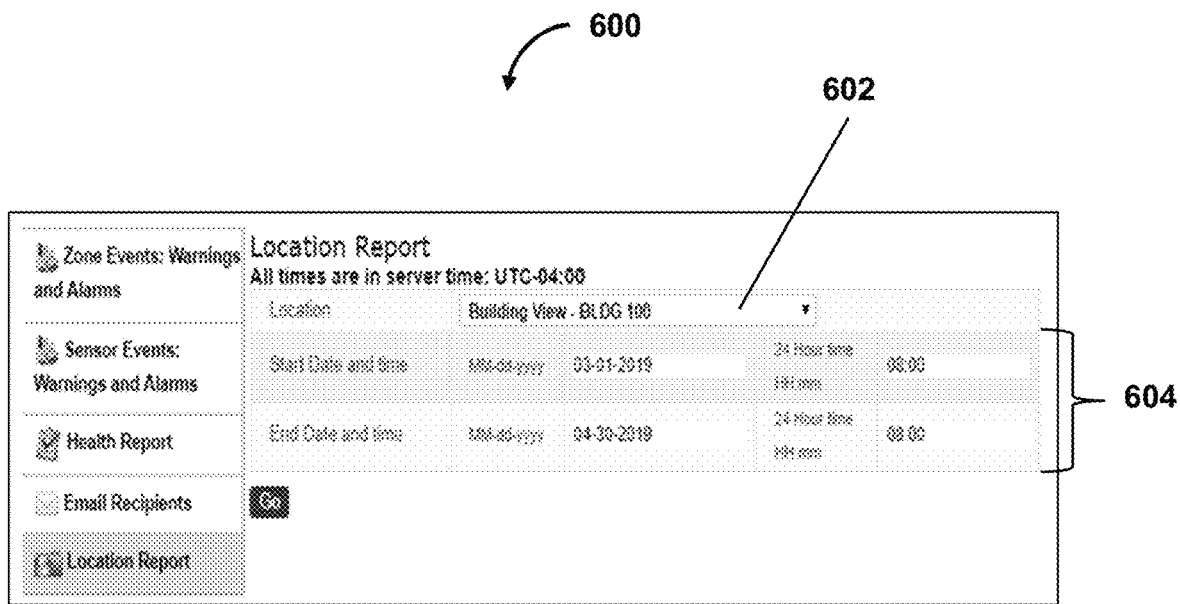


FIG. 6A

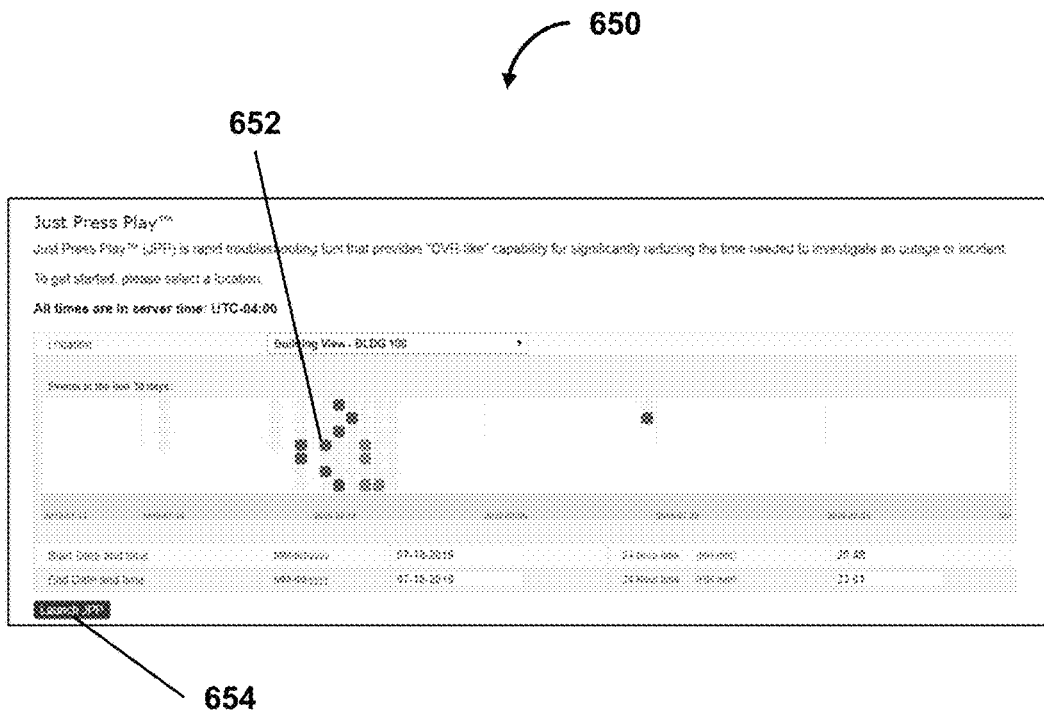


FIG. 6B

U.S. Patent

Jun. 21, 2022

Sheet 8 of 12

US 11,367,342 B2

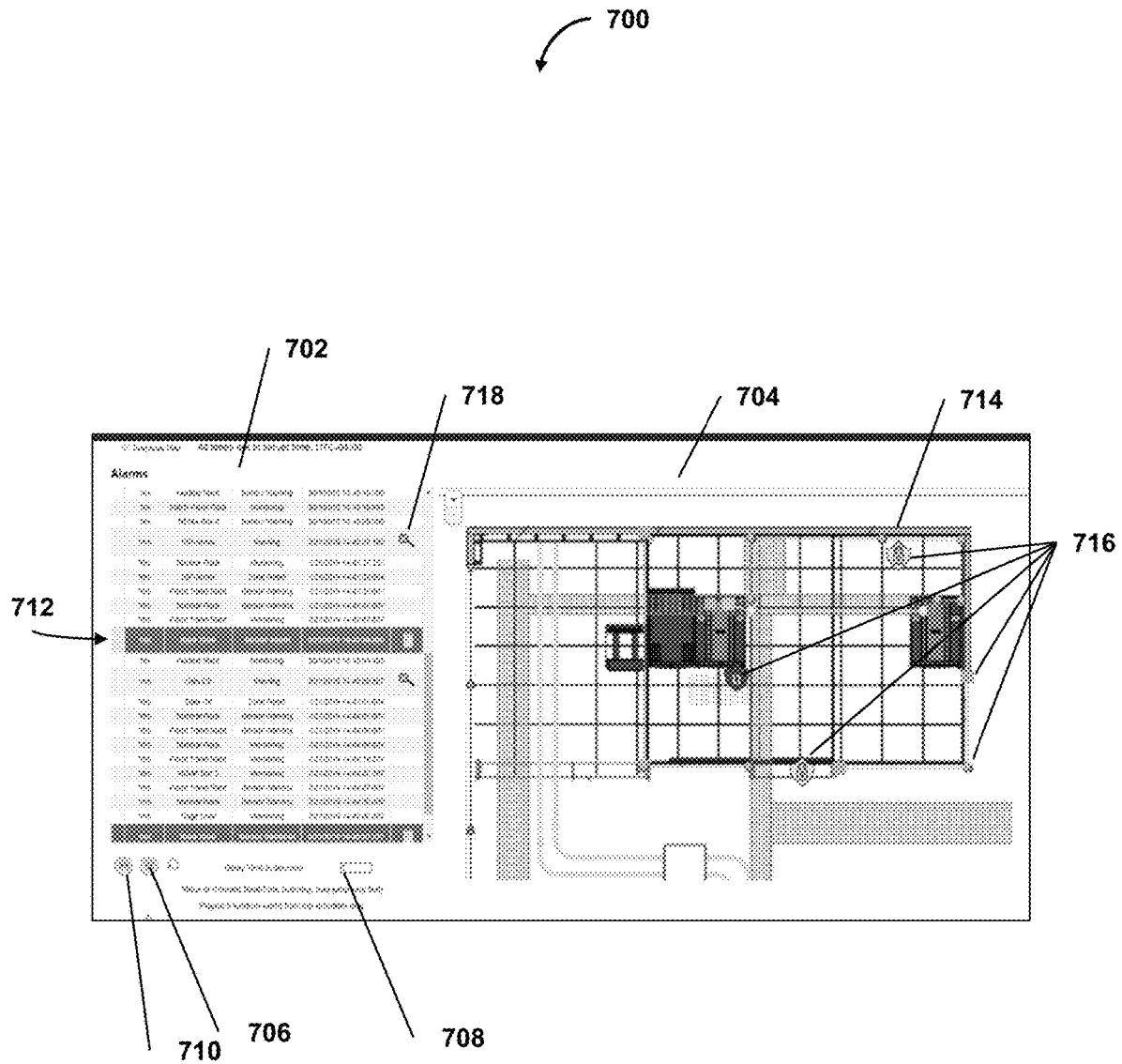


FIG. 7

U.S. Patent

Jun. 21, 2022

Sheet 9 of 12

US 11,367,342 B2

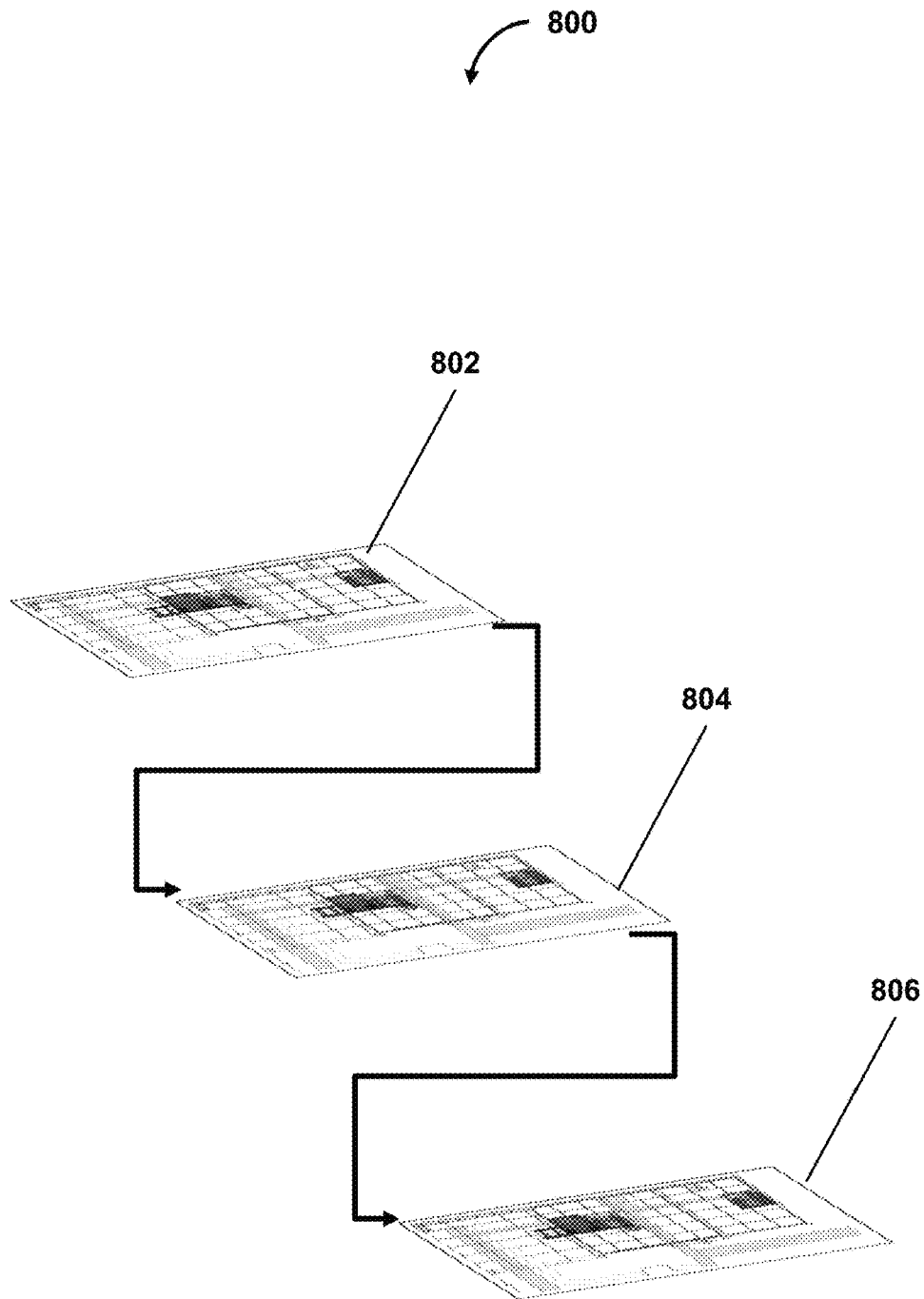


FIG. 8

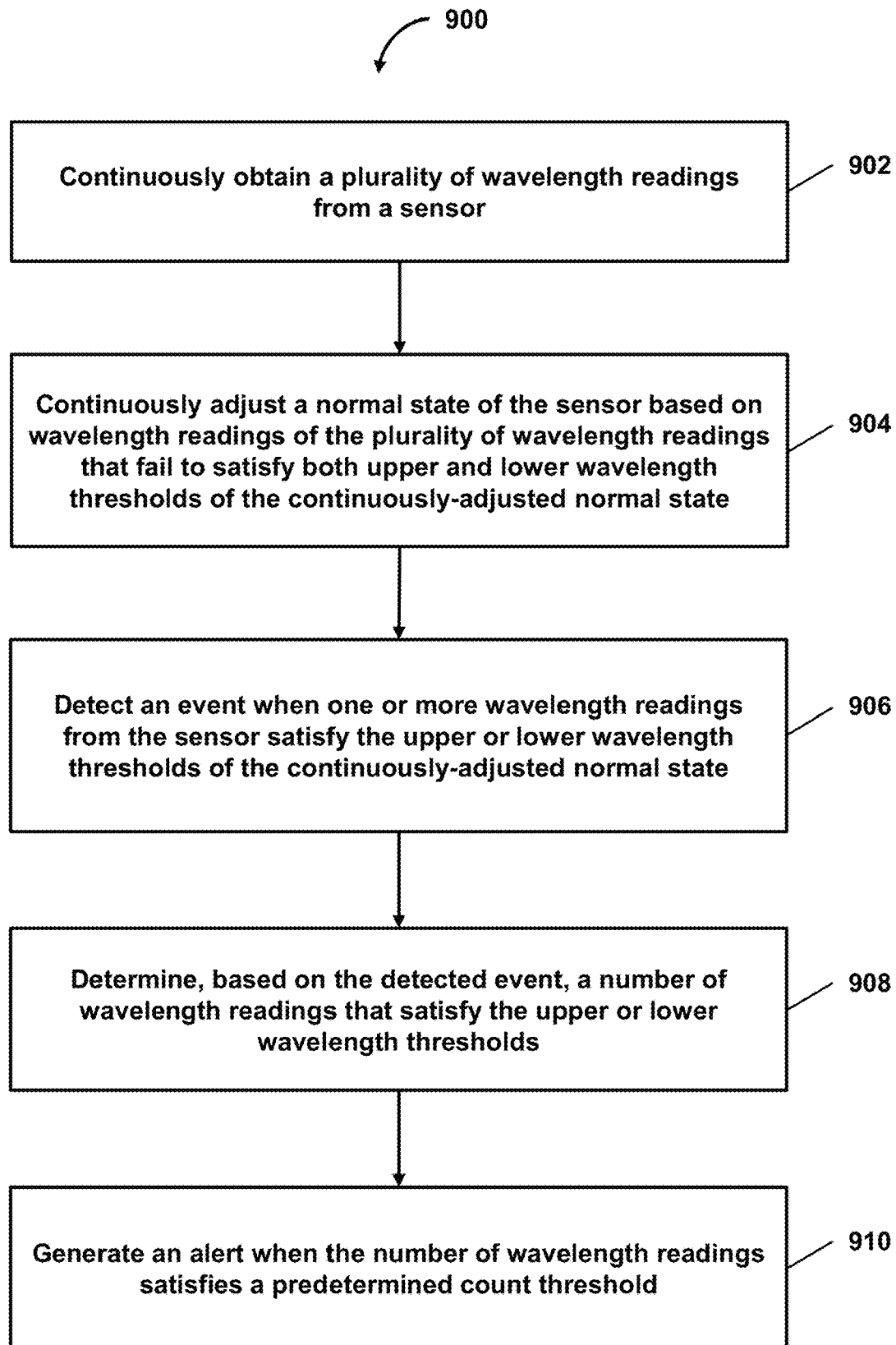


FIG. 9

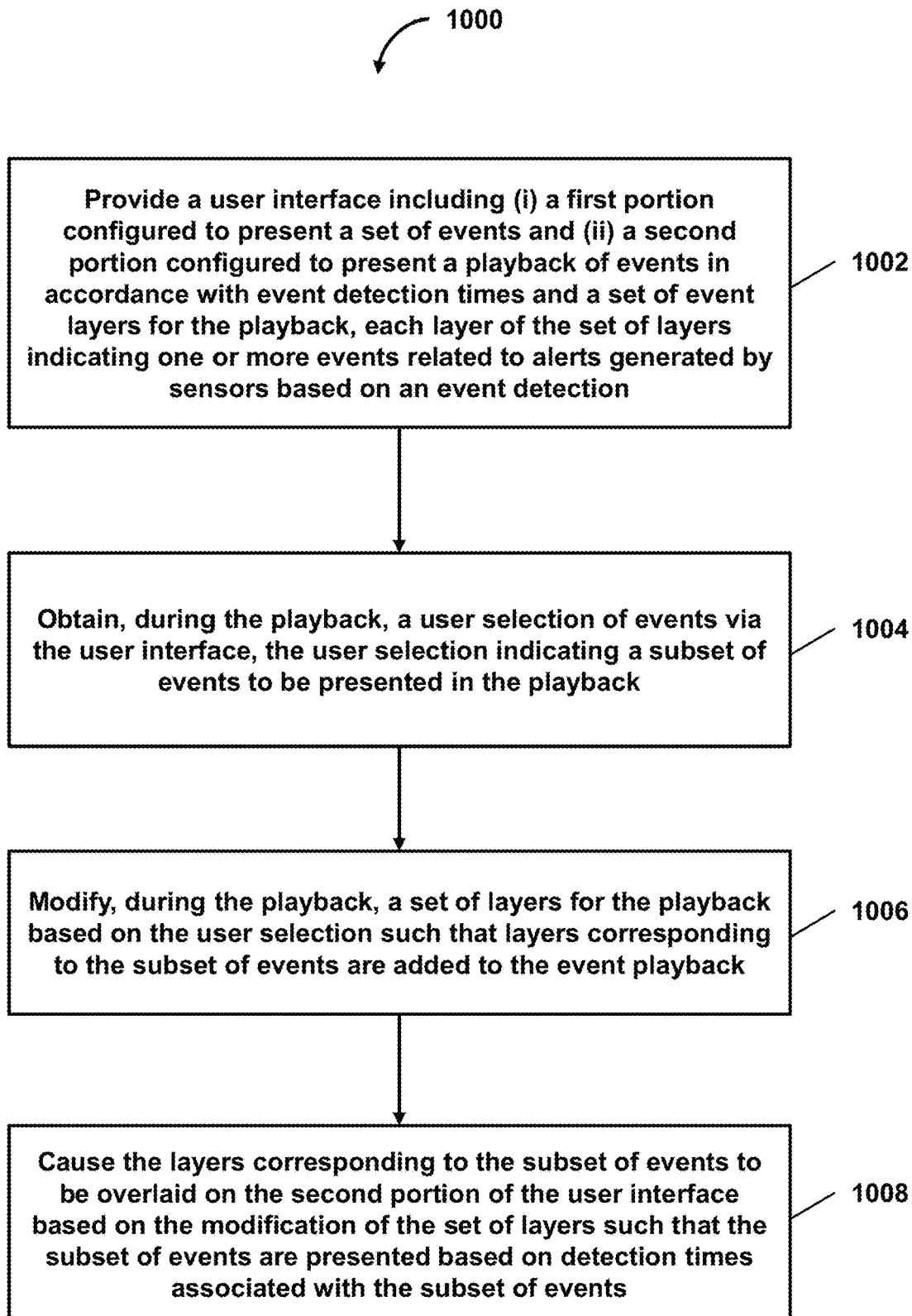


FIG. 10

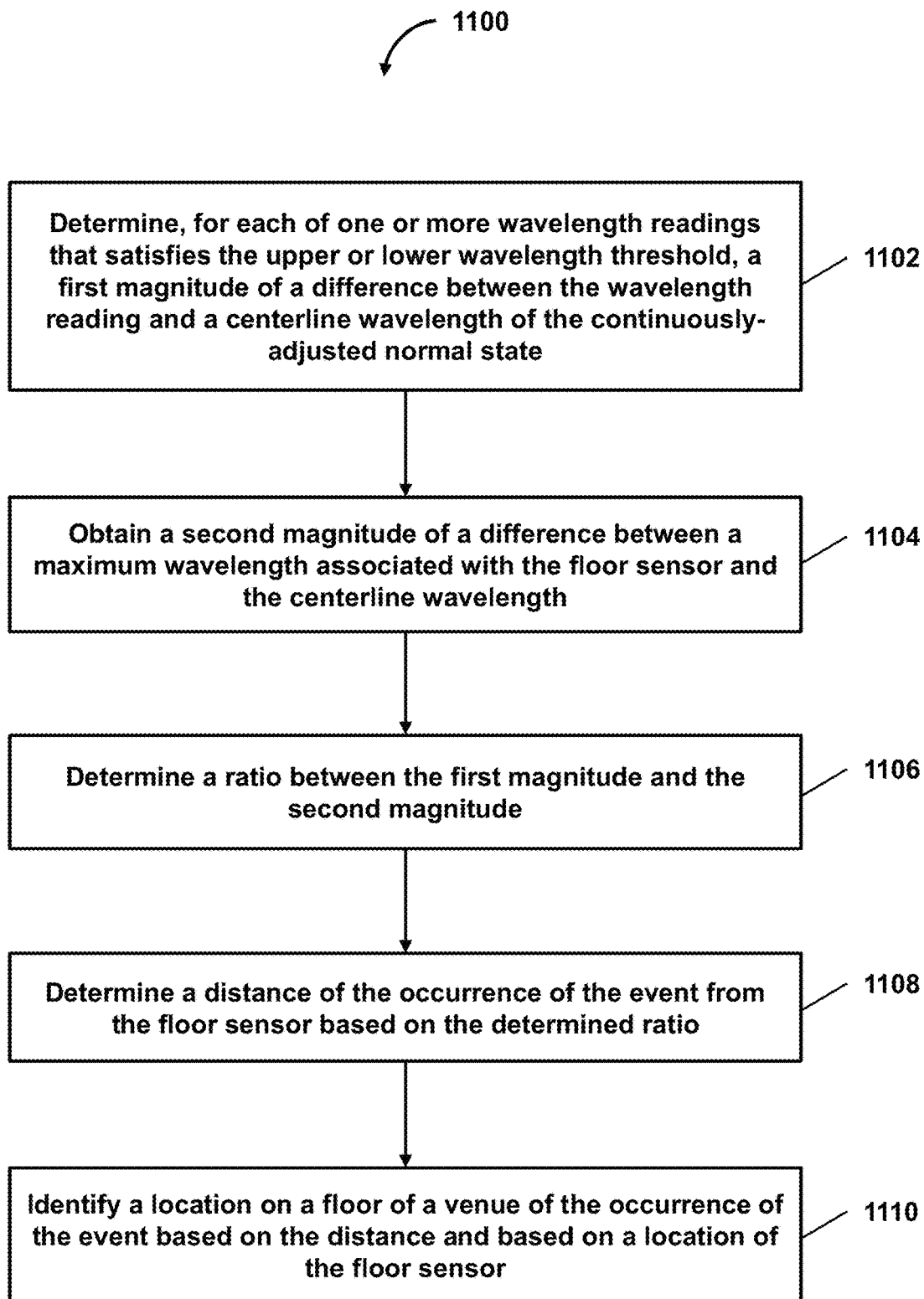


FIG. 11

US 11,367,342 B2

1

**REAL-TIME PLAYBACK MODIFICATION
FOR ACTIVITY EVENT PLAYBACK**

INCORPORATED BY REFERENCE

This application claims the benefit of U.S. Provisional Application No. 62/893,121, entitled "Method and System for Generating Sensor Alerts Based On Continuous Adjustment of a Normal State of a Sensor," filed Aug. 28, 2019, and U.S. Provisional Application No. 62/893,112, entitled "Real-Time Playback Modification for Activity Event Playback," filed Aug. 28, 2019, each of which is hereby incorporated by reference herein in its entirety.

FIELD OF THE INVENTION

The invention relates to facilitating real-time playback modification for activity event playback.

SUMMARY OF THE INVENTION

Aspects of the invention relate to methods, apparatuses, and/or systems for reducing false positive floor sensor alerts based on continuous adjustment of a normal state of a floor sensor and for facilitating real-time playback modification for activity event playback.

One aspect of the disclosure relates to a system and/or method for reducing false positive floor sensor alerts based on continuous adjustment of a normal state of a floor sensor. In some embodiments, the system may continuously obtain a plurality of wavelength readings from a sensor and continuously adjust a normal state of the sensor based on the wavelength readings. For example, the system may adjust the normal state based on certain wavelength readings that fail to satisfy both upper and lower wavelength thresholds of the continuously adjusted normal state. In some embodiments, the system may detect an event when one or more wavelength readings from the sensor satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state. The system may determine, based on the detected event, a number of wavelength readings that satisfy the upper or lower wavelength thresholds. When the number of wavelength readings (e.g., that satisfy the upper or lower wavelength thresholds) reaches a predetermined count threshold, the system may generate an alert (e.g., a suspicious activity alert).

Another aspect of the disclosure relates to a system and/or method for facilitating real-time playback modification for activity event playback. In some embodiments, the system may provide a user interface including a first portion and a second portion. For example, the first portion may be configured to present a set of events and the second portion may be configured to present a playback of events. For example, the playback of events may be presented in accordance with event detection times and a set of event layers for the playback. Each layer of the set of layers may indicate one or more events related to alerts generated by sensors based on an event detection. In some embodiments, during the playback, the system may obtain a user selection of events via the user interface. For example, the user selection may indicate a subset of events to be presented in the playback. During playback, the system may modify a set of layers for the playback based on the user selection such that layers corresponding to the subset of events are added to the event playback. In some embodiments, the computer system may cause the layers corresponding to the subset of events to be overlaid on the second portion of the user interface. For

2

example, the layers may be overlaid on the second portion based on the modification of the set of layers. In some embodiments, the subset of events may be presented based on detection times associated with the subset of events.

Various other aspects, features, and advantages of the invention will be apparent through the detailed description of the invention and the drawings attached hereto. It is also to be understood that both the foregoing general description and the following detailed description are examples and not restrictive of the scope of the invention. As used in the specification and in the claims, the singular forms of "a," "an," and "the" include plural referents unless the context clearly dictates otherwise. In addition, as used in the specification and the claims, the term "or" means "and/or" unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a system for facilitating the generation of a sensor alert and for facilitating real-time playback modification for suspicious activity event playback, in accordance with one or more embodiments.

FIGS. 2A and 2B show one or more sensor systems, in accordance with one or more embodiments.

FIGS. 3A and 3B show wavelength readings from sensors, in accordance with one or more embodiments.

FIG. 4 shows a machine learning model configured to facilitate generation of a sensor alert, in accordance with one or more embodiments.

FIGS. 5A, 5B, and 5C show user interfaces for monitoring multiple sources of information, in accordance with one or more embodiments.

FIGS. 6A and 6B show user interfaces for user requests, in accordance with one or more embodiments.

FIG. 7 shows a user interface for playback of events, in accordance with one or more embodiments.

FIG. 8 shows a plurality of layers for playback of events, in accordance with one or more embodiments.

FIG. 9 shows a flowchart of a method for generating a sensor alert based on continuous adjustment of a normal state of a sensor, in accordance with one or more embodiments.

FIG. 10 shows a flowchart of a method for facilitating real-time playback modification for suspicious activity event playback, in accordance with one or more embodiments.

FIG. 11 shows a flowchart of a method for facilitating identification of a location of an occurrence of an event, in accordance with one or more embodiments.

DETAILED DESCRIPTION OF THE
INVENTION

In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the embodiments of the invention. It will be appreciated, however, by those having skill in the art that the embodiments of the invention may be practiced without these specific details or with an equivalent arrangement. In other cases, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the embodiments of the invention.

FIG. 1 shows a system 100 for facilitating the generation of a sensor alert based on continuous adjustment of a normal state of a sensor and for facilitating real-time playback modification for activity event playback, in accordance with one or more embodiments.

US 11,367,342 B2

3

One aspect of the disclosure relates to a system and/or method for reducing false positive floor sensor alerts based on continuous adjustment of a normal state of a floor sensor. In some embodiments, the system **100** may continuously obtain a plurality of wavelength readings from a sensor and continuously adjust a normal state of the sensor based on the wavelength readings. For example, the system **100** may adjust the normal state based on certain wavelength readings that fail to satisfy both upper and lower wavelength thresholds of the continuously adjusted normal state. While those wavelengths readings that fall within the upper and lower thresholds are used to adjust the normal state, wavelength readings that satisfy the upper or lower wavelength thresholds may be used to detect an event. In other words, the system **100** may detect an event when one or more wavelength readings from the sensor satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state. The system **100** may determine, based on the detected event, a number of wavelength readings that satisfy the upper or lower wavelength thresholds. When the number of wavelength readings (e.g., that satisfy the upper or lower wavelength thresholds) reaches a predetermined count threshold, the system **100** may generate an alert.

Another aspect of the disclosure relates to a system and/or method for facilitating real-time playback modification for activity event playback. In some embodiments, the system **100** may provide a user interface including a first portion and a second portion. For example, the first portion may present a set of events and the second portion may present a playback of events. For example, the playback of events may be presented according to event detection times and a set of event layers for the playback. Each layer of the set of layers may indicate one or more events related to alerts generated by sensors (e.g., based on an event detection). In some embodiments, during the playback, the system **100** may obtain a user selection of events via the user interface. For example, the user selection may indicate a subset of events to be presented in the playback. In some embodiments, the user selection may additionally indicate another subset of events that is not to be presented in the playback. During playback, the system **100** may modify a set of layers for the playback based on the user selection such that layers corresponding to the subset of events are added to the event playback. In some embodiments, layers corresponding to the other subset of events (i.e., which is not to be presented in the playback) may be removed from the event playback. In some embodiments, the system **100** may cause the added layers corresponding to the subset of events to be overlaid on the second portion of the user interface. For example, the layers may be overlaid on the second portion based on the modification of the set of layers, such that the subset of events is presented based on detection times associated with the subset of events.

These methods may be used individually or in conjunction with each other and with any other methods for facilitating event detection and playback. For example, in some embodiments, system **100** may reduce false positive floor sensor alerts based on continuous adjustment of a normal state of a floor sensor and/or facilitate real-time playback modification for activity event playback. For example, as system **100** continuously adjusts the normal state of a floor sensor, the floor sensor becomes more accurate, i.e., less likely to generate a false positive alert. Reducing false positive alerts may cause system **100** to detect fewer false positive events, thereby reducing a quantity of activity events that must be listed for a user during activity event playback. The user modification of playback of activity

4

events in real-time may be performed more quickly and efficiently due to the lack of false positive events listed on the display for selection. In another example, event playback may provide context for and additional information about detected events. For example, event playback may indicate the circumstances surrounding a sensor alert in response to a detected event. Other examples may likewise use the methods described herein in conjunction with each other or with any other methods for improving event detection and playback.

As shown in FIG. 1, system **100** may include computer system **102**, sensor system **104a** (or sensor systems **104a-104n**), database **132**, or other components. Computer system **102** may include adjustment subsystem **110**, event detection subsystem **112**, communication subsystem **114**, presentation subsystem **116**, user interaction subsystem **118**, or other components. Sensor system **104a** may include sensors **142**, communication subsystem **144**, display subsystem **146**, data collection subsystem **148**, or other components. In some embodiments, computer system **102** may include any type of mobile terminal, fixed terminal, or other device. By way of example, computer system **102** may include a desktop computer, a notebook computer, a tablet computer, a smart-phone, a wearable device, a device on the cloud, or other device. It should be noted that, while one or more operations are described herein as being performed by particular components of computer system **102**, those operations may, in some embodiments, be performed by other components of computer system **102** or other components of system **100**. As an example, while one or more operations are described herein as being performed by components of computer system **102**, those operations may, in some embodiments, be performed by components of sensor system **104a** or other components of system **100** and while one or more operations are described herein as being performed by components of sensor system **104a**, those operations may, in some embodiments, be performed by components of computer system **102** or other components of system **100**.

Generation of a Sensor Alert Based on Continuous Adjustment of a Normal State of a Sensor

In some embodiments, system **100** may facilitate generation of a sensor alert based on continuous adjustment of a normal state of a sensor. In some embodiments, system **100** may facilitate a reduction of false positive alerts.

In some embodiments, computer system **102** may continuously obtain a plurality of readings from a sensor **142** (or a plurality of sensors **142**). The sensor **142** may include a camera, a cable tray sensor, temperature, air quality, or moisture sensors, or, for example, an optical sensor (e.g., a Fiber Bragg Grating (FBG) sensor, silicon microsphere sensor, or laser cavity sensor). Such an optical sensor may be distributed on or within a floor of a venue or infrastructure. Examples of an optical sensor may include a photoelectric sensor that uses a light transmitter and a photoelectric receiver (e.g., see FIG. 2A). The sensor **142** may be used to determine whether an object or a person is in proximity to the sensor **142**. Although the optical sensor is provided as an example, it should be understood that any sensor that is capable of detecting an object or a person in proximity of the sensor may be used, including, for example, ultrasonic, capacitive, inductive, or magnetic sensors. Further, although the sensor **142** is described as being distributed on or within a floor of a venue or infrastructure, it should be understood that the placement of sensor **142** is not limited thereto and that the sensors **142** can be placed in any other location within a venue or an infrastructure.

US 11,367,342 B2

5

FIG. 2A shows a sensor system 200, in accordance with one or more embodiments. FIG. 2A includes floor sensor 208 and floor sensor 210 (e.g., representing floor sensors 1-n) and a sensing component 204. For example, each floor sensor 1-n may be associated with a corresponding sensing component 204 or a plurality of floor sensors may be associated with one or more sensing components 204. Although only one sensing component 204 is illustrated in FIG. 2A, it should be understood that sensor system 200 may include a plurality of sensing components 204. In some embodiments, sensing component 204 may be a light source and a receiver of light reflected from floor sensors 208/210 and floor sensors 208/210 may be reflectors (e.g., wavelength-specific reflectors). Sensors 142 illustrated in FIG. 1 may include or correspond to floor sensors 208/210, sensing component 204, and/or compute component 202 illustrated in FIG. 2A. In some embodiments, computer system 102 illustrated in FIG. 1 may include compute component 202 illustrated in FIG. 2A. In some embodiments, floor sensors 208-210 may be distributed throughout a floor system in an infrastructure. For example, floor sensors 208-210 may be integrated into an elevated floor system or into a mat that rests directly on a non-elevated floor system.

In some embodiments, computer system 102 (e.g., via data collection subsystem 148 and communication subsystem 114) may continuously obtain a plurality of wavelength readings from one or more sensors 142. As shown in FIG. 2A, sensing component 204 may continuously detect wavelengths of reflected light (e.g., reflected wavelength of light 214). The wavelength of light 214 reflected by the floor sensors 208/210 may vary based on people or objects proximate to the floor sensors 208-210. In other words, the sensing component 204 may detect a particular wavelength of light 214 (which may or may not be different from the wavelength of the light emitted (e.g., light 206 emitted by a light source of the sensing component 204) by the sensing component 204 and reflected by the floor sensors 208/210 and the wavelength of light 214 reflected by the floor sensors 208/210 may vary depending on people or objects proximate to the floor sensors 208-210. The sensing component 204 may detect unique wavelength readings 212 of the reflected light 214 and may send the unique wavelength readings 212 to compute component 202. The sensing component 204 may be an optical controller or other sensing component. The sensing component 204 may include a light emitter and a light receiver. The compute component 202 may process the unique wavelength readings 212.

FIG. 2B shows a sensor system 250, in accordance with one or more embodiments. In some embodiments, sensor system 250 may comprise an optical sensor 252 (e.g., Fiber Bragg Grating (FBG) sensor) that may be attached to a floor 258 of an infrastructure. In some embodiments, the optical sensor 252 may detect multi-directional strain induction or vibration in floor 258. For example, the wavelength and amplitude readings measured by optical sensor 252 may change with vibration and strain. In some embodiments, sensor system 250 may include a section (e.g., ten-inch section 254) of optical sensor 252 for detecting multi-directional strain or vibrations. In some embodiments, optical sensor 252 may detect horizontal, vertical, or vibrational strain. In some embodiments, optical sensor 252 may be mounted (e.g., using mount 256) to floor 258. For example, mount 256 and the orientation of optical sensor 252 may be changed to measure the effect of strain or vibrations at various points. For example, the orientation of optical sensor 252 may affect the sensitivity of optical sensor 252. As raised floor systems are typically structured to be strong and

6

sturdy, it is important that optical sensor 252 is mounted and oriented correctly. This ensures that optical sensor 252 is able to detect strain or vibrations caused by personnel walking across the floor or other events. In some embodiments, other components of sensor system 250 include an armored lead-in 260, connectors 262 (e.g., LC/APC connectors), and an armored lead-out 264. In some embodiments, armored lead-in 260 and armored lead-out 264 may protect the sensor from damage. For example, floor tiles in raised floor environments may be heavy or personnel working in the space may accidentally snag a cable. In these examples, armored lead-in 260 and armored lead-out 264 may protect the sensor from breaking. In some embodiments, optical sensor 252 may correspond to sensors 142, as shown in FIG. 1.

FIG. 3A illustrates a plurality of wavelength readings 300 from a sensor, in accordance with one or more embodiments. In some embodiments, wavelength readings 300 may be measured by an optical controller (e.g., sensing component 204 in FIG. 2A) working in conjunction with the sensor (e.g., optical sensor 252, as shown in FIG. 2B, and/or sensors 208/210, as shown in FIG. 2A). For example, the optical controller (e.g., sensing component 204 in FIG. 2A) may send a laser down a fiber to an FBG sensor (e.g., optical sensor 252 and/or sensors 208/210). The FBG sensor may reflect laser light back to the optical controller. The optical controller may then read the reflected light and send the wavelength and amplitude readings to computer system 102 and/or compute component 202 for processing. FIG. 3A illustrates wavelength readings in an initial state (e.g., with no applied strain or vibration), whereas FIG. 3B illustrates wavelength readings when a strain or vibration is detected. In some embodiments, wavelength readings 300 may be received from a sensor 142 (as shown in FIG. 1), sensor system 200 (as shown in FIG. 2A), or sensor system 250 (as shown in FIG. 2B). In some embodiments, wavelength readings 300 may correspond to wavelength readings 212, as shown in FIG. 2A. Computer system 102 (e.g., event detection subsystem 112) may determine a normal state of the sensor 142 based on the obtained plurality of wavelength readings.

For example, each sensor 142 may be initialized and a plurality of wavelength readings may be obtained (e.g., via data collection subsystem 148 and communication subsystem 144) from each sensor 142. In some embodiments, during the initialization phase, wavelength readings from a sensor 142 may be added to a queue of readings. Computer system 102 may monitor the queue of wavelength readings to determine if the queue is full and may remain in the initialization phase until the queue has filled. In some embodiments, the queue size may be predetermined, set by computer system 102, set by a user, or determined in another way. In some embodiments, computer system 102 may begin event detection once the initialization phase is complete. In some embodiments, once computer system 102 determines that the queue is full, computer system 102 may move from the initialization phase to an event detection phase (e.g., as discussed in detail below). The initialization phase may correspond to a phase in which no strain or vibration is applied to the sensors 142 and the wavelength readings are obtained from such sensors 142 (e.g., via data collection subsystem 148 and communication subsystem 144).

Based on the plurality of wavelength readings received during the initialization phase, adjustment subsystem 110 may determine a normal state including a centerline wavelength, an upper wavelength threshold, and a lower wave-

US 11,367,342 B2

7

length threshold for each sensor 142 in a normal state. In some embodiments, the centerline wavelength may be a specific wavelength to which a sensor has been manufactured. In some embodiments, adjustment subsystem 110 may continuously update the centerline wavelength based on information (e.g., readings) collected from sensors 142, in order to account for changes in sensors 142 over time (e.g., due to fatigue, environmental factors, etc.). As an example, adjustment subsystem 110 may determine a centerline wavelength to be a mean, median, or mode of the plurality of wavelength readings. For example, the centerline wavelength may be an average of the wavelength readings received during the initialization phase.

In some embodiments, the upper and lower wavelength thresholds may be determined based on one or more factors (e.g., the value of the largest wavelength reading, the value of the smallest wavelength reading, any multiplier of the largest wavelength reading or the smallest wavelength reading, a standard deviation (e.g., one standard deviation, two standard deviations, three standard deviations, etc.) associated with the plurality of wavelength readings, or any multiplier of the standard deviation associated with the plurality of wavelength readings). In some embodiments, the wavelength readings may be associated with a time stamp and wavelength readings that are more recent may be associated with a higher weight than wavelength readings that are older. Accordingly, the centerline wavelength and the upper and lower wavelength thresholds may be determined based on the values associated with the plurality of wavelength readings and the weights associated such wavelength readings. In some embodiments, the weights may be dynamic. In other words, the weights associated with each of the plurality of readings may vary with time. As shown in FIG. 3A, a plurality of wavelength readings 302 may represent wavelength readings obtained in an initialization phase and such wavelength readings may be used to determine the normal state of the sensor 142 (e.g., including a centerline wavelength, an upper wavelength threshold, and a lower wavelength threshold for the sensor 142). The measured wavelengths of a sensor 142 may vary based on reflection from cable connections, vibrations, and strain to environmental factors such as temperature.

In some embodiments, after the initialization phase of the sensors 142, computer system 102 may continuously obtain a plurality of wavelength readings from the sensor 142 (e.g., via data collection subsystem 148 and communication subsystem 144). Further, computer system 102 (e.g., adjustment subsystem 110) may continuously adjust a normal state of the sensor 142 based on wavelength readings of the plurality of wavelength readings that fail to satisfy both upper and lower wavelength thresholds of the continuously-adjusted normal state. In other words, the adjustment subsystem 110 may only utilize the wavelength readings that fall between the upper and lower wavelength thresholds in order to adjust the normal state of the sensor 142 (e.g., in order to adjust the centerline wavelength, upper wavelength threshold, and/or lower wavelength threshold). In some embodiments, this may avoid the inclusion of events (e.g., disturbances near sensors 142 that cause the wavelength readings to exceed the upper wavelength threshold or fall below the lower wavelength threshold) in the adjustment of the normal state. For example, in some embodiments, the centerline wavelength may be a dynamic average of the wavelength readings that are continuously obtained and which fall between the upper and lower wavelength thresholds.

It is advantageous to continuously adjust the normal state for various reasons. As an example, the sensitivity of the

8

sensors may deteriorate over time and the normal state may need to be adjusted in order to properly detect an event. As another example, due to external factors (e.g., vibration of an A/C unit), sensors 142 may detect vibrations (e.g., continuous vibrations) and accordingly the plurality of wavelength readings may vary. As another example, environmental factors such as temperature can cause wavelength readings to vary over time. As such, it is advantageous to continuously determine and adjust the normal state of the sensor 142 in order to reduce false positive sensor alerts. Continuously adjusting the normal state of the sensor 142 may include continuously adjusting a centerline wavelength, the upper wavelength threshold, and the lower wavelength threshold associated with the sensor 142.

FIG. 3B illustrates a plurality of wavelength readings 350 from a sensor, in accordance with one or more embodiments. As shown in FIG. 3B, one or more wavelength readings 352 exceed an upper wavelength threshold 354. In some embodiments, upper wavelength threshold 354 (or a lower wavelength threshold) may represent a threshold past which computer system 102 may begin to calculate a number of wavelength readings that satisfy the upper wavelength threshold 354 (e.g., that exceed the upper wavelength threshold 354) or satisfy a lower wavelength threshold (e.g., that falls below the lower wavelength threshold). FIG. 3B also illustrates a maximum wavelength threshold 356 associated with a sensor 142. In some embodiments, each sensor 142 may be associated with corresponding upper and lower wavelength thresholds and maximum and minimum wavelength threshold limits.

In some embodiments, the maximum and minimum wavelength threshold limits of sensors 142 may be limited by manufacturer of the sensors 142 (e.g., the sensors 142 may be built such that they can detect wavelengths within maximum and minimum wavelength threshold limits). The maximum and minimum wavelength threshold limits (e.g., maximum wavelength threshold 356) for sensors 142 may be vary based on the type of sensors, manufacture specifications, or other attributes of sensors 142. In some embodiments, maximum and minimum threshold limits may be determined via calculations. For example, maximum and minimum threshold limits may be determined by stepping on a sensor and measuring the resulting wavelength(s).

In some embodiments, the upper and lower wavelength thresholds may be determined and adjusted based on wavelength measurements, based on the continuous adjustment of the centerline wavelength, or based on other factors. For example, the upper and lower wavelength thresholds may be determined by computer system 102 based on variability of wavelength readings during the initialization phase. For example, computer system 102 may determine upper and lower wavelength thresholds based on maximum and minimum wavelength readings obtained during the initialization phase, during normal use, or during another time period. In some embodiments, upper and lower wavelength thresholds may be set based on such variability. For example, the upper and lower wavelength thresholds may be set such that they are greater than typical wavelength variability to avoid false positives. For example, typical wavelength variability may correspond to wavelength readings that fall within maximum and minimum wavelength readings (e.g., obtained during the initialization phase, during normal use, or during another time period). In some embodiments, upper and lower wavelength thresholds may be adjusted to control sensitivity of sensors 142. For example, in environments having high strain levels or high vibration levels, upper and lower wavelength thresholds may be increased for a specific

US 11,367,342 B2

9

sensor. This may prevent a sensor from triggering false positive alarms due to environmental impact. In some embodiments, the centerline wavelength may also be adjusted based on a plurality of readings obtained from a sensor **142**. For example, the centerline wavelength may be adjusted to control sensitivity of sensors **142**. For example, in environments having high strain levels or high vibration levels, the mean (median or mode) of the plurality of readings may increase for a specific sensor.

In some embodiments, event detection subsystem **112** may detect an event when one or more wavelength readings satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state. In other words, event detection subsystem **112** may detect an event when one or more wavelength readings exceed the upper wavelength threshold or fall below the lower wavelength threshold of the continuously-adjusted normal state. For example, computer system **102** (e.g., event detection subsystem **112**) may analyze wavelength readings **352** in time slices (e.g., time slices **358**). In some embodiments, time slices **358** may have a fixed length (e.g., one second, two seconds, five seconds, etc.). Event detection subsystem **112** may identify a time slice during which one or more wavelength readings **352** cross the upper wavelength threshold **354**. In some embodiments, event detection subsystem **112** may identify each time slice during which wavelength reading **352** remains above upper wavelength threshold **354**. In some embodiments, one or more time slices during which a wavelength reading **352** crosses or is above upper wavelength threshold **354** may correspond to an event. In some embodiments, an event may be detected when one wavelength reading during a single time slice **358** exceeds the upper wavelength threshold **354**, when a plurality of wavelength readings (e.g., a threshold number of a plurality of readings) during a single time slice **358** exceed the upper wavelength threshold **354**, and/or when a plurality of readings (e.g., a threshold number of a plurality of readings) during a plurality of time slices **358** (e.g., during a threshold number of a plurality of consecutive time slices **358**) exceed upper wavelength threshold **354**.

In some embodiments, event detection subsystem **112** may identify each time slice during which one or more wavelength readings **352** are below a lower wavelength threshold. In some embodiments, one or more time slices during which wavelength reading **352** crosses or is below the lower wavelength threshold may correspond to an event. In some embodiments, an event may be detected when one wavelength reading during a single time slice **358** falls below the lower wavelength threshold, when a plurality of wavelength readings (e.g., a threshold number of a plurality of readings) during a single time slice **358** fall below the lower wavelength threshold, and/or when a plurality of readings (e.g., a threshold number of a plurality of readings) during a plurality of time slices **358** (e.g., during a threshold number of a plurality of consecutive time slices **358**) fall below the lower wavelength threshold. In other words, computer system **102** (e.g., event detection subsystem **112**) may identify or detect an event when one or more wavelength readings during a time slice satisfy the upper or lower wavelength threshold.

In some embodiments, when one or more wavelength readings satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state, computer system **102** may send one or more messages to a central server (e.g., an infrastructure monitoring system). For example, a message may include one or more wavelength readings (e.g., wavelength readings that satisfy the upper or lower wave-

10

length thresholds of the continuously-adjusted normal state) for processing. In some embodiments, a message may include all wavelength readings within a certain time period. For example, a message may include all consecutive wavelength readings that satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state. The central server may process the wavelength readings included in the message in order to determine information about the detected event. In another example, a message may include an alert indicating a detected event. For example, the central server may have access to other systems and data which may provide context to the detected event or the central server may include systems for playback of a detected event indicated by a message. Although a central server is noted above, it should be understood that the computer system **102** may perform all functions of a central server.

In some embodiments, several comparisons may be performed (e.g., by computer system **102**, a central server, or another processor) on received wavelength readings that satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state in order to determine information about the detected event (e.g., disturbance or activity). For example, computer system **102** (e.g., event detection subsystem **112**) may compare current wavelength readings to the upper wavelength threshold and lower wavelength threshold to determine if the wavelength readings are rising or falling. This may allow computer system **102** to determine wave direction. In some embodiments, event detection subsystem **112** may determine, for each of the one or more wavelength readings that satisfies the upper wavelength threshold, a first magnitude of a difference between the wavelength reading and a centerline wavelength of the continuously-adjusted normal state. Event detection subsystem **112** may also obtain or determine a second magnitude of a difference between a maximum threshold limit or minimum threshold limit associated with the sensor **142** and the centerline wavelength. For example, if the wave is determined to be rising, the first magnitude (e.g., a difference between the wavelength reading and the centerline wavelength) may be compared to the second magnitude (e.g., a difference between a maximum threshold limit (e.g., maximum wavelength threshold **356**) and the centerline wavelength). If the wave is determined to be falling, the first magnitude (e.g., a difference between the wavelength reading and the centerline wavelength) may be compared to the second magnitude (e.g., a difference between a minimum threshold limit and the centerline wavelength). Each sensor **142** may have a maximum and a minimum threshold limit associated with the sensor, as discussed above.

In some embodiments, event detection subsystem **112** may determine a ratio between the first magnitude and the second magnitude. The ratio may indicate a distance of the occurrence of the event from the sensor **142**. In other words, a distance of the occurrence of the event from the sensor **142** may be determined based on the determined ratio. In some embodiments, the ratio between the first magnitude and the second magnitude may be inversely proportional to the distance of the occurrence of the event from the sensor. In other words, a smaller ratio would indicate a larger distance of the occurrence of the event from the sensor **142** and a larger ratio would indicate a smaller distance of the occurrence of the event from the sensor **142**. In some embodiments, a location of the occurrence of the event may be identified based on the determined distance (e.g., the determined distance of the occurrence of the event from the sensor **142**) and based on a location of the sensor **142**. The location of the sensor **142** may be known and may be stored

US 11,367,342 B2

11

in the database **132**. The database **132** may also store wavelength readings and the continuously adjust the normal state. The wavelength readings may also be stored in a buffer of computer system **102** for a predetermined amount of time (e.g., to be used in calculations at a later time). The database **132** may store any data described in this disclosure.

In some embodiments, a maximum of one event per second may be detected. In some embodiments, each event may represent all associated calculations that are generated during the event (e.g., first magnitude, second magnitude, ratio, distance, etc.). In some embodiments, an event may correspond to an interaction (e.g., of a person or object) in close proximity to a floor sensor (e.g., sensor system **200**, as shown in FIG. **2A**, or sensor system **250**, as shown in FIG. **2B**). In some embodiments, an event may be detected by computer system **102** (e.g., event detection subsystem **112**) when one or more wavelength readings from the sensor satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state (e.g., as described above). In other words, an event may be detected when one or more wavelength readings exceed an upper wavelength threshold (e.g., upper wavelength threshold **354**) or fall below a lower wavelength threshold.

In some embodiments, based on a detected event, a number of wavelength readings that satisfy the upper or lower wavelength thresholds may be determined by computer system **102** (e.g., event detection subsystem **112**). As an example, a number of wavelength readings that are above the upper wavelength threshold for a threshold amount of time, a number of consecutive wavelength readings that are above the upper wavelength threshold, a number of wavelength readings that are below the lower wavelength threshold for a threshold amount of time, or a number of consecutive wavelength readings that are below the lower wavelength threshold may be determined. The number of wavelength readings may correspond to a number of changes (e.g., a number of consecutive changes) in the wavelength readings that are above the upper wavelength threshold or below the lower wavelength threshold for a threshold amount of time.

In some embodiments, a duration of the detected event occurring at or near the sensor may be determined by event detection subsystem **112** based on the number of wavelength readings (e.g., or a number of time slices for wavelength readings) that exceed the upper wavelength threshold (or fall below the lower wavelength threshold). In some embodiments, the number of wavelength readings that exceed the upper wavelength threshold (or fall below the lower wavelength threshold) or a number of time slices during which one or more wavelength readings exceed the upper wavelength threshold (or fall below the lower wavelength threshold) may be directly proportional to the duration of the event occurring at or near the sensor. In other words, a higher number of wavelength readings that exceed the upper wavelength threshold (or fall below the lower wavelength threshold) or a higher number of time slices during which one or more wavelength readings exceed the upper wavelength threshold (or fall below the lower wavelength threshold) may indicate a longer duration of occurrence of the event and a smaller number of wavelength readings that exceed the upper wavelength threshold (or fall below the lower wavelength threshold) or a smaller number of time slices during which one or more wavelength readings exceed the upper wavelength threshold (or fall below the lower wavelength threshold) may indicate a shorter duration of occurrence of the event.

12

In some embodiments, event detection subsystem **112** may adjust the rate at which wavelength readings are obtained from sensor **142** or a rate at which the sensors **142** read. Such adjustment may be based on the number of the one or more wavelength readings that satisfy the upper or lower wavelength thresholds. As an example, the rate may be increased when the number of the one or more wavelength readings exceeds the predetermined count threshold. Event detection subsystem **112** may adjust the rate back to its initial value when the number of the one or more wavelength readings does not exceed the predetermined count threshold. This adjustment of rate may be continuous.

In some embodiments, computer system **102** (e.g., event detection subsystem **112**) may generate an alert when the number of wavelength readings (e.g., wavelength readings that satisfy an upper or lower wavelength threshold) satisfies a predetermined count threshold. In other words, when the number of wavelength readings that exceed the upper wavelength threshold or fall below the lower wavelength threshold is equal to or greater than a predetermined count threshold, an alert may be generated. The alert may indicate an occurrence of a suspicious event. By generating an alert when wavelength readings exceed the upper wavelength threshold (or fall below the lower wavelength threshold) and when the number of the wavelength readings that exceed the upper wavelength threshold (or fall below the lower wavelength threshold) is equal to or greater than a predetermined count threshold, the system **100** may reduce false positive sensor alerts. In other words, event detection subsystem **112** may detect an event when a wavelength reading exceeds the upper wavelength threshold (or falls below the lower wavelength threshold). However, such an event may not be associated with suspicious activity. For example, if a fixture from a ceiling falls on a floor, the sensor **142** may detect an event because the wavelength reading may exceed the upper wavelength threshold (or may fall below the lower wavelength threshold). However, such an event may not trigger an alert (e.g., a suspicious activity alert).

As shown in FIG. **3B**, wavelength reading **352** exceeds upper wavelength threshold **354** for a certain number of wavelengths. For example, each one-second time slice (e.g., time slices **358**) may comprise at least one reading and, in some embodiments, readings may be generated, collected (e.g., via data collection subsystem **148**), and sent to computer system **102** (e.g., via communication subsystem **144**) at a rate of 200-500 readings per second. Event detection subsystem **112** may compare a number of readings that exceed wavelength threshold **354** with a predetermined count threshold. In some embodiments, an alert may only be generated when the number of the wavelength readings that exceed the upper wavelength threshold (or fall below the lower wavelength threshold) is equal to or greater than a predetermined count threshold. This may reduce false positive sensor alerts. In this example, event detection subsystem **112** may determine that the predetermined count threshold (e.g., 2,500 readings) has not been exceeded and may not generate an alert. In some embodiments, if event detection subsystem **112** determines that the predetermined count threshold has been exceeded, a generated alert may be presented via a user interface of computer system **102** (e.g., presentation subsystem **116**). The sensor system **104a** may include a display subsystem **146**. Display subsystem **146** may light up (e.g., using LEDs or other lighting mechanism) to generate an alert with respect to a particular sensor. For example, each sensor **142** may include a light source that lights up when the sensor **142** detects an event.

US 11,367,342 B2

13

In some embodiments, a sensor may “clear” an event or otherwise indicate that an event has ended. For example, computer system **102** may output a message, change a color of one or more sensors, or emit a sound (e.g., via presentation subsystem **116**) to indicate that the event has ended. In some embodiments, failure of a sensor to “clear” after an initialization phase may indicate that an upper wavelength threshold (e.g., upper wavelength threshold **354**, as shown in FIG. 3B) or a lower wavelength threshold may be set incorrectly (e.g., too sensitive).

In some embodiments, system **100** may utilize the data received from various sensors and other sources in order to further reduce false positive alerts. For example, system **100** may determine that an employee badge was scanned at a location near a detected event and that the employee badge belonged to authorized personnel. In some embodiments, system **100** may apply facial recognition techniques to video footage received from a camera sensor in order to identify personnel in a location. System **100** may determine that the detected event is not suspicious based on the recognition of authorized personnel. In some embodiments, system **100** may retrieve a history of events associated with a person in the vicinity of a detected event. For example, if a person often triggers floor sensors (e.g., due to handling or dropping heavy objects), the system may determine that the detected event is not suspicious. In another example, system **100** may cross reference the timeline and location of a detected event with planned maintenance. If the detected event occurred at a location and during a scheduled time of planned maintenance, system **100** may determine that the detected event is not suspicious. In another example, system **100** may determine a function of the location at which the event was detected. For example, if the location is a work space, system **100** may disregard certain events that are detected during work hours. In another example, system **100** may cross reference a detected event with weather data from the time of the detected event. If system **100** determines that severe weather occurred at the time of the event, system **100** may determine that the detected event is not suspicious.

In some embodiments, system **100** may train or configure a prediction model to facilitate generation of a sensor alert. In some embodiments, the prediction model may include one or more neural networks or other machine learning models. As an example, neural networks may be based on a large collection of neural units (or artificial neurons). Neural networks may loosely mimic the manner in which a biological brain works (e.g., via large clusters of biological neurons connected by axons). Each neural unit of a neural network may be connected with many other neural units of the neural network. Such connections can be enforcing or inhibitory in their effect on the activation state of connected neural units. In some embodiments, each individual neural unit may have a summation function which combines the values of all its inputs together. In some embodiments, each connection (or the neural unit itself) may have a threshold function such that the signal must surpass the threshold before it propagates to other neural units. These neural network systems may be self-learning and trained, rather than explicitly programmed, and can perform significantly better in certain areas of problem solving, as compared to traditional computer programs. In some embodiments, neural networks may include multiple layers (e.g., where a signal path traverses from front layers to back layers). In some embodiments, back propagation techniques may be utilized by the neural networks, where forward stimulation is used to reset weights on the “front” neural units. In some embodiments, stimulation and inhibition for neural networks

14

may be more free flowing, with connections interacting in a more chaotic and complex fashion.

In some embodiments, the prediction model may update its configurations (e.g., weights, biases, or other parameters) based on its assessment of the predictions. The database **132** may include training data and one or more trained prediction models.

FIG. 4 shows a machine learning model **400** configured to facilitate generation of a sensor alert, in accordance with one or more embodiments. For example, machine learning model **402** may take inputs **404** and provide outputs **406**. For example, inputs **404** may include wavelength readings from sensors (e.g., sensors **142**, as shown in FIG. 1). In some embodiments, the wavelength readings may correspond to detected strain, no detected strain, an event, or some other state of the sensors. In some embodiments, outputs **406** may include predicted sensor alerts (e.g., including non-alert responses). For example, outputs **406** may include various alert type predictions based on the wavelength readings. In one use case, outputs **406** may be fed back (e.g., active feedback) to machine learning model **402** as input to train machine learning model **402** (e.g., alone or in conjunction with user indications of the accuracy of outputs **406**, labels associated with the inputs, or with other reference feedback information). In another use case, machine learning model **402** may update its configurations (e.g., weights, biases, or other parameters) based on its assessment of its prediction (e.g., outputs **406**) and reference feedback information (e.g., user indication of accuracy, reference labels, or other information). In another use case, where machine learning model **402** is a neural network, connection weights may be adjusted to reconcile differences between the neural network’s prediction and the reference feedback. In a further use case, one or more neurons (or nodes) of the neural network may require that their respective errors be sent backward through the neural network to them to facilitate the update process (e.g., backpropagation of error). Updates to the connection weights may, for example, be reflective of the magnitude of error propagated backward after a forward pass has been completed. In this way, for example, the machine learning model **402** may be trained to generate better predictions.

Real-Time Playback Modification for Activity Event Playback

In some embodiments, computer system **102** (e.g., event detection subsystem **112**) may compile information from multiple sources in order to assess a detected event. For example, event detection subsystem **112** may take into account wavelength readings and generated alerts from sensor system **104a** and computer system **102**, feeds from visual sensors (e.g., cameras) located in and around the infrastructure, other sensor data (e.g., cable tray sensors and temperature, air quality, and moisture sensors), location specific data (e.g., work orders, hours of operation), spatial specific data (e.g., locations of key assets), intrusion sensor data, access control data (e.g., data obtained via sensors that allow access to a venue or infrastructure), weather data, and other received data. Computer system **102** may use all received data in order to contextualize triggered alerts (e.g., based on readings from sensors **142**). In some embodiments, computer system **102** may override triggered alerts or may initiate emergency protocol based on all received data. In some embodiments, data received by computer system **102** may cause adjustment subsystem **110** to adjust normal states and wavelength thresholds associated with sensors **142** (e.g., based on data indicating that standard environmental factors triggered the alert). In some embodiments, computer system

US 11,367,342 B2

15

102 may use all available data to continuously adjust the normal state of the sensors 142 to reduce the occurrence of false positive alerts.

In some embodiments, computer system 102 (e.g., user interaction subsystem 118) may provide one or more user interface for monitoring these various sources of information. For example, FIGS. 5A and 5B show user interfaces for monitoring multiple sources of information, in accordance with one or more embodiments. In some embodiments, computer system 102 may obtain data (e.g., such as the data shown in FIGS. 5A and 5B) from one or more sources (e.g., from a camera feed, from sensors 142, etc.). As shown in FIG. 5A, user interface 500 may show a timeline view of multiple streams of data. For example, user interface 500 may show access information 502 for one or more personnel, one or more camera feeds 504, one or more sensor feeds 506, or other information 508 (e.g., weather data). In some embodiments, user interface 500 may show how the streams of data relate to each other with respect to time. For example, for an event that is displayed in the sensor feed 506 (e.g., by a floor sensor 510), user interface 500 may show a camera feed 504 having recordings for the time period of the event. In some embodiments, computer system 102 may additionally have spatial information for camera feeds 504 and sensor feeds 506 (e.g., which cameras are pointed at the areas surrounding the sensors). Therefore, computer system 102 may retrieve the data (e.g., via data collection subsystem 148 and communication subsystem 144) recorded by the camera (e.g., camera feeds 504) in order to gain more information about the event detected by the floor sensor (e.g., sensor feeds 506).

As shown in FIG. 5B, user interface 550 may show an event thread view, which may correlate disturbance data with spatial information (e.g., asset 512, floor 526), one or more cameras (e.g., camera 522, camera 524), one or more sensors (e.g., sensors 518), access information (e.g., access 520), personnel information (e.g., actor 516, actor 528), and other information.

In some embodiments, both user interface 500 and user interface 550 may contribute to the computation of a threat likelihood of an event. For example, computer system 102 (e.g., event detection subsystem 112) may determine a likelihood that one or more personnel detected in a location is a threat based on the information provided by user interface 500 and user interface 550. As shown in FIG. 5C, user interface 575 may show a threat analysis 530. For example, if a first person (e.g., actor 532) is detected in a location to which they do not have personnel access, event detection subsystem 112 may calculate a high probability (e.g., 95%) that the person is a threat. If a second person (e.g., actor 534) is detected in a location to which they have personnel access, event detection subsystem 112 may calculate a low probability (e.g., 5%) that the person is a threat. In some embodiments, factors which may contribute to a high probability of a threat may include who is in a location, who has access to the location, a history of people who have been in the location, whether a disturbance in the location was expected (e.g., due to planned maintenance), if the disturbance was triggered by a person or some other cause, and other factors. The threat analysis 530 may rely in part on a listing of events 536. The listing of events 536 may list date and time information, event type information, and event data (e.g., personnel information) relating to detected events. For example, event detection subsystem 112 may compare event information from event listing 536 to personnel access information (e.g., access information 502, as shown in FIG.

16

5A) or other information provided by user interface 500 and user interface 550 in order to perform the threat analysis.

In some embodiments, computer system 102 may output (e.g., via presentation subsystem 116) an alert indicating a suspected threat, a predicted event, or other information. For example, as discussed above in relation to FIG. 3B, computer system 102 (e.g., event detection subsystem 112) may detect an event based on wavelength readings that satisfy an upper or lower wavelength threshold. In some embodiments, computer system 102 may receive input from the user (e.g., via user interaction subsystem 118) in response to the alert. For example, the user may input a request to lock down a portion of a building in which the suspected threat or the predicted event are located. In some embodiments, the user may add or remove personnel access via user interaction subsystem 118. In some embodiments, the user may add or remove one or more camera feeds, one or more sensor feeds, one or more detectors, or may activate or deactivate other devices.

In some embodiments, system 100 may utilize the data received from various sensors, cameras, and other sources (as shown in FIGS. 5A and 5B) in order to further reduce false positive alerts. For example, system 100 may determine that an employee badge was scanned at a location near a detected event and that the employee badge belonged to authorized personnel. In some embodiments, system 100 may apply facial recognition techniques to video footage received from a camera sensor in order to identify personnel in a location. System 100 may determine that the detected event is not suspicious based on the recognition of authorized personnel. In some embodiments, system 100 may determine a history of events associated with a person in the vicinity of a detected event. For example, if a person often triggers events (e.g., due to handling or dropping heavy objects), the system may determine that the detected event is not suspicious. In another example, system 100 may cross reference the timeline and location of a detected event with planned maintenance. If the detected event occurred at a location and during a scheduled time of planned maintenance, system 100 may determine that the detected event is not suspicious. In another example, system 100 may determine a function of the location at which the event was detected. For example, if the location is a work space, system 100 may disregard events that are detected during work hours. In another example, system 100 may cross reference a detected event with weather data from the time of the detected event. If system 100 determines that severe weather occurred at the time of the event, system 100 may determine that the detected event is not suspicious.

Returning to FIG. 1, system 100 may facilitate real-time playback modification for activity event playback. For example, system 100 may modify playback of events, alerts, feeds, and other assets depicted in FIGS. 5A and 5B. Computer system 102 (e.g., presentation subsystem 116), in some embodiments, may provide a user interface (e.g., via presentation subsystem 116 and user interaction subsystem 118) for modifying activity event playback. In some embodiments, computer system 102 may receive a user request (or query) via a user interface. For example, FIGS. 6A and 6B show user interfaces 600 and 650 for a user request, in accordance with one or more embodiments. In some embodiments, the user can request presentation of a listing of events via user interface 600. In a user request (or query), the user may indicate a location (e.g., location 602) of interest (e.g., from a drop down menu, by selecting items from a checklist, by typing a location identifier, or through another input method). The user may also indicate a time and

US 11,367,342 B2

17

date (e.g., time and date range **604**) of interest. In some embodiments, computer system **102** may retrieve (e.g., from the database **132**) a listing of events that correspond to the user request and search criteria.

As shown in FIG. 6B, the user may request a replay of events via user interface **650**. For example, user interface **650** may display a timeline corresponding to a timeline or date range (e.g., last thirty days) selected by the user (e.g., via user interaction subsystem **118**). In some embodiments, the timeline may be displayed (e.g., via presentation subsystem **116**) with selectable portions (e.g., selectable squares **652**). In some embodiments, each square of selectable squares **652** may represent an event. In some embodiments, selectable squares **652** may be color coded (e.g., yellow for warnings, red for alarms, green for normal states, etc.). In some embodiments, the user may select one or more squares to set a start or end of events for replay. In some embodiments, the user may manually enter a start or end of events for replay. In some embodiments, the user may request playback of the selected events (e.g., by selecting the launch button **654**). In some embodiments, other methods of selecting events for playback may be used.

In some embodiments, one or more events specified or selected by the user (e.g., via user interface **600** or user interface **650**) may be played back via a user interface. The user interface may include a first portion and a second portion (or a window on the user interface may include a first portion and a second portion). The first portion may be configured to play back one or more events (e.g., one or more detected events by event detection subsystem **112** described above). As an example, FIG. 7 shows a user interface **700** for playback of events, in accordance with one or more embodiments. FIG. 7 illustrates a first portion **702** of the user interface that includes a listing of events. In some embodiments, the listing of events in the first portion **702** may correspond to events specified or selected by the user (e.g., via user interface **600** or user interface **650**, as shown in FIGS. 6A and 6B). In some embodiments, the first portion **702** of the user interface **700** may provide additional information associated with the events. For example, the additional information associated with the events may include a category associated with each event of the set of events, a date and time associated with each event of the set events, or a location associated with each event of the set of events.

In some embodiments, the user interface may include a second portion **704**, as illustrated in FIG. 7. The second portion **704** of the user interface may be configured to present playback of events in accordance with event detection times. For example, the first portion **702** of the user interface may present a listing of events based on a time and a location associated with the events. In other words, the set of events listed on the first portion **702** of the user interface may be based on times of detection of the events by one or more sensors **142** and locations of the events. In some embodiments, responsive to a selection of an action icon (e.g., action icon **706**), playback may commence or continue. While playback of the set of events listed on the first portion **702** is occurring, the second portion **704** of the user interface may present a playback of events by overlaying a set of layers corresponding to the events onto the second portion **704** of the user interface. For example, the second portion **704** may overlay one layer for each event listed in the first portion **702**. In some embodiments, a layer may include a location map. In other words, an event layer may include an illustration of an event on top of a location map such that a user viewing the overlaid layer may visualize the occurrence of the event at the location at which it occurred.

18

For example, as shown in FIG. 7, the second portion **704** includes a location map of infrastructure at a particular location. In some embodiments, event layers may be overlaid on top of this location map in order to demonstrate where certain events occurred relative to the infrastructure. In some embodiments, each event layer may correspond to an event listed in the first portion **702**. In other words, each layer may correspond to one or more events related to activity alerts generated by sensors **142** (e.g., as shown in FIG. 1) based on event detection. For example, each event related to activity alerts generated by sensors **142** may be associated with a location and a time at which the event was detected. The event may then be mapped to a location on a location map of infrastructure (e.g., second portion **704**). Based on this mapping, the event layers (associated with events) may be visually overlaid onto the location map. In some embodiments, a different event layer (associated with a different event) detected at a different location may be overlaid onto a different location map.

In FIG. 7, layer **714** corresponds to an event playback of event **712**. In some embodiments, event **712** from the listing of events (e.g., in the first portion **702**) may be highlighted while the corresponding layer **714** is being played. For example, the first portion **702** may highlight event **712** and the second portion **704** may simultaneously show all sensors **716** (e.g., floor sensors, rack door sensors, cable tray sensors, etc.) at a particular location associated with event **712** as well as the states associated with sensors **716** at the time of event **712**. For example, second portion **704** may show sensors **716** having certain colors, in various states, monitoring certain contents (e.g., by weight or visually), generating alerts, or in other states. For example, the event layers may be color coded to indicate whether event **712** is suspicious. In other words, the sensors **716** may be illustrated in red if the event is determined to be suspicious or yellow if the event is determined not to be suspicious (e.g., based on the disclosure above). In some embodiments, the sensors **716** may be illustrated in green if no event was detected by the corresponding sensors **142** during the time period of the selected event. In some embodiments, the sensors **716** may blink or otherwise convey additional information (e.g., indicating that the sensors **716** are active).

In some embodiments, additional information may be provided during the presentation of event layer **714**. For example, if a particular sensor (e.g., from sensors **716**) is associated with a door (e.g., rack door), the playback may indicate whether the door was opened. For example, an icon (e.g., a lock icon) may be presented with the event layer **714** at a location corresponding to the location of a door sensor. The icon may change color, morph (e.g., into an open lock), or otherwise change to indicate that a door was opened. In some embodiments, the user may interact with (e.g., click, hover over, select) various areas of the user interface **700**. Such user interaction allows additional information about the event to be overlaid on the first portion **702** or the second portion **704** of the user interface **700**. This is advantageous because the user is provided with additional information about the event without leaving the current window or needing to go back and forth between different windows. For example, a user may interact with the illustration of sensors **716** in FIG. 7 in order to view additional information about the sensors **716** (e.g., which contents each sensor is monitoring, more details about the state of the sensor, etc.). In some embodiments, the user may interact with button **718** in order to view additional information about an event in the first portion **702**. For example, an interaction with button **718** may cause additional information about the severity of

US 11,367,342 B2

19

an event to be displayed, including disturbance and movement information associated with a sensor during the time period of the event.

In some embodiments, while the event playback (e.g., of events listed in the first portion **702**) is occurring via the second portion **704**, a user selection of events may be obtained via user interface **700** (e.g., by user interaction subsystem **118**). This real-time modification of playback improves upon the speed and efficiency of conventional systems. For example, enabling a user to select a subset of a listing of events during playback of the listing of events allows a user to quickly find and play back one or more events of interest without compromising playback. In other words, the real-time modification may allow the user to narrow in on a subset of events without stopping, exiting, or otherwise delaying playback. The increased efficiency of the methods and systems described herein may allow the user to more quickly identify a suspicious event and determine the cause of the event. The increased speed and efficiency of these methods and systems may allow the user to correct for a suspicious activity before the event becomes dangerous (e.g., to personnel or to property).

In some embodiments, a user may select a subset of events from the listing of events (e.g., first portion **702**) to be presented in the playback via the second portion **704**. In some embodiments, a user may select a first subset of events from the listing of events (e.g., first portion **702**) that the user does not wish to be presented in the playback via the second portion **704** and a second subset of events from the listing of events (e.g., first portion **702**) that the user wishes to be presented on the playback via the second portion **704**. Although not shown in FIG. 7, a user may select the one or more events via a checkbox associated with each event listed on the first portion **702** of the user interface or may select from a drop-down list. The drop-down list may allow a user to select the one or more events based on, for example, a category associated with the one or more events. For example, a user may only be interested in the category “warning” and can select “warning” from a drop-down list such that one or more events associated with the category “warning” are selected to be presented via the second portion **704** of the user interface. In other words, the user selection indicates a second subset of events that the user wishes to playback via the user interface. Accordingly, the second subset of events may be presented via the second portion **704** of the user interface based on the user selection. In some embodiments, a size of a text associated with the subset of events may be increased in response to the user selection of the one or more events. In other words, a size of the text associated with the listing of events may be smaller than a size of the text associated with the subset of events. A size of text associated with the subset of events may be increased in proportion to a difference between a number of events in the entire set of events and a number of events in the subset of events. In some embodiments, the text associated with the listing of events may be wrapped around so that it fits within the first portion **702** of the user interface. In some embodiments, only a portion of the text associated with the event may be presented via the first portion **702** of the user interface. In response to a user selection (or, for example, in response to a user hovering the mouse over the event), the entire text corresponding to the event may be displayed by overlaying such text on the user interface.

In some embodiments, in response to a user selection of a subset of events for playback, during the playback, the set of layers associated with the listing of events (e.g., as described above) may be modified such that layers corre-

20

sponding to the subset of events are added to the playback. In some embodiments, in response to a user selection of a first subset of events not to be presented in the playback and a second subset of events to be presented in the playback, the set of layers associated with the listing of events (e.g., as described above) may be modified such that layers corresponding to the first subset of events are removed from the event playback and layers corresponding to the second subset of events are added to the event playback. For example, layers corresponding to the second subset of events may be retrieved from database **132** and added to the event playback. In other words, layers that are associated with the first subset of events may be removed from the event playback such that the layers that are used for the event playback correspond to the second subset of events. The layers may be stored in a presentation buffer (not shown), for example, in database **132** and may be retrieved from the database **132** in response to a user request and search criteria discussed above. Accordingly, in response to the user selection of one or more events from the listing of events, the presentation buffer may be updated such that the presentation buffer includes the layers corresponding to the second subset of events. Computer system **102** (e.g., presentation subsystem **116**) may cause the layers (corresponding to the subset of events) to be overlaid on the second portion **704** of the user interface. In some embodiments, updating the presentation buffer may include removing, from the presentation buffer, one or more layers corresponding to one or more events that are included in the set of events and excluded from the second subset of events or one or more layers corresponding to one or more events that are included in the first subset of events. This allows a user to playback the new set of layers relatively quickly after the user selection of one or more subsets of events from the listing of events because the entire presentation buffer does not need to be replaced in response to the user selection of one or more events.

In some embodiments, computer system **102** may cause the layers corresponding to the second subset of events to be overlaid on the second portion **704** of user interface **700**, as shown in FIG. 7, based on the modification of the set of layers such that the second subset of events is presented or played back based on detection times associated with the second subset of events. For example, layers corresponding to the second subset of events may be overlaid onto the second portion **704** (e.g., over a location map) of the user interface **700**. Each layer may correspond to a location map, and the location map for one layer may be different from a location map associated with another layer. In other words, a first layer presented on the second portion **704** of the user interface may correspond to a first event detected at a first time (e.g., detected by one or more sensors **142**) and a second layer presented on the second portion **704** of the user interface may correspond to a second event detected at a second time (e.g., detected by one or more sensors **142**), where the second time is after the first time.

In some embodiments, each layer may be overlaid on the second portion **704** of user interface **700** for a predetermined amount of time. For example, FIG. 7 illustrates a portion **708** via which a user may enter a time. Each layer may be overlaid on the second portion **704** of the user interface based on the user-entered time. In some embodiments, the user interface may include a rewind button **710** that will allow a previously overlaid layer to be overlaid again onto the second portion of the user interface in response to the user selection of the rewind button **710**.

US 11,367,342 B2

21

FIG. 8 shows a plurality of layers 800 for playback of events, in accordance with one or more embodiments. For example, FIG. 8 illustrates a previously played layer 802, a currently playing layer 804, and a next layer to be played 806. In some embodiments, sensor event data is loaded onto each of the layers. Sensors may be shown as pins on the layers (e.g., to mark locations of the sensors). For example, pins may be standard shapes, lines, or custom icons or images. In some embodiments, a state of each sensor (e.g., at a time corresponding to the particular layer) may be represented with a color of the sensor (e.g., green, yellow, red, blue, etc.). In some embodiments, when a user navigates to an event (e.g., by selecting an event from first portion 702 of user interface 700, as shown in FIG. 7), the layer corresponding to the selected event is retrieved (e.g., from memory, from database 132, or from another location). In some embodiments, computer system 102 may create a linkage between the layer corresponding to the selected event and previous layers. In some embodiments, computer system 102 may cross reference the current layer with previous layers to ensure that the pins (e.g., corresponding to sensors) are depicted correctly (e.g., location, state, etc.). In some embodiments, computer system 102 may ensure that the layer corresponding to a selected event (e.g., currently playing layer 804) is displayed to the user (e.g., via presentation subsystem 116). In some embodiments, the layer corresponding to the selected event (e.g., currently playing layer 804) may be displayed in the second portion 704 of user interface 700, as shown in FIG. 7.

In some embodiments, layers 802, 804, and 806 may correspond to layers or layer groups. For example, each layer group may comprise multiple events, displays, time points, or other data. In some embodiments, a user selection of an event in a layer group may cause a layer corresponding to the event to be displayed as the visible portion of the corresponding layer group.

Accordingly, the user interface may present activity alerts. In other words, a visual presentation of activity in one or more areas of a venue may be presented for playback, thereby allowing a user to reconstruct a series of events in a monitored area or venue.

Example Flowcharts

FIGS. 9 and 10 are example flowcharts of processing operations of methods that enable the various features and functionality of the system as described in detail above. The processing operations of each method presented below are intended to be illustrative and non-limiting. In some embodiments, for example, the methods may be accomplished with one or more additional operations not described, and/or without one or more of the operations discussed. Additionally, the order in which the processing operations of the methods are illustrated (and described below) is not intended to be limiting.

In some embodiments, the methods may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The processing devices may include one or more devices executing some or all of the operations of the methods in response to instructions stored electronically on an electronic storage medium. The processing devices may include one or more devices configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of the methods.

22

FIG. 9 shows a flowchart of a method 900 for generating a sensor alert based on continuous adjustment of a normal state of a sensor, in accordance with one or more embodiments.

In an operation 902, a plurality of wavelength readings may be obtained from a sensor. For example, the plurality of wavelengths may be continuously received from one or more camera sensors, cable tray sensors, temperature, air quality, or moisture sensors, optical sensors, or other sensors. In some embodiments, operation 902 may be performed by a subsystem that is the same as or similar to communication subsystem 114, in accordance with one or more embodiments.

In an operation 904, a normal state of the sensor may be continuously adjusted based on wavelength readings of the plurality of wavelength readings that fail to satisfy both upper and lower wavelength thresholds of the continuously-adjusted normal state. For example, continuously adjusting the normal state of the sensor may include continuously adjusting a centerline wavelength, the upper wavelength threshold, or the lower wavelength threshold associated with the sensor. In some embodiments, operation 904 may be performed by a subsystem that is the same as or similar to adjustment subsystem 110, in accordance with one or more embodiments.

In an operation 906, an event may be detected when one or more wavelength readings from the sensor satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state. In other words, an event may be detected when one or more wavelength readings exceed the upper wavelength threshold or fall below the lower wavelength threshold of the continuously-adjusted normal state. In some embodiments, operation 906 may be performed by a subsystem that is the same as or similar to event detection subsystem 112, in accordance with one or more embodiments.

In an operation 908, based on the detected event, a number of wavelength readings that satisfy the upper or lower wavelength thresholds may be determined. As an example, a number of wavelength readings that are above the upper wavelength threshold for a threshold amount of time, a number of consecutive wavelength readings that are above the upper wavelength threshold, a number of wavelength readings that are below the lower wavelength threshold for a threshold amount of time, or a number of consecutive wavelength readings that are below the lower wavelength threshold may be determined. The number of wavelength readings may correspond to a number of changes (e.g., a number of consecutive changes) in the wavelength readings that are above the upper wavelength threshold or below the lower wavelength threshold for a threshold amount of time. In some embodiments, operation 908 may be performed by a subsystem that is the same as or similar to event detection subsystem 112, in accordance with one or more embodiments.

In an operation 910, an alert may be generated when the number of wavelength readings satisfies a predetermined count threshold. In other words, when the number of wavelength readings that exceed the upper wavelength threshold or fall below the lower wavelength threshold is equal to or greater than a predetermined count threshold, an alert may be generated. In some embodiments, operation 908 may be performed by a subsystem that is the same as or similar to presentation subsystem 116 or user interaction subsystem 118, in accordance with one or more embodiments.

US 11,367,342 B2

23

FIG. 10 shows a flowchart of a method 1000 for facilitating real-time playback modification for suspicious activity event playback, in accordance with one or more embodiments.

In an operation 1002, a user interface may be provided. The user interface may include (i) a first portion configured to present a set of events and (ii) a second portion configured to present a playback of events in accordance with event detection times and a set of event layers for the playback. Each layer of the set of layers may indicate one or more events related to alerts generated by sensors based on an event detection. In some embodiments, the first portion of the user interface may provide additional information associated with the events. For example, the additional information associated with the events may include a category associated with each event of the set of events, a date and time associated with each event of the set of events, or a location associated with each event of the set of events. In some embodiments, the second portion of the user interface may include a location map of infrastructure at a particular location. In some embodiments, operation 1002 may be performed by a subsystem that is the same as or similar to presentation subsystem 116 or user interaction subsystem 118, in accordance with one or more embodiments.

In an operation 1004, during the playback, a user selection of events may be obtained via the user interface. The user selection may indicate a subset of events to be presented in the playback. For example, the user may select a time range, a location, a type of event, a category of events, or another selection. The subset of events may include events which match the user's selections. In some embodiments, operation 1004 may be performed by a subsystem that is the same as or similar to user interaction subsystem 118, in accordance with one or more embodiments.

In an operation 1006, during the playback, a set of layers for the playback may be modified based on the user selection such that layers corresponding to the subset of events are added to the event playback. In some embodiments, in response to a user selection of a subset of events to be presented in the playback, the set of layers associated with the listing of events may be modified such that layers corresponding to the subset of events are added to the event playback and layers not corresponding to the subset of events are removed from the event playback. For example, layers corresponding to the subset of events may be retrieved from a database and added to the event playback. Layers that are not associated with the subset of events may be removed from the event playback. Layers may be stored in a presentation buffer in a database and may be retrieved from the database in response to a user request and search criteria. In some embodiments, operation 1006 may be performed by a subsystem that is the same as or similar to presentation subsystem 116, in accordance with one or more embodiments.

In an operation 1008, the layers corresponding to the subset of events may be caused to be overlaid on the second portion of the user interface based on the modification of the set of layers such that the subset of events are presented based on detection times associated with the subset of events. For example, each event of the subset of events may be associated with a location and a time at which the event was detected. The event may then be mapped to a location on a location map of the infrastructure. For example, the second portion may be overlaid with one layer for each event of the subset of events. In other words, an event layer may include an illustration of an event on top of a location map such that the event layer illustrates where in the infrastruc-

24

ture the event took place. In some embodiments, each layer may correspond to a location map, and the location map associated with one layer may be different from a location map associated with another layer. In some embodiments, operation 1008 may be performed by a subsystem that is the same as or similar to presentation subsystem 116, in accordance with one or more embodiments.

FIG. 11 shows a flowchart of a method 1100 for facilitating identification of a location of an occurrence of an event, in accordance with one or more embodiments.

In an operation 1102, for each of one or more wavelength readings that satisfies the upper or lower wavelength threshold, a first magnitude of a difference between the wavelength reading and a centerline wavelength of the continuously-adjusted normal state may be determined. For example, the first magnitude may be calculated for any wavelength that is greater than the upper wavelength threshold or lower than the lower wavelength threshold. In some embodiments, operation 1102, may be performed by a subsystem that is the same as or similar to event detection subsystem 112, in accordance with one or more embodiments.

In an operation 1104, a second magnitude of a difference between a maximum wavelength associated with the floor sensor and the centerline wavelength may be obtained. In some embodiments, the maximum wavelength may be a maximum threshold limit or minimum threshold limit associated with the sensor. In some embodiments, operation 1104, may be performed by a subsystem that is the same as or similar to event detection subsystem 112, in accordance with one or more embodiments.

In an operation 1106, a ratio between the first magnitude and the second magnitude may be determined. In some embodiments, the ratio between the first magnitude and the second magnitude may be inversely proportional to the distance of the occurrence of the event from the floor sensor. In some embodiments, operation 1106, may be performed by a subsystem that is the same as or similar to event detection subsystem 112, in accordance with one or more embodiments.

In an operation 1108, a distance of the occurrence of the event from the floor sensor based on the determined ratio may be determined. For example, a ratio of one would indicate that the event occurred at the location of the floor sensor. A smaller ratio (e.g., closer to zero) would indicate a larger distance of the occurrence of the event from the sensor and a larger ratio (e.g., closer to one) would indicate a smaller distance of the occurrence of the event from the sensor. In some embodiments, operation 1108, may be performed by a subsystem that is the same as or similar to event detection subsystem 112, in accordance with one or more embodiments.

In an operation 1110, a location on a floor of a venue of the occurrence of the event based on the distance and based on a location of the floor sensor may be identified. The location of the sensor may be known and may be stored in the database. In some embodiments, operation 1110, may be performed by a subsystem that is the same as or similar to event detection subsystem 112, in accordance with one or more embodiments.

In some embodiments, the various computers and subsystems illustrated in FIG. 1 may include one or more computing devices that are programmed to perform the functions described herein. The computing devices may include one or more electronic storages (e.g., database(s) 132), one or more physical processors programmed with one or more computer program instructions, and/or other components. The computing devices may include communica-

US 11,367,342 B2

25

tion lines or ports to enable the exchange of information within a network (e.g., network 150) or other computing platforms via wired or wireless techniques (e.g., Ethernet, fiber optics, coaxial cable, Wi-Fi, Bluetooth, near field communication, or other technologies). The computing devices may include a plurality of hardware, software, and/or firmware components operating together. For example, the computing devices may be implemented by a cloud of computing platforms operating together as the computing devices.

The electronic storages may include non-transitory storage media that electronically stores information. The storage media of the electronic storages may include one or both of (i) system storage that is provided integrally (e.g., substantially non-removable) with servers or client devices or (ii) removable storage that is removably connectable to the servers or client devices via, for example, a port (e.g., a USB port, a firewire port, etc.) or a drive (e.g., a disk drive, etc.). The electronic storages may include one or more of optically readable storage media (e.g., optical disks, etc.), magnetically readable storage media (e.g., magnetic tape, magnetic hard drive, floppy drive, etc.), electrical charge-based storage media (e.g., EEPROM, RAM, etc.), solid-state storage media (e.g., flash drive, etc.), and/or other electronically readable storage media. The electronic storages may include one or more virtual storage resources (e.g., cloud storage, a virtual private network, and/or other virtual storage resources). The electronic storage may store software algorithms, information determined by the processors, information obtained from servers, information obtained from client devices, or other information that enables the functionality as described herein.

The processors may be programmed to provide information processing capabilities in the computing devices. As such, the processors may include one or more of a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information. In some embodiments, the processors may include a plurality of processing units. These processing units may be physically located within the same device, or the processors may represent processing functionality of a plurality of devices operating in coordination. The processors may be programmed to execute computer program instructions to perform functions described herein of subsystems 110-118, 142-148, or other subsystems. The processors may be programmed to execute computer program instructions by software; hardware; firmware; some combination of software, hardware, or firmware; and/or other mechanisms for configuring processing capabilities on the processors.

It should be appreciated that the description of the functionality provided by the different subsystems 110-118 and 142-148 described herein is for illustrative purposes, and is not intended to be limiting, as any of subsystems 110-118 and 142-148 may provide more or less functionality than is described. For example, one or more of subsystems 110-118 and 142-148 may be eliminated, and some or all of its functionality may be provided by other ones of subsystems 110-118 and 142-148. As another example, additional subsystems may be programmed to perform some or all of the functionality attributed herein to one of subsystems 110-118 and 142-148.

Although the present invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely

26

for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the scope of the appended claims. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

The present patent filing is one of a set of two filed on the same day by the same applicant. These patent filings have the following titles: METHOD AND SYSTEM FOR GENERATING SENSOR ALERTS BASED ON CONTINUOUS ADJUSTMENT OF A NORMAL STATE OF A SENSOR and REAL-TIME PLAYBACK MODIFICATION FOR ACTIVITY EVENT PLAYBACK. The entire contents of each of the patent filings other than this one is hereby incorporated by reference.

The present techniques will be better understood with reference to the following enumerated embodiments:

1. A method comprising: continuously obtaining a plurality of wavelength readings from a sensor; continuously adjusting a normal state of the sensor based on wavelength readings of the plurality of wavelength readings that fail to satisfy both upper and lower wavelength thresholds of the continuously-adjusted normal state; detecting an event when one or more wavelength readings from the sensor satisfy the upper or lower wavelength thresholds of the continuously-adjusted normal state; determining, based on the detected event, a number of wavelength readings that satisfy the upper or lower wavelength threshold; and generating an alert when the number of wavelength readings satisfies a predetermined count threshold.

2. The method according to embodiment 1, further comprising: determining a duration of the event occurring at or near the sensor based on the number of wavelength readings, wherein the number of wavelength readings is directly proportional to the duration of the event occurring at or near the sensor.

3. The method according to any of embodiments 1-2, further comprising: determining, for each of the one or more wavelength readings that satisfies the upper wavelength threshold, a first magnitude of a difference between the wavelength reading and a centerline wavelength of the continuously-adjusted normal state; obtaining a second magnitude of a difference between a maximum wavelength associated with the sensor and the centerline wavelength; determining a ratio between the first magnitude and the second magnitude; determining a distance of the occurrence of the event from the sensor based on the determined ratio; and identifying a location on a floor of a venue of the occurrence of the event based on the distance and based on a location of the sensor, wherein the ratio between the first magnitude and the second magnitude is inversely proportional to the distance of the occurrence of the event from the sensor.

4. The method according to any of embodiments 1-3, further comprising: determining, for each of the one or more wavelength readings that satisfies the lower wavelength threshold, a first magnitude of a difference between the wavelength reading and a centerline wavelength of the continuously-adjusted normal state; obtaining a second magnitude of a difference between a maximum wavelength associated with the sensor and the centerline wavelength; determining a ratio between the first magnitude and the second magnitude; determining a distance of the occurrence of the event from the sensor based on the determined ratio; and identifying a location on a floor of a venue of the

US 11,367,342 B2

27

occurrence of the event based on the distance and based on a location of the sensor, wherein the ratio between the first magnitude and the second magnitude is inversely proportional to the distance of the occurrence of the event from the sensor.

5. The method according to any of embodiments 1-4, wherein the centerline wavelength is an average of the plurality of wavelength readings.

6. The method according to any of embodiments 1-5, further comprising: adjusting a rate of obtaining additional wavelength readings based on the number of the one or more wavelength readings that satisfy the upper or lower wavelength thresholds, wherein the rate is increased when the number of the one or more wavelength readings exceeds the predetermined count threshold.

7. The method according to any of embodiments 1-6, wherein continuously adjusting the normal state of the sensor includes continuously adjusting a centerline wavelength, the upper wavelength threshold, and the lower wavelength threshold associated with the sensor.

8. The method according to any of embodiments 1-7, wherein the sensor is a floor sensor, wherein the floor sensor is a wavelength-specific reflector.

9. A method comprising: providing a user interface including (i) a first portion configured to present a listing of events and (ii) a second portion configured to present a playback of events on a location map in accordance with event detection times and a set of event layers for the event playback, each layer of the set of event layers indicating one or more events related to activity alerts generated by sensors based on an event detection; obtaining, during the playback, a user selection of events via the user interface, the user selection indicating a subset of events to be presented in the playback; modifying, during the playback, a set of layers for the playback based on the user selection such that layers corresponding to the subset of events are added to the event playback; and causing the layers corresponding to the subset of events to be overlaid on the second portion of the user interface based on the modification of the set of layers such that the subset of events is presented based on detection times associated with the subset of events.

10. The method according to embodiment 8, wherein the first portion is an event list portion.

11. The method according to any of embodiments embodiment 9-10, wherein the second portion is an event playback portion.

12. The method according to any of embodiment 9-11, further comprising: while the event playback is occurring, obtaining another user selection of events via the event list portion of the user interface, the second user selection indicating another subset of events that is not to be presented in the event playback; and while the event playback is occurring, modifying the set of layers for the event playback based on the user selection such that other event layers corresponding to the other subset of events are removed from the event playback.

13. The method according to any of embodiments 9-12, wherein each layer of the set of layers is overlaid onto the location map for a predetermined amount of time.

14. The method according to any of embodiments embodiment 9-13, wherein the set of events includes a category associated with each event of the set of events, a date and time associated with each event of the set of events, a location associated with each event of the set of events, and an action icon associated with one or more events of the set of events.

15. The method according to any of embodiments 9-14, further comprising: responsive to a selection of the action

28

icon associated with an event of the set of events, causing a new window to be loaded on the user interface, the new window including additional information associated with the event.

16. The method according to any of embodiments 9-15, further comprising: causing a previously overlaid layer to be overlaid again onto the second portion of the user interface in response to another user selection, wherein the other user selection corresponds to a selection to rewind the playback.

17. The method according to any of embodiments 9-16, further comprising: causing a listing of an event associated with a currently overlaid layer to be highlighted on the first portion of the user interface.

18. The method according to any of embodiments 9-17, further comprising: causing a size of text associated with the subset of events to be increased in proportion to a difference between a number of events in the set of events and a number of events in the subset of events.

19. The method according to any of embodiments 9-18, further comprising: updating a presentation buffer in response to the user selection such that the presentation buffer is updated to include the layers corresponding to the subset of events; and causing the layers from the presentation buffer to be overlaid on the second portion of the user interface.

20. The method according to any of embodiments 9-19, wherein updating the presentation buffer includes removing, from the presentation buffer, one or more layers corresponding to one or more events that are included in the set of events and excluded from the subset of events.

21. A tangible, non-transitory, computer-readable medium storing instructions that, when executed by a data processing apparatus, cause the data processing apparatus to perform operations comprising those of any of embodiments 1-20.

22. A system comprising: one or more processors; and memory storing instructions that, when executed by the processors, cause the processors to effectuate operations comprising those of any of embodiments 1-20.

What is claimed is:

1. A method for facilitating real-time playback modification for activity event playback, the method being implemented by one or more processors configured to execute one or more computer program instructions, the method comprising:

providing a user interface including (i) an event list portion configured to present a listing of events and (ii) an event playback portion configured to present a playback of events on a location map in accordance with event detection times and a set of event layers for the event playback, each layer of the set of event layers indicating one or more events related to activity alerts generated by sensors based on an event detection;

while the event playback is occurring, obtaining a user selection of events via the event list portion of the user interface, the user selection indicating a first subset of events not to be presented in the event playback and a second subset of events to be presented in the event playback;

while the event playback is occurring, modifying a set of layers for the event playback based on the user selection such that, first event layers corresponding to the first subset of events are removed from the event playback, and second event layers corresponding to the second subset of events are retrieved from a database and added to the event playback; and

causing the second event layers to be overlaid onto the location map based on the modification of the set of

US 11,367,342 B2

29

layers such that the second subset of events is presented based on detection times associated with the second subset of events.

2. The method according to claim 1, wherein each layer of the set of layers is overlaid onto the location map for a predetermined amount of time.

3. The method according to claim 1, wherein the listing of events includes a category associated with each event of the listing of events, a date and time associated with each event of the listing of events, a location associated with each event of the listing of events, and an action icon associated with one or more events of the listing of events.

4. The method according to claim 3, further comprising: responsive to a selection of the action icon associated with an event of the second subset of events, causing a new window to be loaded on the user interface, the new window including additional information associated with the event.

5. The method according to claim 1, further comprising: causing a previously overlaid layer to be overlaid again onto the location map in response to another user selection, wherein the other user selection corresponds to a selection to rewind the event playback.

6. The method according to claim 1, further comprising: causing a listing of an event associated with a currently overlaid layer to be highlighted on the event list portion of the user interface.

7. The method according to claim 1, further comprising: causing a size of text associated with the second subset of events to be increased in proportion to a difference between a number of events in the listing of events and a number of events in the second subset of events.

8. A system, comprising:

a computer system that comprises one or more processors programed with computer program instructions that, when executed, cause the computer system to:

provide a user interface including (i) a first portion configured to present a set of events and (ii) a second portion configured to present a playback of events in accordance with event detection times and a set of event layers for the playback, each layer of the set of layers indicating one or more events related to alerts generated by sensors based on an event detection;

obtain, during the playback, a user selection of events via the user interface, the user selection indicating a subset of events to be presented in the playback;

modify, during the playback, a set of layers for the playback based on the user selection such that layers corresponding to the subset of events are added to the event playback; and

cause the layers corresponding to the subset of events to be overlaid on the second portion of the user interface based on the modification of the set of layers such that the subset of events is presented based on detection times associated with the subset of events.

9. The system according to claim 8, wherein each layer of the set of layers is overlaid on the second portion of the user interface for a predetermined amount of time.

10. The system according to claim 8, wherein the set of events includes a category associated with each event of the set of events, a date and time associated with each event of the set of events, a location associated with each event of the set of events, and an action icon associated with one or more events of the set of events.

11. The system according to claim 10, wherein the computer system is caused to:

30

responsive to a selection of the action icon associated with an event of the set of events, cause a new window to be loaded on the user interface, the new window including additional information associated with the event.

12. The system according to claim 8, wherein the computer system is caused to:

cause a previously overlaid layer to be overlaid again onto the second portion of the user interface in response to another user selection, wherein the other user selection corresponds to a selection to rewind the playback.

13. The system according to claim 8, wherein the computer system is caused to:

cause a listing of an event associated with a currently overlaid layer to be highlighted on the first portion of the user interface.

14. The system according to claim 8, wherein the computer system is caused to:

cause a size of text associated with the subset of events to be increased in proportion to a difference between a number of events in the set of events and a number of events in the subset of events.

15. The system according to claim 8, wherein the computer system is caused to:

update a presentation buffer in response to the user selection such that the presentation buffer is updated to include the layers corresponding to the subset of events; and

cause the layers from the presentation buffer to be overlaid on the second portion of the user interface.

16. The system according to claim 15, wherein updating the presentation buffer includes removing, from the presentation buffer, one or more layers corresponding to one or more events that are included in the set of events and excluded from the subset of events.

17. One or more non-transitory, computer-readable media storing instructions that, when executed by one or more processors, effectuate operations comprising:

providing a user interface including (i) a first portion configured to present a set of events and (ii) a second portion configured to present a playback of events in accordance with event detection times and a set of event layers for the playback, each layer of the set of layers indicating one or more events related to alerts generated by sensors based on an event detection;

obtaining, during the playback, a user selection of events via the user interface, the user selection indicating a subset of events to be presented in the playback;

modifying, during the playback, a set of layers for the playback based on the user selection such that layers corresponding to the subset of events are added to the event playback; and

causing the layers corresponding to the subset of events to be overlaid on the second portion of the user interface based on the modification of the set of layers such that the subset of events is presented based on detection times associated with the subset of events.

18. The non-transitory, computer-readable media according to claim 17, further comprising:

causing a size of text associated with the subset of events to be increased in proportion to a difference between a number of events in the set of events and a number of events in the subset of events.

19. The non-transitory, computer-readable media according to claim 17, further comprising:

US 11,367,342 B2

31

updating a presentation buffer in response to the user selection such that the presentation buffer is updated to include the layers corresponding to the subset of events; and

causing the layers from the presentation buffer to be overlaid on the second portion of the user interface. 5

20. The non-transitory, computer-readable media according to claim 19, wherein updating the presentation buffer includes removing, from the presentation buffer, one or more layers corresponding to one or more events that are included in the set of events and excluded from the subset of events. 10

* * * * *

32

Exhibit 5

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
 Stylesheet Version v1.2

EPAS ID: PAT7943274

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT
CONVEYING PARTY DATA	
Name	Execution Date
NETWORK INTEGRITY SYSTEMS, INC.	05/05/2023
RECEIVING PARTY DATA	
Name:	CYBERSECURE IPS LLC
Street Address:	3 BETHESDA METRO CENTER
Internal Address:	SUITE 700
City:	BETHESDA
State/Country:	MARYLAND
Postal Code:	20814
PROPERTY NUMBERS Total: 13	
Property Type	Number
Patent Number:	10914047
Patent Number:	11401680
Application Number:	62303280
Patent Number:	11190271
Patent Number:	11515940
Patent Number:	11501616
Patent Number:	11502749
Patent Number:	11502751
Patent Number:	11502750
Patent Number:	11631308
Patent Number:	11502748
Patent Number:	11501617
Application Number:	17966235
CORRESPONDENCE DATA	
Fax Number:	(619)696-7124
<i>Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.</i>	
Phone:	(202) 399-1009
Email:	IPDocket@grsm.com

PATENT EX-2008

507896150

REEL: 063578 FRAME: 0915

Page 180

Correspondent Name: GORDON REES SCULLY MANSUKHANI, LLP
Address Line 1: 101 WEST BROADWAY
Address Line 2: SUITE 1600
Address Line 4: SAN DIEGO, CALIFORNIA 92101

ATTORNEY DOCKET NUMBER:	NKIS-1309474
NAME OF SUBMITTER:	HOWARD N. SHIPLEY
SIGNATURE:	/Howard N. Shipley/
DATE SIGNED:	05/09/2023

Total Attachments: 3

source=Patent_Assignment_Executed#page1.tif
source=Patent_Assignment_Executed#page2.tif
source=Patent_Assignment_Executed#page3.tif

PATENT ASSIGNMENT

This Patent Assignment Agreement is entered into between Network Integrity Systems, Inc. of 1937 Tate Blvd., S.E., Hickory, NC 28602 ("Assignor") and CyberSecure IPS, LLC of 3 Bethesda Metro Center, Suite 700, Bethesda, MD 20814 ("Assignee").

WHEREAS, Assignee hereby desires to purchase, acquire and accept from Assignor, and Assignor hereby desires to sell, transfer, assign, convey and deliver to Assignee, all of Assignor's entire worldwide right, title and interest in, to and under the U.S. patents and applications listed below in Appendix A (the "Assigned Patents").

NOW, THEREFORE, for good and valuable consideration, the sufficiency and receipt of which is hereby acknowledged, the Parties, intending to be legally bound, hereby agree as follows:

Assignor hereby sells, transfers, assigns, conveys and delivers to Assignee all of its right, title and interest in, to and under the Assigned Patents, all related applications, continuations, continuations-in-part, divisionals, reissues, re-examinations, substitutions and extensions thereof, and all foreign counterparts of the foregoing, the same to be held and enjoyed by Assignee for its own use and enjoyment and the use and enjoyment of its successors, assigns and other legal representatives as the same would have been held and enjoyed by Assignor (or its Affiliates, as applicable) if this Assignment had not been made, as assignee of its respective entire right, title and interest therein, including, without limitation, all statutory and other claims, demands, and causes of action of Assignor or any of its Affiliates, for royalties, fees, or other income from, or infringement, misappropriation or violation of, any of the Assigned Patents, all rights to apply for and to maintain all registrations, renewals and extensions thereof and all right of priority with respect thereto, and all of the proceeds from the foregoing.

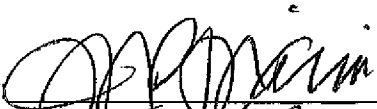
Assignor hereby authorizes and requests the officials of the United States Patent and Trademark Office, and the corresponding entities or agencies in any applicable foreign jurisdiction, to record Assignee as assignee and owner of the entire right, title and interest in, to and under the Assigned Patents.

Assignor further agrees to execute all instruments or documents required or reasonably requested to perfect or record the right, title or interest of Assignee and hereby irrevocably designates and appoints Assignee and its duly authorized officers and agents, as Assignor's agents and attorney in-fact, coupled with an interest to do all other lawfully permitted acts to record, perfect, or otherwise secure that transfer contemplated hereunder.

[SIGNATURES APPEAR ON THE FOLLOWING PAGE]

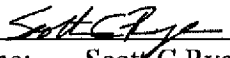
Network Integrity Systems, Inc.

Date: 5-5-23

By: 
Name: Joseph C. Giovanni
Title: CEO

CyberSecure IPS LLC

Date: 5/5/2023

By: 
Name: Scott C Rye Sr.
Title: President / CEO

APPENDIX A

Application No.	Filing Date	Issued Patent	Title
62/303,280	03/03/2016		METHODS AND APPARATUS FOR MONITORING FIBER OPTIC MANHOLE AND DOOR SENSORS
15/449,880	03/03/2017	10,914,047	SYSTEM AND METHOD FOR MONITORING A FIBER AND A DETECTOR ATTACHED TO THE FIBER
17/162,703	01/29/2021	11,401,680	SYSTEM AND METHOD FOR MONITORING A FIBER AND A DETECTOR ATTACHED TO THE FIBER
17/192,091	03/04/2021	11,190,271	METHOD OF MONITORING EVENTS IN AN AREA DIVIDED INTO ZONES
17/018,535	09/11/2020	11,515,940	TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM
17/088,890	11/04/2020	11,501,616	TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM UTILIZING A FAR END OPTICAL SHUTTER
17/088,913	11/04/2020	11,502,749	TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM UTILIZING OUTGOING COMMUNICATION
17/088,968	11/04/2020	11,502,751	TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM ORGANIZED IN A COMMON HOUSING
17/088,931	11/04/2020	11,502,750	TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM PROTECTING MULTIPLE FIBER RUNS
17/088,952	11/04/2020	11,631,308	TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM BY INJECTION OF LONGITUDINAL STRAIN
17/088,905	11/04/2020	11,502,748	TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM UTILIZING COMPLEX TEST SIGNAL
17/089,186	11/04/2020	11,501,617	TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM UTILIZING DIRECT OPTICAL INJECTION
17/966,235	10/14/2022		TEST DEVICE FOR VERIFYING OPERATION OF AN OPTICAL FIBER MONITORING SYSTEM UTILIZING DIRECT OPTICAL INJECTION

Exhibit 6



777 EAST WISCONSIN AVENUE
MILWAUKEE, WI 53202-5306
414.271.2400 TEL
414.297.4900 FAX
FOLEY.COM

WRITER'S DIRECT LINE
414.319.7345
kdodd@foley.com

January 24, 2025

Via Hand Delivery

Dave Cunningham
Network Integrity Systems
1937 Tate Blvd. SE
Hickory, NC 28602

RE: Patent Infringement by Network Integrity Systems

Dear Mr. Cunningham:

My firm represents CyberSecure IPS ("CyberSecure") for purposes of the issues raised in this letter.

Despite CyberSecure's best efforts in the past to amicably resolve outstanding disputes with Network Integrity Systems ("NIS"), it appears NIS continues to take advantage of CyberSecure's technology without permission and without compensation to CyberSecure.

We have identified several patents NIS appears to be infringing, as set forth below. We demand that NIS immediately cease and desist all patent infringement and provide sales information for all products and systems NIS has sold with infringing features.

Testing Technologies

As you know, CyberSecure owns many patents covering testing technologies, such as U.S. Patent No. 11,515,940 ("the '940 patent")¹ and related patents (U.S. Patent Nos. 11,502,749, 11,502,751; 11,501,617; 11,735,016; 11,502,750; 11,631,308; 11,502,748; and 11,501,616). NIS assigned these patents to CyberSecure after CyberSecure learned NIS secretly obtained these patents based on CyberSecure's technology, without permission from CyberSecure.

Although NIS agreed to cease selling its PULSE product, which is covered by at least the '940 patent, it appears NIS continues to offer a testing system. NIS's specification sheet for its AFFIRM product states:

¹ <https://patents.google.com/patent/US11515940B2/en?q=us11%2c515%2c940>



Dave Cunningham
 Network Integrity
 Systems
 January 24, 2025
 Page 2

The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading INTERCEPTOR™ Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our INSIGHT™ Alarm Management and Response software, conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the CNSSI 7003 requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards. Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.

Such a testing system, used in conjunction with NIS's detection products (such as its FOCUS products), infringes at least claim 9 of the '940 patent based on the limited information in NIS's marketing materials. Although we cannot confirm based on the limited information available, it is likely NIS's testing system also infringes other patent claims from this family of patents.

Use of Machine Learning

Even without a testing system, NIS's detection systems infringe CyberSecure's U.S. Patent No. 11,388,181 ("the '181 patent").² The '181 patent covers the use of machine learning in conjunction with detection systems (see, e.g., claim 14). NIS advertises that its detection systems use machine learning. For example, the INTERCEPTOR FOCUS product specification sheet states:

INTERCEPTOR FOCUS^{NX}™ is our next generation long-haul sensing technology that immediately detects and identifies any threat to your classified network infrastructure, while pinpointing its exact location.

The Network Integrity Systems INTERCEPTOR FOCUS^{NX} Optical Intrusion Detection System utilizes Distributed Acoustic Sensing (DAS) technology to monitor long-haul cables and pathways, up to 100km per device, with pinpoint location of any disturbances to your network communications cables, to 1-meter of resolution. INTERCEPTOR FOCUS^{NX} utilizes Phase DAS technology with an improved noise floor and machine learning for accurate event detection.

Presumably, the VANGUARD FOCUS also uses this machine-learning technology.

The Sentinel FOCUS product specification sheet also refers to use of machine learning:

² <https://patents.google.com/patent/US11388181B2/en?q=us11%2c388%2c181+>

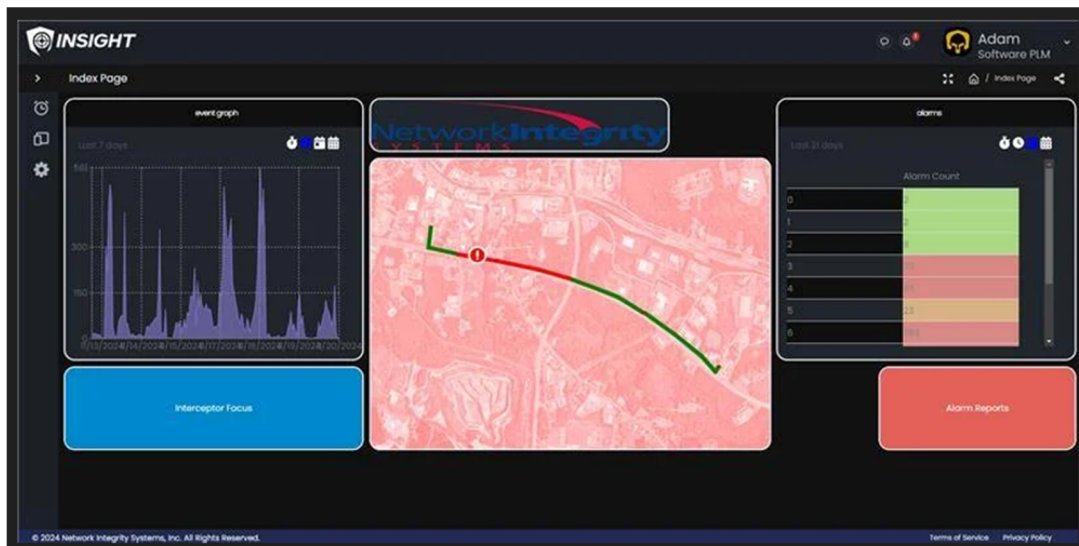
SENTINEL FOCUS^{NX}™ is the next generation Perimeter Intrusion Detection System from NIS, providing a state-of-the-art long-range fiber optic sensor that utilizes Distributed Acoustic Sensing (DAS) to detect and pinpoint the exact location of intrusions on a perimeter. It has proven its capabilities by protecting highly classified U.S. Government facilities and other critical infrastructure sites. A centrally located SENTINEL FOCUS^{NX} sends and receives light into and from optical fibers that are covertly buried, fence-mounted, or wall-mounted along borders and facility perimeters. When physical intrusions create vibrations that reach the optical fibers, the interrogator discerns changes in the light. Then, machine learning-based AI instantly and simultaneously classifies and locates the multiple physical intrusions.

This use of machine learning infringes at least claim 14 of the '181 patent.

Patents Covering Additional Features

It also appears NIS is likely infringing patents for other features of detection systems.

For example, CyberSecure's U.S. Patent No. 9,455,999 ("the '999 patent")³ covers a method for managing a protective distribution system. NIS's website suggests its INSIGHT application infringes this patent (see, e.g., claim 1). The screenshot below indicates the INSIGHT application triggers alerts based on the number of disturbances (shown as green, orange, or red depending on the number of disturbances), which is covered by this patent:



CyberSecure also owns a patent covering aspects of a user interface for a detection system, U.S. Patent No. 11,367,342 ("the '342 patent")⁴ (see, e.g., claim 1). Based on screenshots for INSIGHT on NIS's website (such as the one below), NIS is likely infringing this patent, as well.

³ <https://patents.google.com/patent/US9455999B2/en?q=us9%2c455%2c999+>

⁴ <https://patents.google.com/patent/US11367342B2/en?q=us11%2c367%2c342+>



Claim 1 of the '342 patent covers a user interface that includes: an event list portion (such as the event list in the upper right corner of this screenshot); a location map (such as the map in the middle of this screenshot); selecting events from the list; and layering them on the location map (such as the green line layered on the location map of this screenshot).

In addition to these user-interface patents, CyberSecure owns a patent covering continuous adjustment of a normal state of a sensor, U.S. Patent No. 11,094,189 ("the '189 patent")⁵ (see, e.g., claim 7). It appears NIS is likely infringing this patent with its systems. NIS states the INTERCEPTOR and VANGUARD systems incorporate a "Smart Filtering" technology to "auto-configure" the systems and "eliminate[s] false alarms by learning normal day-to-day activity within the environment." NIS describes its SENTINEL product as a "self-tuning optical sensor." These descriptions suggest infringement of this patent by the INTERCEPTOR, VANGUARD, and SENTINEL systems.

We demand that NIS immediately cease and desist infringement of the '940 and '181 patents, i.e., cease sales of its testing systems (including Pulse, Affirm, and any other testing systems) and remove all machine learning capabilities from its detection systems (including its FOCUS systems and any other detection systems using machine learning).

We also demand that NIS immediately cease and desist any infringement of the '999 patent (covering the trigger of alerts based on disturbance counts), the '342 patent (covering event laying on a location map) and the '189 patent (covering continuous adjustment of a normal state of a sensor).

⁵ <https://patents.google.com/patent/US11094189B2/en?q=us11%2c094%2c189+>



Dave Cunningham
Network Integrity
Systems
January 24, 2025
Page 5

Please also provide sales data (units and revenue information) for all sales of products and systems with these infringing features.

If NIS contends it is not infringing any of these patents, please provide a detailed explanation.

CyberSecure has invested substantial resources to develop the technologies covered by these patents. NIS has repeatedly taken unfair advantage of its past partnership with CyberSecure and is now infringing CyberSecure's patents without seeking permission or offering any compensation. NIS has left CyberSecure with no choice but to rigorously enforce its patents.

Please comply with these demands by February 24, 2025. Failure to respond and address all infringement described in this letter will result in CyberSecure IPS initiating immediate legal action. Please feel free to contact me in the meantime if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Kimberly K. Dodd".

Kimberly K. Dodd

cc: David Vokey
Joseph Giovannini
Lee Brown
Robert Dennis
Amanda Hetzel
Cary Murphy
Trampus Landrum
Mark Bridges
Adam Millan
Sakellarios Spirtos

Exhibit 7

JOE MEADOWS
JMEADOWS@GRSM.COM
DIRECT DIAL: (703) 650-7011



ATTORNEYS AT LAW
277 SOUTH WASHINGTON STREET SUITE 550
ALEXANDRIA, VA 22314
WWW.GRSM.COM

February 24, 2025

BY EMAIL (kdodd@foley.com)

Kimberly K. Dodd
Foley & Lardner LLP
777 East Wisconsin Avenue
Milwaukee, WI 53202-5306

Re: Alleged Patent Infringement by Network Integrity Systems

Dear Ms. Dodd:

We represent Network Integrity Systems, Inc. ("NIS") and we write in response to your and CyberSecure IPS LLC ("CS") letter of January 24, 2025, which was overpublished and personally served on, among others, NIS employees and third persons. Please limit and direct all future communications regarding this matter to our attention.

Contrary to your allegations, NIS has never taken "advantage of CyberSecure's technology without permission" and has not infringed CS patents. We respond to the baseless and speculative infringement allegations in more detail below.

"Testing Technologies" / U.S. Patent No. 11,515,940

All of the claims of the '940 patent require the use of a "fiber disturbance actuator." However, unlike the PULSE system, the NIS AFFIRM system does not include any such "actuator." Thus, there can be no infringement of this patent.

"Use of Machine Learning" / U.S. Patent No. 11,388,181

Your letter contends that the '181 patent covers the use of "machine learning." It does not. There is no mention of "machine learning" in any of the claims, including claim 14 mentioned in your letter. If, as you suggest, the '181 patent broadly covers the use of machine learning with detection systems, the patent would be invalid since machine learning, including pattern recognition and neural networks, has been used in fiber optic detection systems for many years prior to the filing of the '181 patent.

The '181 patent is a "multiple sensor" patent and not a "machine learning" patent. All of the claims of the '181 patent require "multiple sensors associated with a physical transmission line." As CS knows, NIS does not use or sell any products with "multiple sensors associated with a physical transmission line." Thus, there can be no infringement of this patent.

February 24, 2025

Page 2

In fact, NIS owns U.S. Patent No. 8,233,755, which includes claims to a method used with optical fibers. The claims include a step of comparing currently received signals to previously received signals in a manner similar to the claims of your client's '181 patent. Thus, if CS is practicing the claims of the '181 patent, it may be infringing our client's '755 patent.

"Patents Covering Additional Features"

U.S. Patent No. 9,455,999

First, your letter contends that the '999 patent covers a "method for managing a protective distribution system" and that triggering "alerts based on the number of disturbances...is covered by this patent." However, any such method, including the counting of disturbances, predates the filing of the '999 patent by years. *See, e.g.*, U.S. Patent No. 7,375,817.

Indeed, CS knows of the WhatsUpGold system that was in use with NIS products before the filing of the '999 patent, because CS has received detailed information on that system from NIS. The WhatsUpGold system included triggering an alert based on counting of SNMP "traps" that exceed a threshold and occur within a set time period. Thus, to the extent that you contend that the '999 patent broadly covers triggering alerts "based on the number of disturbances", the patent is invalid.

Second, the claims of the '999 patent require use of both "a first preset threshold" and "a second present threshold," as well as determining "a count for the number of disturbances within a preset time period that do not exceed the first preset threshold." NIS products do not count any disturbances that "do not exceed" a threshold. In fact, NIS is not aware of any commercial system that would conduct such a count. Thus, there can be no infringement of this patent.

U.S. Patent No. 11,367,342

All of the claims of the '342 patent require a user interface that includes a "portion configured to present a playback of events on a location map in accordance with event detection times." Your letter notably fails to mention this. NIS does not use or sell any products that include a user interface that presents "a playback of events" whether on a location map or otherwise. Thus, there can be no infringement of this patent.

U.S. Patent No. 11,094,189

All of the claims of the '189 patent require "wavelength readings from a sensor" and "continuous adjustment of a normal state" of a sensor. Given its experience working with the NIS products, CS knows that no NIS products utilize "wavelength readings." Thus, there can be no infringement of this patent.

* * *

February 24, 2025

Page 3

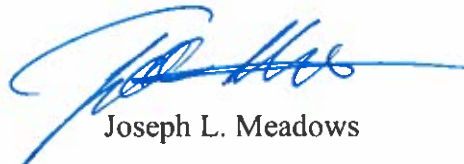
In sum, the infringement allegations are without any merit. We note that your letter includes language such as “appears to be infringing” and “likely infringing” and “suggest infringement.” But a claim for patent infringement cannot be based on such speculation. There must be a reasonable and good faith basis for bringing an infringement claim. Based on your letter and reliance simply on speculation and statements made on NIS’s website, CS and its counsel have not conducted the necessary pre-filing investigation to ensure against a frivolous infringement claim.

We can only assume that you are already aware of the lack of merit to CS’s claims because CS has had ample access to information regarding NIS products. CS employees have worked with and installed hundreds of NIS products. CS had possession of, or access to, all NIS hardware developed during its relationship with NIS, as well as experimental and production firmware versions for each device and has retained possession of multiple versions of NIS hardware. Stephen Sohn, a CS co-founder, had access to NIS confidential information from at least 2013 and, since joining CS in 2017, Bobby Nakanelua, CS CTO, had the same access as Mr. Sohn. CS also had custody of an NIS Interceptor Focus product because Dave Cunningham of NIS transferred this product to Mr. Sohn on November 2, 2018, when they met in a Starbucks parking lot in Commerce, Georgia. The product then remained in the CS testing lab for over five years.

We consider your letter to be an improper attempt by CS to use meritless infringement allegations to unfairly and improperly extract money or other concessions from NIS. That won’t happen.

NIS reserves all rights and remedies.

Sincerely,



Joseph L. Meadows

cc: Dave Cunningham, CEO (via email)
Howard N. Shipley (via email)

Exhibit 8

US Patent No.: 11,515,940 vs. Network Integrity System's Products

Claim	Support for Infringing Product(s) [Annotations in Green]
Claim 9	
<p>[9] A method for verifying operation of an optical fiber monitoring system comprising:</p>	<p>Network Integrity Systems (NIS) sells and has sold products for verifying operation of an optical fiber monitoring system.</p> <p>See 15:00 – 26:00 of the FOSA webinar Lifetime Sensor Verification for DAS Systems presented by Network Integrity System (Available at: https://www.youtube.com/watch?v=gYtfqc-D7H0 (hereinafter “FOSA Webinar”))</p> <div data-bbox="613 537 1728 682">  <p>INTERCEPTOR™ AFFIRM Automated Sensor Verification System</p> </div> <p>Revolutionizing Alarmed PDS Testing with Automated Compliance for CNSSI 7003 Standards</p> <hr/> <div data-bbox="613 820 758 841"> <p>HOW IT WORKS</p> </div> <div data-bbox="613 876 1140 1140"> <p>The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading INTERCEPTOR^{NX} Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our INSIGHT™ Alarm Management and Response software, conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the CNSSI 7003 requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards.</p> </div> <div data-bbox="613 1157 1102 1226"> <p>Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.</p> </div> <div data-bbox="1192 816 1713 1266">  </div> <p>(Available at: https://www.networkintegritysystems.com/interceptor-affirm (hereinafter “AFFIRM Product Page”))</p>

US Patent No.: 11,515,940 vs. *Network Integrity System's Products*

	<p>The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading INTERCEPTOR™ Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our INSIGHT™ Alarm Management and Response software, conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the CNSSI 7003 requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards. Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.</p> <p>(Available at: https://hub.networkintegritysystems.com/hubfs/INTERCEPTOR%20AFFIRM%20Spec%20Sheet%20V2%20page1.pdf (hereinafter: “AFFIRM Product Specifications”))</p> <div data-bbox="535 631 1837 907"> <table border="1"> <thead> <tr> <th>FEATURES & BENEFITS</th> <th>PRODUCT SPECIFICATIONS</th> </tr> </thead> <tbody> <tr> <td colspan="2"> <ul style="list-style-type: none"> ✓ Automated Testing and Reduced Manual Oversight: Automatically conducts periodic testing of the INTERCEPTOR™ Alarmed Carrier PDS system, minimizing the need for labor-intensive, manual testing processes. ✓ Seamless Integration: Works with INSIGHT™ Alarm Management and Response software for automated zone testing. ✓ Operational Integrity Validation and Improved Security: Verifies the functionality of sensing cables to ensure optimal performance. ✓ Compliance Assurance: Meets CNSSI 7003 standards for zone verification testing. ✓ Audit Trail Documentation: INSIGHT generates detailed records of completed inspections and tests. </td> </tr> </tbody> </table> </div> <p>(Available at: AFFIRM Product Page)</p>	FEATURES & BENEFITS	PRODUCT SPECIFICATIONS	<ul style="list-style-type: none"> ✓ Automated Testing and Reduced Manual Oversight: Automatically conducts periodic testing of the INTERCEPTOR™ Alarmed Carrier PDS system, minimizing the need for labor-intensive, manual testing processes. ✓ Seamless Integration: Works with INSIGHT™ Alarm Management and Response software for automated zone testing. ✓ Operational Integrity Validation and Improved Security: Verifies the functionality of sensing cables to ensure optimal performance. ✓ Compliance Assurance: Meets CNSSI 7003 standards for zone verification testing. ✓ Audit Trail Documentation: INSIGHT generates detailed records of completed inspections and tests. 	
FEATURES & BENEFITS	PRODUCT SPECIFICATIONS				
<ul style="list-style-type: none"> ✓ Automated Testing and Reduced Manual Oversight: Automatically conducts periodic testing of the INTERCEPTOR™ Alarmed Carrier PDS system, minimizing the need for labor-intensive, manual testing processes. ✓ Seamless Integration: Works with INSIGHT™ Alarm Management and Response software for automated zone testing. ✓ Operational Integrity Validation and Improved Security: Verifies the functionality of sensing cables to ensure optimal performance. ✓ Compliance Assurance: Meets CNSSI 7003 standards for zone verification testing. ✓ Audit Trail Documentation: INSIGHT generates detailed records of completed inspections and tests. 					
<p>[9][a] using a detection system to detect changes in an optical fiber caused by an event to be monitored by:</p>	<p><i>See supra</i> [9].</p> <p>The NIS products detect changes in an optical fiber caused by an event to be monitored.</p>				



INTERCEPTOR^{NX}TM

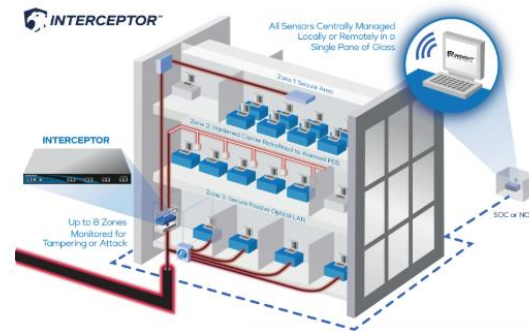
Optical Intrusion Detection System

The most widely deployed centrally managed Alarmed PDS Solution

Designed specifically for the US Federal Government and Military, INTERCEPTOR NX meets the demand for securing classified networks at the physical layer. Adhering to CNSSI 7003 standards, it offers a thorough solution that guarantees organizations pass their CCRI on the first attempt —consistently. This leads to substantial cost savings while also enhancing security measures and boosting overall situational awareness.

HOW IT WORKS

The **INTERCEPTOR^{NX} Optical Network Security System** is capable of protecting up to 8-separate zones or cable paths distributed throughout the building by monitoring spare strands of fibers within optical cables making up the network infrastructure. The system immediately detects and reports even the most subtle tampering or the most sophisticated intrusion attempts conducted for the purposes of data theft (tapping) or denial of service. With Plug-and-ProtectTM capability, INTERCEPTOR^{NX} can be rapidly added to new or existing network infrastructure and can be used in a variety of applications and network architectures.



US Patent No.: 11,515,940 vs. *Network Integrity System's Products*

Alarm Management

SNMPv2c, SNMPv3, Syslog,

Self-Test Heartbeat LED Indicator

Email, SMS alerts

NO/NC Contacts

INTERCEPTOR incorporates a Unidirectional Simplex Optical Communications Port for sending alarms to an optional Cross-Domain Communications Unit

Optional Features

Rear connections

Connector types other than SC/UPC

Aerial fiber monitoring

Active fiber monitoring

Optical

2, 4 or 8 Ports (multimode)

2 or 4 Ports (single-mode)

SC/UPC Duplex Connectors

Dynamic range: multimode 50dB (8 Port mm - 20dB)

Dynamic range: single-mode 55dB

Note: Designed for 3dB Excess/Safety

Lead-in fiber multimode: Sensitive or Desensitized

Lead-in fiber single-mode: Sensitive

(Available at: <https://www.networkintegritysystems.com/interceptor-products> (hereinafter "InterceptorNX Product Page"))

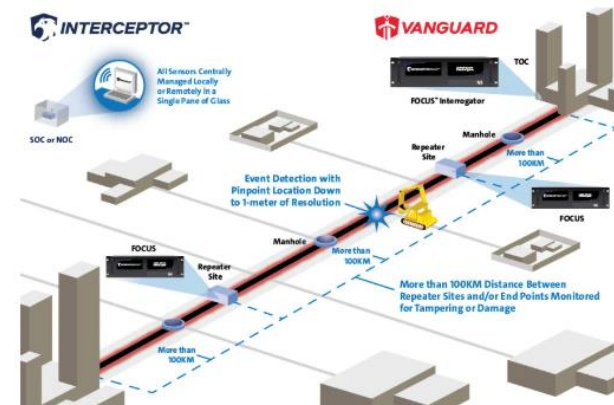
INTERCEPTOR FOCUS^{NX}TM Optical Intrusion Detection System

The U.S. Government and Military utilizes INTERCEPTOR FOCUS NX DAS technology to monitor and protect long-haul classified network infrastructure.

How It Works

INTERCEPTOR FOCUS^{NX} employs Distributed Acoustic Sensing (DAS) technology to effectively monitor your cables in real time, identifying risks with a precision of up to 1-meter resolution.

The INTERCEPTOR FOCUS^{NX} system monitors a single strand of SM cable within long-haul cables and pathways, accurately locating events such as conduit impacts or cable tampering. This minimizes the chances of downtime or data security breaches. By utilizing daisy-chaining techniques, protection for any cable length can be ensured.



(Available at: <https://www.networkintegritysystems.com/interceptor-products-3> (hereinafter “FOCUS NX Product Page”))

2. DAS Capabilities

The Network Integrity Systems INTERCEPTORTM, SENTINELTM and VANGUARDTM FOCUS Optical Intrusion Detection Systems utilize Distributed Acoustic Sensing (DAS) technology to provide long range detection capability along with pinpoint location of any physical disturbances to an optical fiber, either one installed as a dedicated sensor cable or or a fiber intrinsic to an optical communications network. By pulsing light down a single-mode optical fiber, the FOCUS solutions can detect events caused by vibrational disturbances created by abnormal activities such as cable handling, tampering, environmental changes, vehicle or foot traffic, heavy machinery, climbing, cutting or lifting of fence fabric, and tunneling under barriers. Identification of these disturbances can be detected anywhere along the cable up to 100km in length. Also, multiple disturbances, no matter how close or how far to each other, can be detected and located simultaneously.

(Available at: <https://hub.networkintegritysystems.com/hubfs/DAS%20in%20the%20Age%20of%20AI.pdf>
(hereinafter "DAS in the Age of AI"))

The screenshot shows a webinar interface. On the left, a small video window displays a man speaking. The main area features a presentation slide titled "The PULSE™ Sensor Verification System". The slide includes a bullet point: "Precise, Repeatabile results". Below this, there are two side-by-side plots: a blue spectrogram on the left and a heatmap on the right. At the top right of the slide is an image of a black PULSE sensor device. At the bottom, four categories are listed with corresponding icons: "Frequency" (waveform icon), "Amplitude" (up-down arrow icon), "Duration" (clock icon), and "Pattern" (grid icon). The NIS logo is in the bottom right corner. Copyright text at the bottom left reads "©2023 Network Integrity Systems, Inc. All Rights Reserved." and the website "www.networkintegritysystems.com" is at the bottom right.

(Available at: FOSA Webinar at 18:45-19:30)



FOCUS

PULSE



<https://hub.networkintegritysystems.com/hubfs/Documents/Brochures/Pulse/PULSE%20Brochure%20V2.pdf>
(hereinafter “Pulse Brochure”))

6. Summary

INTERCEPTOR FOCUS utilizes state-of-the-art Distributed Acoustic Sensing (DAS) technology to provide long-range capability and pinpoint location of any physical disturbance to your classified communications cable up to 40km in length. The system continuously monitors the entire cable and pathway to immediately detect and report the most sophisticated intrusion attempts, or even the subtlest tampering conducted for the purposes of data theft (tapping) or denial of service.

Fully integrated with our proprietary CyberSecure software platform, the INTERCEPTOR FOCUS solution will centrally monitor and continually automate CNSSI 7003 required inspections and customized Standard Operating Procedures (SOP) for immediate response to any threat to your classified network. The INTERCEPTOR FOCUS can be rapidly deployed in new or existing network infrastructure to rapidly provide security to your physical layer.

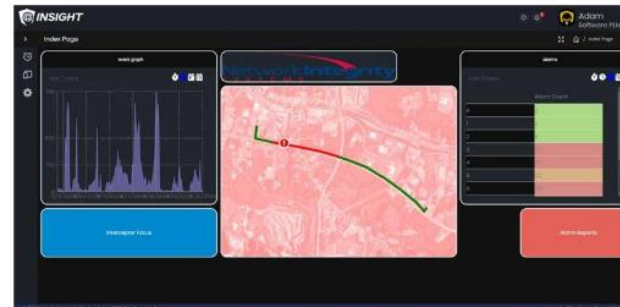


(Available at: <https://hub.networkintegritysystems.com/hubfs/Documents/Brochures/White%20Paper%20-%20INTERCEPTOR%20FOCUS%20Technology.pdf> (hereinafter “FOCUS Whitepaper”))

User-Friendly and Customizable Alarm Management Platform

INSIGHT™ is a sophisticated alarm response and management application crafted to effortlessly integrate with the INTERCEPTOR FOCUS^{NX} and other systems, delivering a thorough and effective security management solution. INSIGHT is developed from the ground up with security in mind and scales effortlessly from single to multi-site installations to meet any security need.

For clients who already have existing alarm response infrastructure in place, we offer INTERLINK™. This specialized feature set within INSIGHT is designed to seamlessly integrate a wide range of sensors into your current infrastructure.



INSIGHT FEATURES & BENEFITS

PRODUCT INFORMATION

- ✓ Seamlessly integrates with NIS' sensor solutions, as well as other systems
- ✓ Provides real-time visibility and instant alarms/notifications
- ✓ Widget-based dashboards allow a customized view for each user
- ✓ Event Processor escalates as each zone alarms
- ✓ Streamlines processes like data analysis, personnel dispatch, and investigations
- ✓ Empowers proactive protection of assets and maintenance of secure environment
- ✓ Flexible licensing to meet your specific requirement

(Available at: FOCUS NX Product Page)



INTERCEPTOR™ AFFIRM

Automated Sensor Verification System

Revolutionizing Alarmed PDS Testing with Automated Compliance for CNSSI 7003 Standards

HOW IT WORKS

The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading INTERCEPTOR^{NX} Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our INSIGHT™ Alarm Management and Response software, conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the CNSSI 7003 requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards.

Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.



FEATURES & BENEFITS

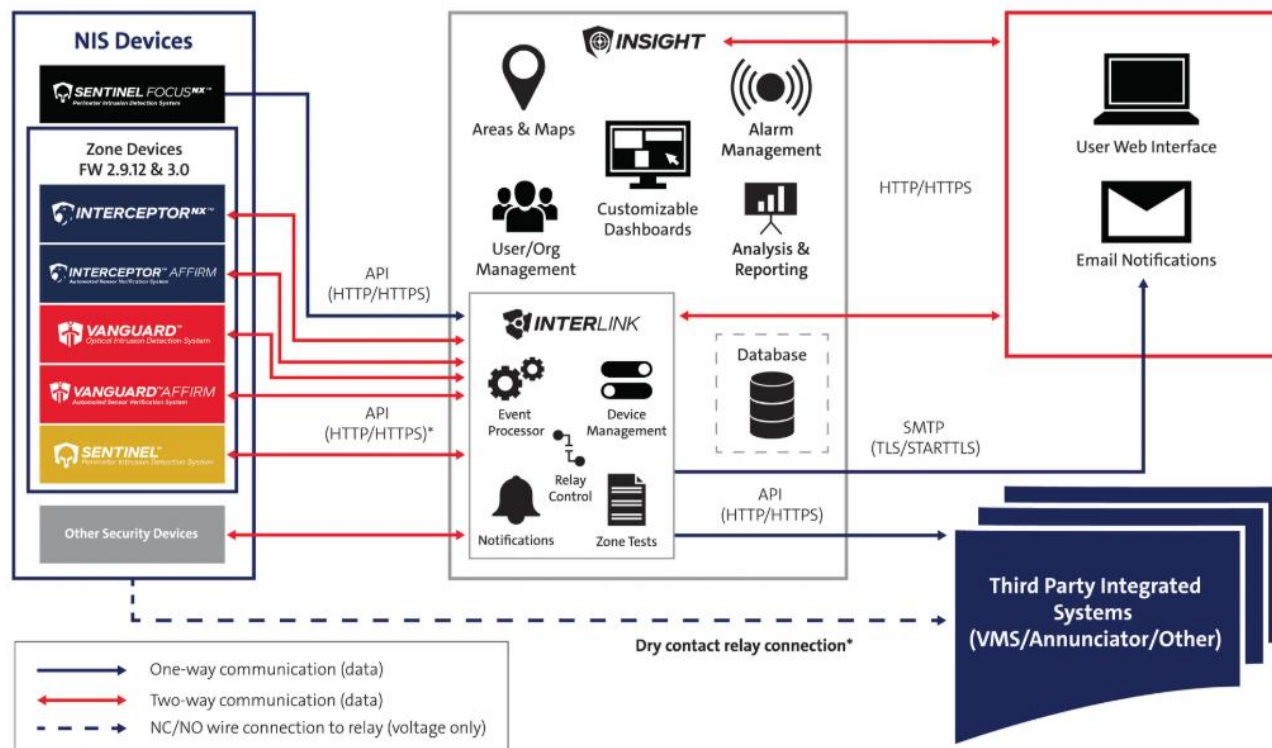
PRODUCT SPECIFICATIONS

- ✓ **Automated Testing and Reduced Manual Oversight:** Automatically conducts periodic testing of the INTERCEPTOR™ Alarmed Carrier PDS system, minimizing the need for labor-intensive, manual testing processes.
- ✓ **Seamless Integration:** Works with INSIGHT™ Alarm Management and Response software for automated zone testing.
- ✓ **Operational Integrity Validation and Improved Security:** Verifies the functionality of sensing cables to ensure optimal performance.
- ✓ **Compliance Assurance:** Meets CNSSI 7003 standards for zone verification testing.
- ✓ **Audit Trail Documentation:** INSIGHT generates detailed records of completed inspections and tests.

(Available at: AFFIRM Product Page)

US Patent No.: 11,515,940 vs. Network Integrity System's Products

System Connectivity Architecture



(Available at: <https://www.networkintegritysystems.com/insight> (herein after "Insight Product Page"))

[9][a][1]transmitti
ng from a source
of light at a
transmit location a
monitor signal
along the optical
fiber;

The NIS products transmit from a source of light at a transmit location a monitor signal along the optical fiber.

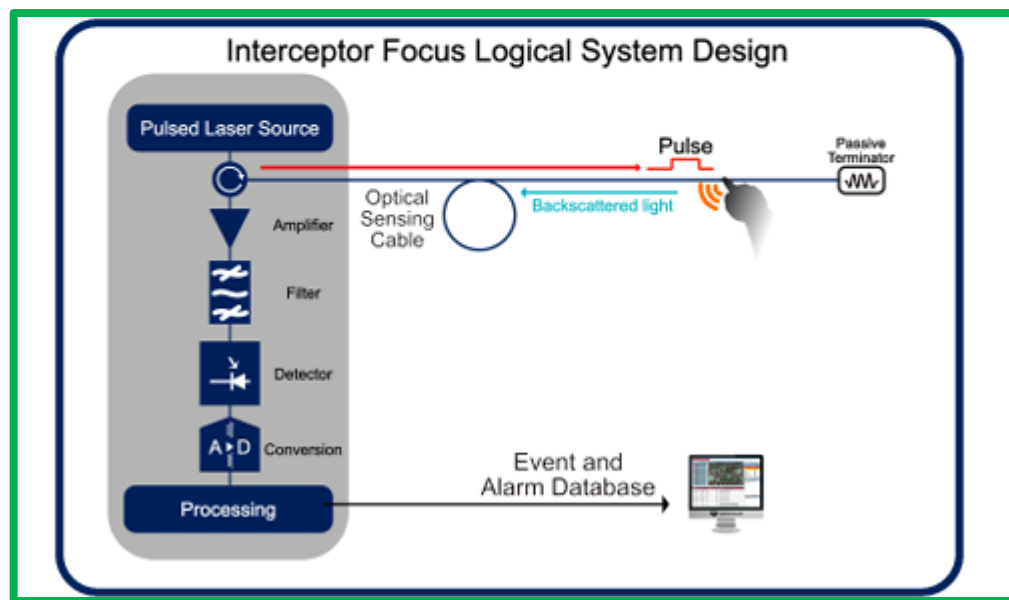
2. Optical Time Domain Reflectometry

Distributed optical fiber sensors typically use a technique called Optical Time Domain Reflectometry (OTDR) to achieve the spatial resolving function mentioned above. This technique is very similar to radar, in that it uses variations in backscatter from intense, short pulses of radiation launched into an optical fiber.

Conventional OTDR instruments are commonly used to measure attenuation profiles of optical fibers in the telecommunication industry. Since optical attenuation does not change rapidly in a fiber, these instruments do not need to respond quickly. They are also optimized to read smoothly from point to point along the fiber under test. This latter aspect of performance requires low noise in the detection system. Instrumental noise arises from two main causes. The first is due to thermal noise in the electronics. The effects of this can be minimized by averaging the results from many interrogation pulses, as well as by increasing the sensitivity of the optical receiver to weak optical signals. The second source of noise that needs to be minimized in conventional OTDR systems is caused by the randomness of the molecular structure of glass fiber, in combination with the narrow relative frequency spread of laser sources. This type of noise is known as Coherent Rayleigh Noise (CRN) and repeats exactly between successive interrogation pulses when the laser and the fiber are stable during the interrogation period. This determinism in the noise precludes any improvement from averaging over repeated pulses and is instead overcome by employing lasers with Wideband optical emission.

4. Spatial Resolution and Vibration Sensitivity

The instantaneous intensity of the CRN is generated by self-interference between all of the reflected signal components from every part of the propagating optical pulse, so the physical length of the pulse limits the spatial resolution of the system. The shorter the pulse is made, the finer the spatial detail. However, shortening the pulse also reduces the mean intensity of the backscatter, making it harder to record the backscatter signature without suffering from random receiver noise. This introduces a tradeoff between spatial resolution and vibration sensitivity. In practice, laser pulses only one or two meters in length can be used to detect mechanical vibrations having amplitudes much smaller than an optical wavelength, thus providing a very good combination of sensitivity and spatial resolution. Helios GS systems offer spatial resolution down to one meter by using optical pulses of only 10 ns duration.



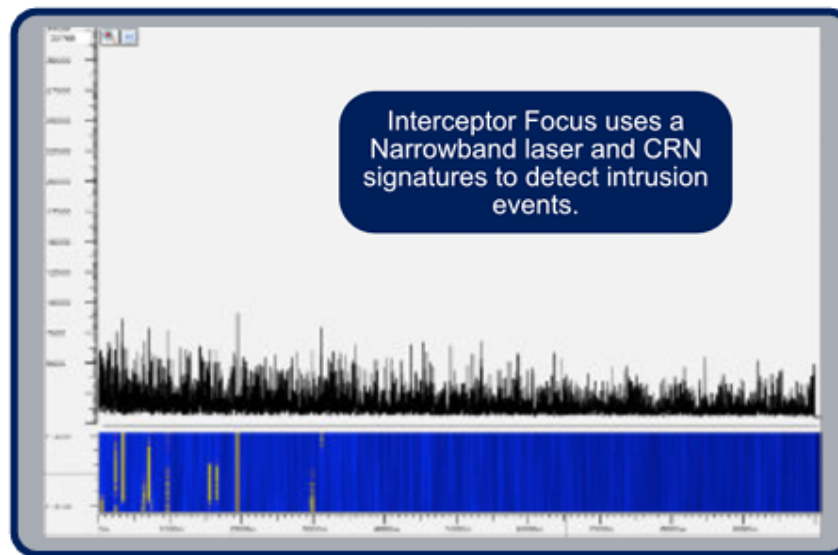
One other advantage of adopting the OTDR method for distributed detection of vibration is that once the backscattered light has left the sensing region, no

US Patent No.: 11,515,940 vs. *Network Integrity System's Products*

	<p>other vibrations can affect its value as it travels back toward the interrogator. This means that from an optical viewpoint, there can be no crosstalk between vibrations present at different points along the sensing fiber. Crucially, this means that even extremely large vibrations at a point close to the interrogator will not disturb signals arising from tiny vibrations far from the interrogator. This allows multiple events to be alarmed and recorded simultaneously.</p> <div data-bbox="726 402 1633 690"> <p>The diagram, titled "Simultaneous Event Reporting", illustrates an optical fiber system. On the left, a computer monitor is connected to a base unit. The monitor displays two red alerts: "Alert! 10.26Km" and "Alert! 23.26Km". The optical fiber is represented by a horizontal line with two circular nodes. Below the first node, a vibration sensor icon is shown with the label "10.26Km". Below the second node, another vibration sensor icon is shown with the label "23.26Km".</p> </div> <p>(Available at: FOCUS Whitepaper)</p>
<p>[9][a][2] receiving the monitor signal after transmission along the optical fiber;</p>	<p>The NIS products receive the monitor signal after transmission along the optical fiber.</p>

3. Distributed Optical Fiber Vibration Sensing

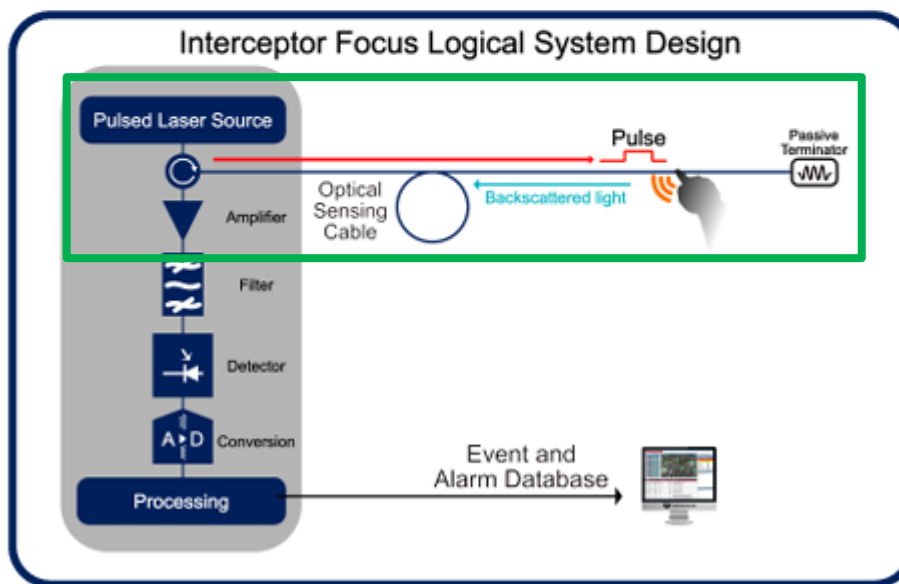
Vibration sensing can be achieved in OTDR systems by shortening the time needed to accurately record the optical backscatter signature of a fiber and by exploiting, rather than minimizing, the CRN signature. Ideally, the backscatter signature should be accurately recorded after a single laser pulse. A narrowband optical source is used to make CRN a large part of the response. CRN is produced by interference between the backscattered contributions from different parts of the traveling pulse of radiation. The received signal is stable if the fiber is undisturbed. INTERCEPTOR FOCUS measures changes in the CRN pattern. Detection noise is minimized by using optical amplification, narrowband optical filtering, and low-pass electronic filtering.



Any changes in the fiber occurring before the next pulse will then lead to associated changes in the backscatter signature from the fiber. The locations of these changes can then be identified in the time domain and converted to known locations. The magnitudes of the changes depend on the strength and type of disturbance acting on the fiber. In order to provide for discrimination of small changes in backscatter signature over distances shorter than the minimum practical pulse length, the data acquisition system in the

4. Spatial Resolution and Vibration Sensitivity

The instantaneous intensity of the CRN is generated by self-interference between all of the reflected signal components from every part of the propagating optical pulse, so the physical length of the pulse limits the spatial resolution of the system. The shorter the pulse is made, the finer the spatial detail. However, shortening the pulse also reduces the mean intensity of the backscatter, making it harder to record the backscatter signature without suffering from random receiver noise. This introduces a tradeoff between spatial resolution and vibration sensitivity. In practice, laser pulses only one or two meters in length can be used to detect mechanical vibrations having amplitudes much smaller than an optical wavelength, thus providing a very good combination of sensitivity and spatial resolution. Helios GS systems offer spatial resolution down to one meter by using optical pulses of only 10 ns duration.



One other advantage of adopting the OTDR method for distributed detection of vibration is that once the backscattered light has left the sensing region, no

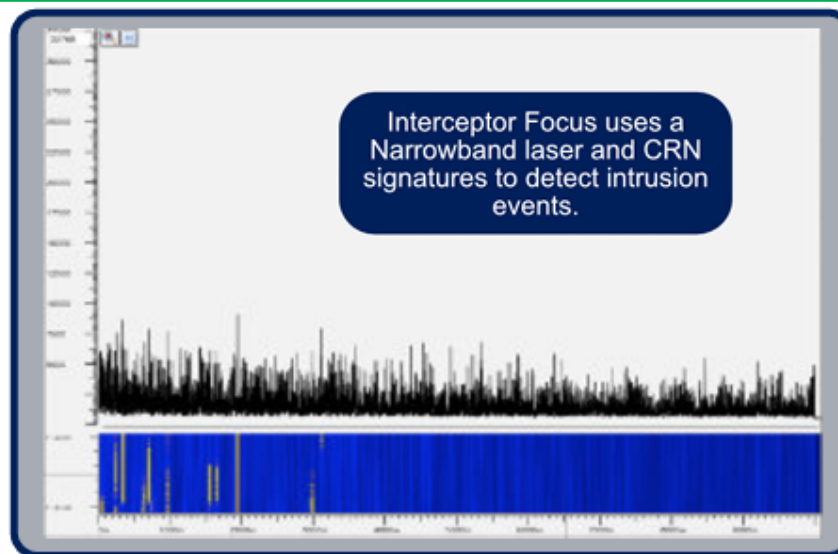
(Available at: FOCUS Whitepaper)

US Patent No.: 11,515,940 vs. *Network Integrity System's Products*

<p>[9][a][3] analyzing the monitor signal after transmission along the optical fiber to detect changes therein caused by the event to be monitored;</p>	<p>The NIS products analyze the monitor signal after transmission along the optical fiber to detect changes therein caused by the event to be monitored.</p>
---	--

3. Distributed Optical Fiber Vibration Sensing

Vibration sensing can be achieved in OTDR systems by shortening the time needed to accurately record the optical backscatter signature of a fiber and by exploiting, rather than minimizing, the CRN signature. Ideally, the backscatter signature should be accurately recorded after a single laser pulse. A narrowband optical source is used to make CRN a large part of the response. CRN is produced by interference between the backscattered contributions from different parts of the traveling pulse of radiation. The received signal is stable if the fiber is undisturbed. INTERCEPTOR FOCUS measures changes in the CRN pattern. Detection noise is minimized by using optical amplification, narrowband optical filtering, and low-pass electronic filtering.

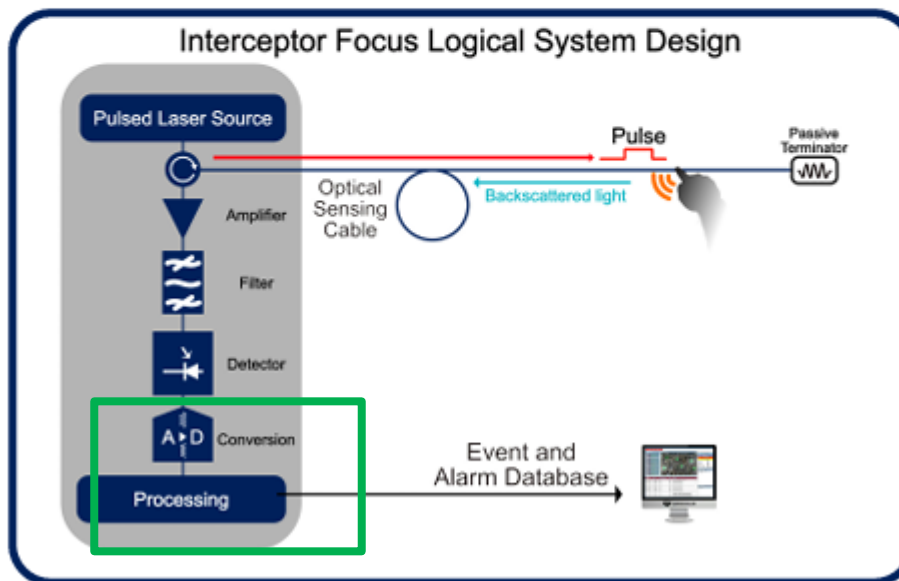


Any changes in the fiber occurring before the next pulse will then lead to associated changes in the backscatter signature from the fiber. The locations of these changes can then be identified in the time domain and converted to known locations. The magnitudes of the changes depend on the strength and type of disturbance acting on the fiber. In order to provide for discrimination of small changes in backscatter signature over distances shorter than the minimum practical pulse length, the data acquisition system in the

(Available at: FOCUS Whitepaper)

4. Spatial Resolution and Vibration Sensitivity

The instantaneous intensity of the CRN is generated by self-interference between all of the reflected signal components from every part of the propagating optical pulse, so the physical length of the pulse limits the spatial resolution of the system. The shorter the pulse is made, the finer the spatial detail. However, shortening the pulse also reduces the mean intensity of the backscatter, making it harder to record the backscatter signature without suffering from random receiver noise. This introduces a tradeoff between spatial resolution and vibration sensitivity. In practice, laser pulses only one or two meters in length can be used to detect mechanical vibrations having amplitudes much smaller than an optical wavelength, thus providing a very good combination of sensitivity and spatial resolution. Helios GS systems offer spatial resolution down to one meter by using optical pulses of only 10 ns duration.



One other advantage of adopting the OTDR method for distributed detection of vibration is that once the backscattered light has left the sensing region, no

US Patent No.: 11,515,940 vs. Network Integrity System's Products

[9][a][4] and generating an alarm in response to said detected changes which are indicative of the event;

The NIS products generate an alarm in response to detected changes which are indicative of the event.

6. Summary

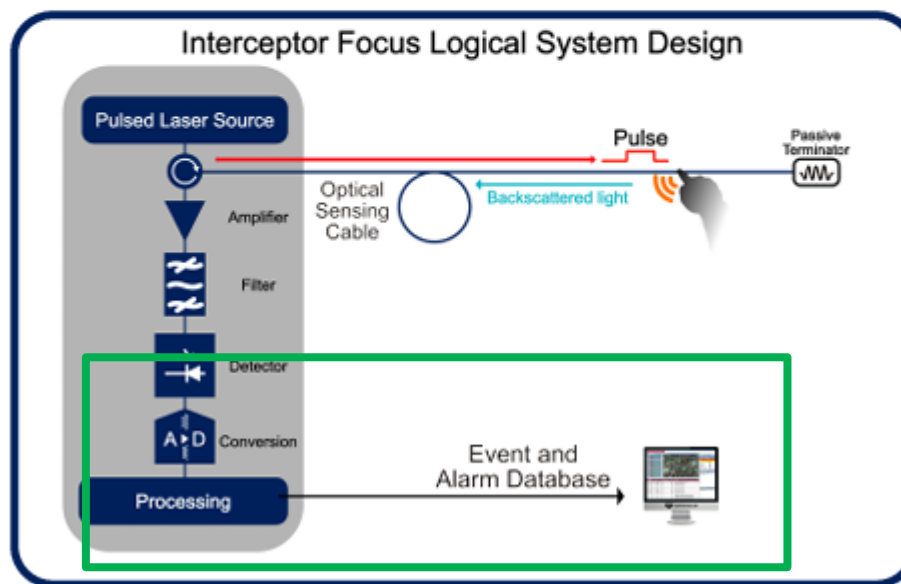
INTERCEPTOR FOCUS utilizes state-of-the-art Distributed Acoustic Sensing (DAS) technology to provide long-range capability and pinpoint location of any physical disturbance to your classified communications cable up to 40km in length. The system continuously monitors the entire cable and pathway to immediately detect and report the most sophisticated intrusion attempts, or even the subtlest tampering conducted for the purposes of data theft (tapping) or denial of service.

Fully integrated with our proprietary CyberSecure software platform, the INTERCEPTOR FOCUS solution will centrally monitor and continually automate CNSSI 7003 required inspections and customized Standard Operating Procedures (SOP) for immediate response to any threat to your classified network. The INTERCEPTOR FOCUS can be rapidly deployed in new or existing network infrastructure to rapidly provide security to your physical layer.



4. Spatial Resolution and Vibration Sensitivity

The instantaneous intensity of the CRN is generated by self-interference between all of the reflected signal components from every part of the propagating optical pulse, so the physical length of the pulse limits the spatial resolution of the system. The shorter the pulse is made, the finer the spatial detail. However, shortening the pulse also reduces the mean intensity of the backscatter, making it harder to record the backscatter signature without suffering from random receiver noise. This introduces a tradeoff between spatial resolution and vibration sensitivity. In practice, laser pulses only one or two meters in length can be used to detect mechanical vibrations having amplitudes much smaller than an optical wavelength, thus providing a very good combination of sensitivity and spatial resolution. Helios GS systems offer spatial resolution down to one meter by using optical pulses of only 10 ns duration.



One other advantage of adopting the OTDR method for distributed detection of vibration is that once the backscattered light has left the sensing region, no

(Available at: FOCUS Whitepaper)

US Patent No.: 11,515,940 vs. Network Integrity System's Products

2. DAS Capabilities

The Network Integrity Systems INTERCEPTOR™, SENTINEL™ and VANGUARD™ FOCUS Optical Intrusion Detection Systems utilize Distributed Acoustic Sensing (DAS) technology to provide long range detection capability along with pinpoint location of any physical disturbances to an optical fiber, either one installed as a dedicated sensor cable or or a fiber intrinsic to an optical communications network. By pulsing light down a single-mode optical fiber, the FOCUS solutions can detect events caused by vibrational disturbances created by abnormal activities such as cable handling, tampering, environmental changes, vehicle or foot traffic, heavy machinery, climbing, cutting or lifting of fence fabric, and tunneling under barriers. Identification of these disturbances can be detected anywhere along the cable up to 100km in length. Also, multiple disturbances, no matter how close or how far to each other, can be detected and located simultaneously.

(Available at: DAS in the Age of AI)

Alarm Management

SNMPv2c, SNMPv3, Syslog,

Self-Test Heartbeat LED Indicator

Email, SMS alerts

NO/NC Contacts

INTERCEPTOR incorporates a Unidirectional Simplex Optical Communications Port for sending alarms to an optional Cross-Domain Communications Unit

Optional Features

Rear connections

Connector types other than SC/UPC

Aerial fiber monitoring

Active fiber monitoring

Optical

2, 4 or 8 Ports (multimode)

2 or 4 Ports (single-mode)

SC/UPC Duplex Connectors

Dynamic range: multimode 50dB (8 Port mm - 20dB)

Dynamic range: single-mode 55dB

Note: Designed for 3dB Excess/Safety

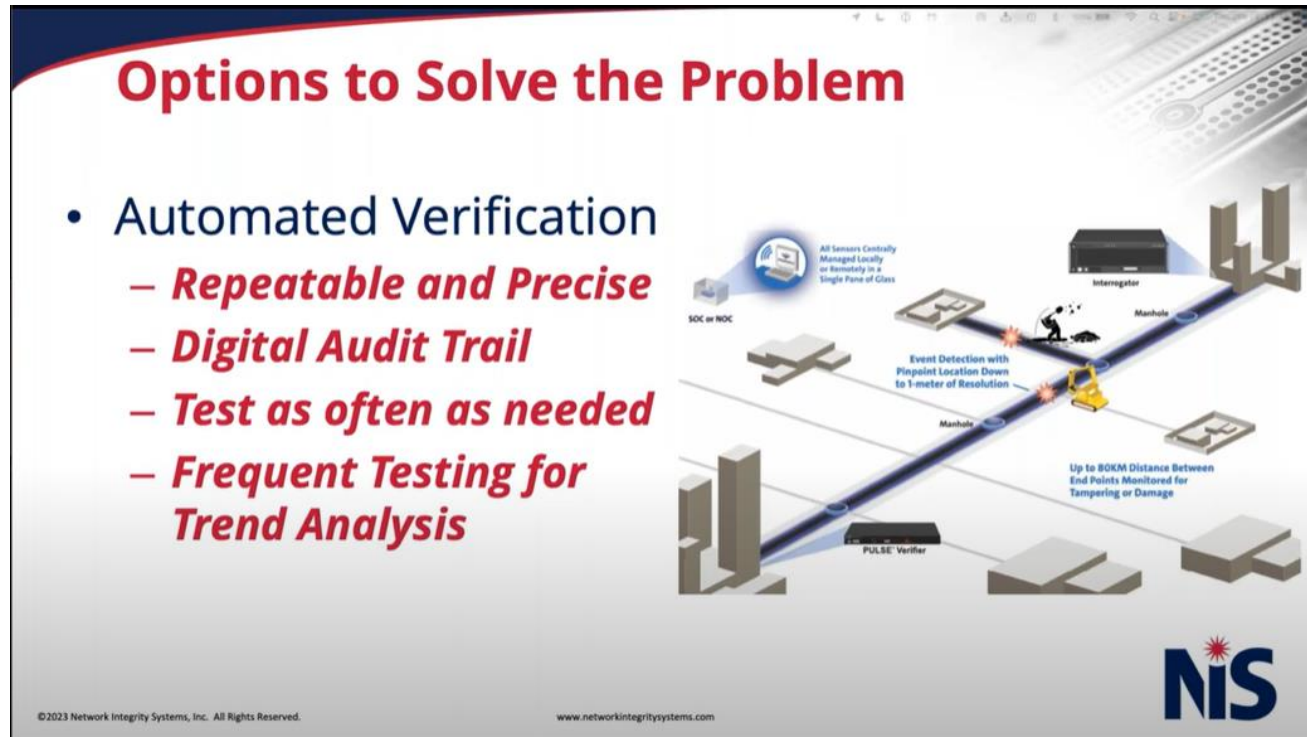
Lead-in fiber multimode: Sensitive or Desensitized

Lead-in fiber single-mode: Sensitive

(Available at: "InterceptorNX Product Page")

[9][b] and repeatedly checking proper operation of the optical fiber monitoring system by:

The NIS products (e.g., *see supra* [9][a]) repeatedly check proper operation of the optical fiber monitoring system.



(Available at: 15:00 – 16:15 FOSA Webinar)

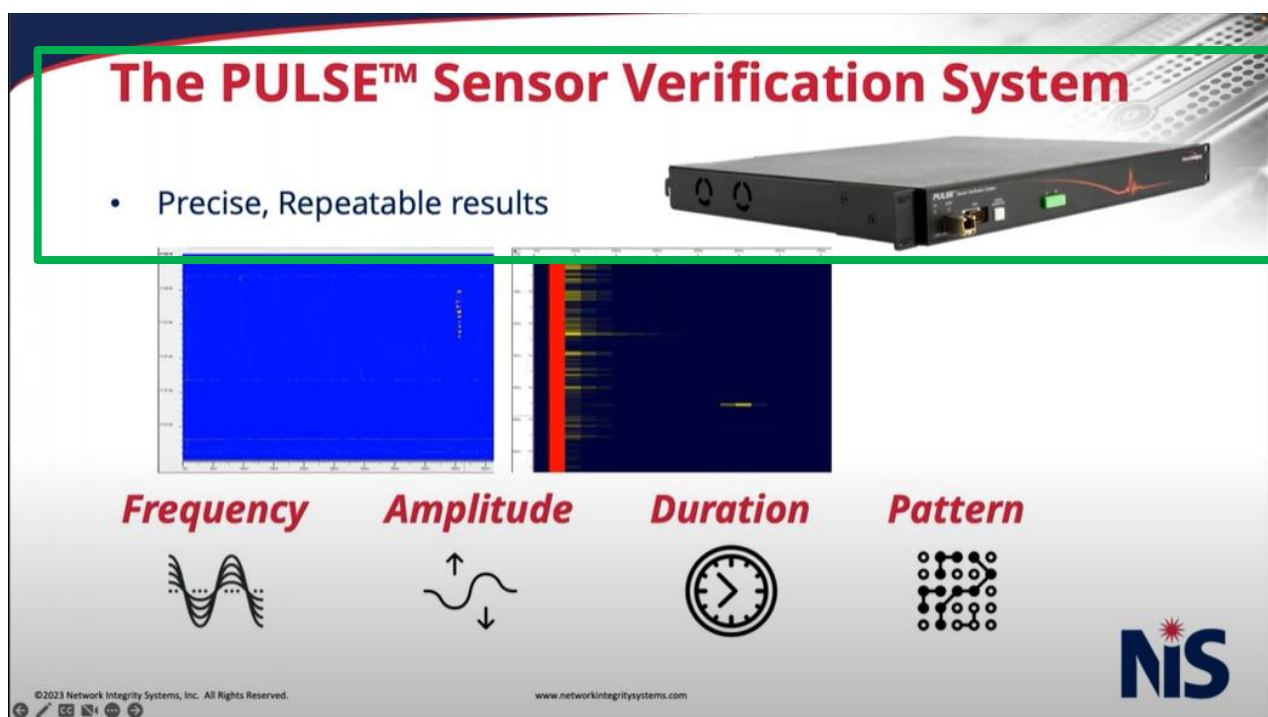
FEATURES & BENEFITS	PRODUCT SPECIFICATIONS
<ul style="list-style-type: none"> ✓ Automated Testing and Reduced Manual Oversight: Automatically conducts periodic testing of the INTERCEPTOR™ Alarmed Carrier PDS system, minimizing the need for labor-intensive, manual testing processes. ✓ Seamless Integration: Works with INSIGHT™ Alarm Management and Response software for automated zone testing. ✓ Operational Integrity Validation and Improved Security: Verifies the functionality of sensing cables to ensure optimal performance. ✓ Compliance Assurance: Meets CNSSI 7003 standards for zone verification testing. ✓ Audit Trail Documentation: INSIGHT generates detailed records of completed inspections and tests. 	

(Available at: AFFIRM Product Page)

[9][b][1] providing a fiber disturbance actuator to cause at least one disturbance of a portion of the optical fiber at a predetermined location thereon where said at least one disturbance is characteristic of the event to be monitored;

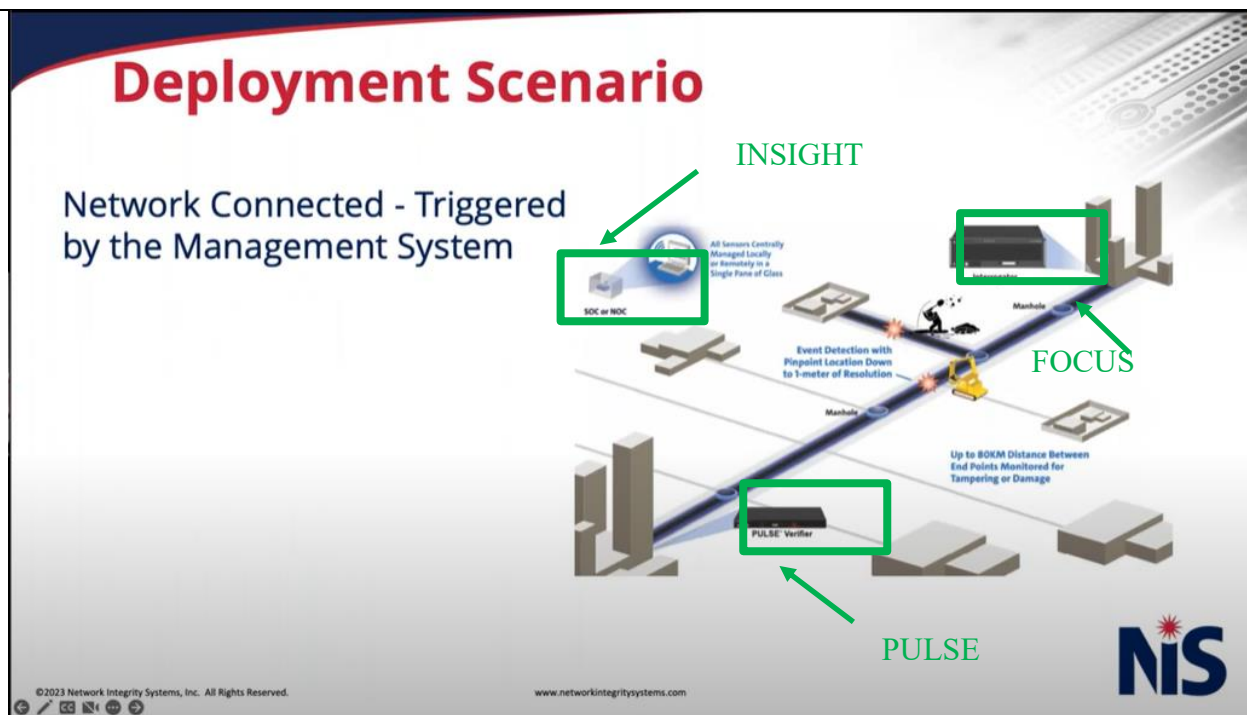
The NIS products have a fiber disturbance actuator to cause at least one disturbance of a portion of the optical fiber at a predetermined location thereon where said at least one disturbance is characteristic of the event to be monitored.

The NIS PULSE Sensor Verification System (hereinafter "PULSE") is a device (e.g., a fiber disturbance actuator) that causes at least one disturbance of a portion of the optical fiber at a predetermined location thereon.



(Available at: 16:15-16:48 FOSA Webinar)

US Patent No.: 11,515,940 vs. *Network Integrity System's Products*

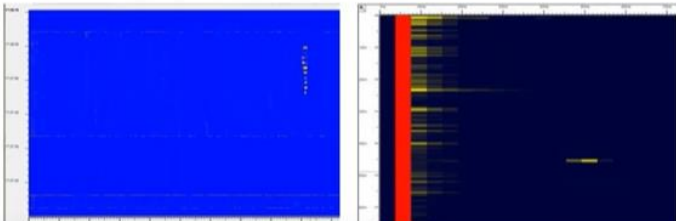


(Predetermined location: Available at: 19:55-20:30 FOSEA Webinar)

PULSE's at least one disturbance is characteristic of the event to be monitored.

The PULSE™ Sensor Verification System

- Precise, Repeatable results

Frequency	Amplitude	Duration	Pattern
			

NIS

©2023 Network Integrity Systems, Inc. All Rights Reserved. www.networkintegritysystems.com

(Available at: 16:50-19:38 FOSA Webinar)

Additionally, The NIS AFFIRM Automated Sensor Verification System (hereinafter “AFFRIM”) is a device (e.g., a fiber disturbance actuator) that causes at least one disturbance of a portion of the optical fiber at a predetermined location thereon.

US Patent No.: 11,515,940 vs. Network Integrity System's Products



The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading INTERCEPTOR™ Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our INSIGHT™ Alarm Management and Response software, conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the CNSI 7003 requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards. Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.

INTERCEPTOR™ AFFIRM Technical Specifications

ELECTRICAL

Power Input	100/240V AC, 60/50 Hz
Power Supply	Single or Dual Internal, Replaceable
Power Supply Connector	IEC C14 3-position
Operating Power	15 Watts
Maximum Power	17 Watts
Power Factor	0.5
Heat Dissipation Normal	52 Btu
Heat Dissipation Maximum	58 Btu

ENVIRONMENTAL

Operating Temperature	0°C - 45°C
Storage Temperature	-10°C - 50°C
Operating Humidity	20%-80% Non-Condensing

PHYSICAL

Installation	19" Rack Mount (1RU)
Dimensions (in)	1.75 x 17.0 x 14.5
Dimensions (mm)	45 x 432 x 368
Weight (lbs)	15
Weight (kg)	6.8

REMOTE MANAGEMENT

Console Port	RS-232 Serial
Network (Ethernet SFP)	1000Base-T SFP module included
Protocols	HTTPS

OPTICAL SPECIFICATIONS

Optical Connection (in/out)	LC/APC Duplex
Ports (in/out)	4 or 8
Insertion Loss (shutter open)	80dB typical
Insertion Loss (shutter closed)	1 dB max

INDUSTRY CERTIFICATIONS

UL, FCC Part 15, IEC Class 1, CDRH Class 1
CE Rated and Certified

AFFIRM is designed such that, if the system loses power, the shutters move to the closed position so that INTERCEPTOR monitoring of the network is maintained.

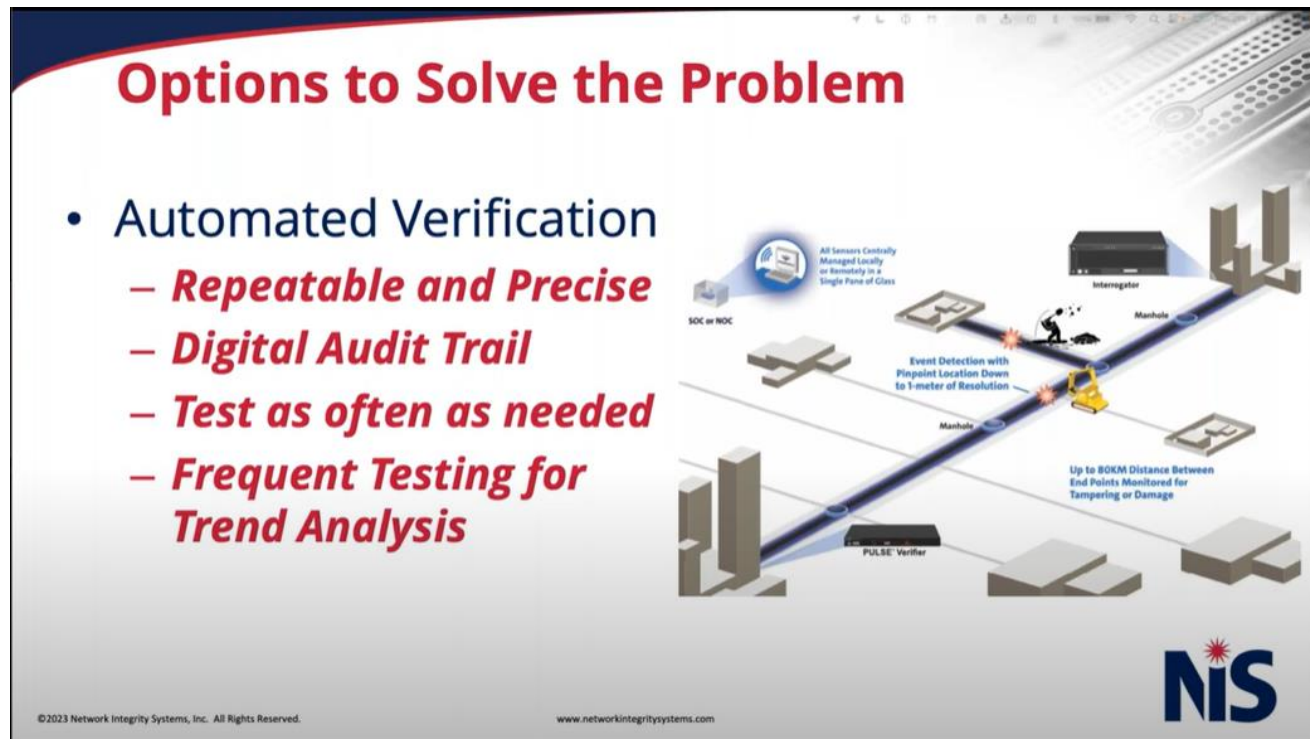
For specifications on all other products and extended warranty and support plans, please refer to our website at www.networkintegritysystems.com

(Available at: AFFIRM Product Specifications)

[9][b][2]
repeatedly
operating the fiber
disturbance
actuator;

The NIS products repeatedly operate the fiber disturbance actuator.

PULSE is repeatedly operated.



(Available at: 15:00 – 16:15 FOSA Webinar)

FOCUS

How does PULSE™ work?

The innovative PULSE solution creates a unique heartbeat on the FOCUS sensor to allow detection of any type of change in the state of the sensor itself, thereby verifying that it is always operating as commissioned. Any variation in or lack of heartbeat is an indication that the system's state of detection has changed, or been altered, and should be investigated.



PULSE

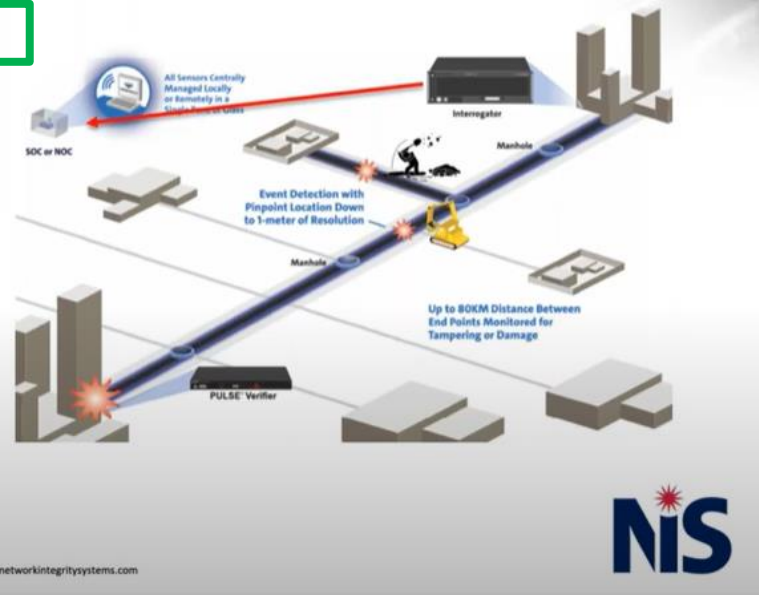


(Available at: PULSE Brochure)

Deployment Scenario

Scheduled in PULSE Firmware

- *MS knows the schedule and expects an event*
- *PULSE executes the disturbance*
- *Interrogator detects the disturbance*
- *MS confirms that Event was detected*
- *If Event is not detected at scheduled time, MS Alarms*



(Available at: 23:00 – 24:40 FOSA Webinar)

US Patent No.: 11,515,940 vs. Network Integrity System's Products

Additionally, AFFIRM is repeatedly operated.

INTERCEPTOR™ AFFIRM **Automated Sensor Verification System**

Revolutionizing Alarmed PDS Testing with Automated Compliance for CNSSI 7003 Standards

HOW IT WORKS

The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading [INTERCEPTOR™ Alarmed Carrier PDS solution](#). Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our [INSIGHT™ Alarm Management and Response software](#), conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the [CNSSI 7003](#) requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards.

Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.



FEATURES & BENEFITS

PRODUCT SPECIFICATIONS

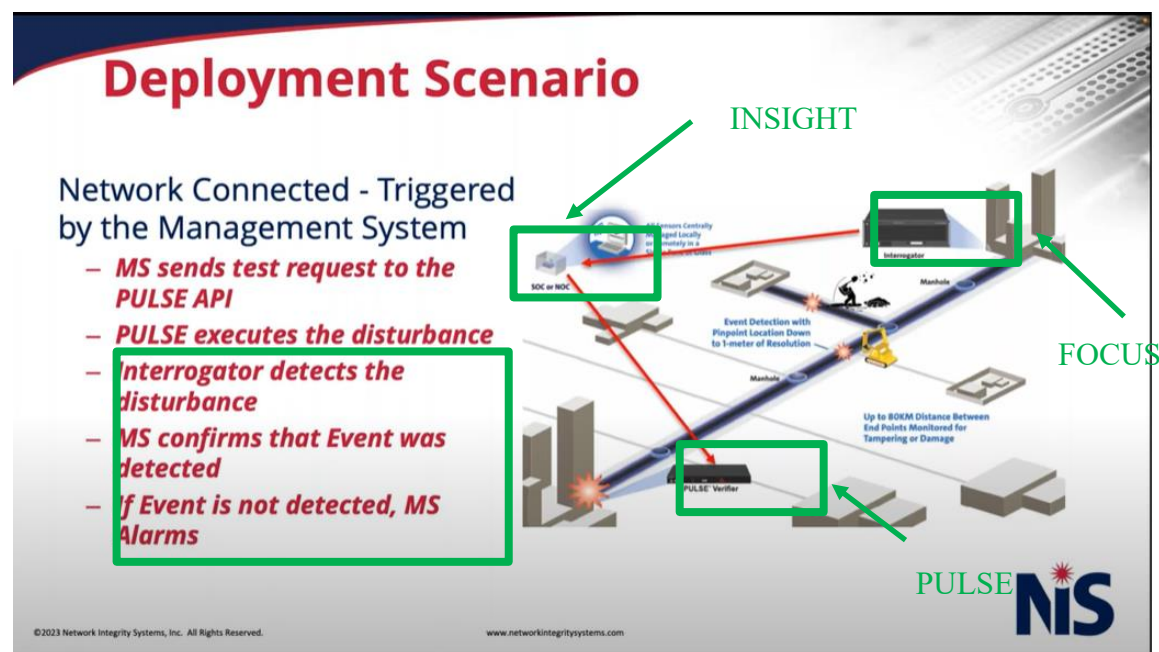
- ✓ **Automated Testing and Reduced Manual Oversight:** Automatically conducts periodic testing of the INTERCEPTOR™ Alarmed Carrier PDS system, minimizing the need for labor-intensive, manual testing processes.
- ✓ **Seamless Integration:** Works with INSIGHT™ Alarm Management and Response software for automated zone testing.
- ✓ **Operational Integrity Validation and Improved Security:** Verifies the functionality of sensing cables to ensure optimal performance.
- ✓ **Compliance Assurance:** Meets CNSSI 7003 standards for zone verification testing.
- ✓ **Audit Trail Documentation:** INSIGHT generates detailed records of completed inspections and tests.

(Available at: AFFIRM Product Page)

	<p>The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading INTERCEPTOR™ Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our INSIGHT™ Alarm Management and Response software, conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the CNSSI 7003 requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards. Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.</p> <p>(Available at: AFFIRM Product Specifications)</p>
<p>[9][b][3] analyzing the monitor signal to detect changes therein caused by said fiber disturbance actuator;</p>	<p>The NIS products analyze the monitor signal to detect changes therein caused by said fiber disturbance actuator.</p> <p>For example, as FOCUS provides the monitor signal, PULSE (e.g., fiber disturbance actuator) causes a disturbance on the optical fiber. FOCUS analyzes the monitor signal to detect changes.</p> <div data-bbox="609 732 1743 1377"> <p>Deployment Scenario</p> <p>Network Connected - Triggered by the Management System</p> <ul style="list-style-type: none"> – MS sends test request to the PULSE API – PULSE executes the disturbance – Interrogator detects the disturbance – MS confirms that Event was detected – If Event is not detected, MS Alarms <p>INSIGHT</p> <p>FOCUS</p> <p>PULSE NIS</p> <p>©2023 Network Integrity Systems, Inc. All Rights Reserved. www.networkintegritysystems.com</p> </div> <p>(Available at: FOSA Webinar 19:55 – 23:00)</p>

When expected changes in response to said fiber disturbance actuator are not detected, the NIS products actuate a warning that the detection system is not properly operating.

When expected changes in response to PULSE are not detected, FOCUS actuates a warning that the detection system is not properly operating. For example, if expected changes in response to PULSE are not detected, FOCUS detects the disturbance and actuates a warning that is provided to INSIGHT to verify whether the expected changes in response to PULSE are not detected. If the expected changes in response to PULSE are verified to not be detected, INSIGHT provides an alarm.



(Available at: FOSA Webinar 19:55 – 23:00)

How does PULSE™ work?

FOCUS

The innovative PULSE solution creates a unique heartbeat on the FOCUS sensor to allow detection of any type of change in the state of the sensor itself, thereby verifying that it is always operating as commissioned. Any variation in or lack of heartbeat is an indication that the system's state of detection has changed, or been altered, and should be investigated.



PULSE



(Available at: PULSE Brochure)

As another example, as FOCUS provides the monitor signal, AFFIRM (e.g., fiber disturbance actuator) causes a disturbance on the optical fiber. FOCUS analyzes the monitor signal to detect changes. When expected changes in response to AFFIRM are not detected, FOCUS actuates a warning that the detection system is not properly operating. For example, if expected changes in response to AFFIRM are not detected, FOCUS detects the disturbance and actuates a warning that is provided to INSIGHT to verify whether the expected changes in response to AFFIRM are not detected. If the expected changes in response to AFFIRM are verified to not be detected, INSIGHT provides an alarm.

The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading INTERCEPTOR™ Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our INSIGHT™ Alarm Management and Response software, conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the CNSSI 7003 requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards. Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.

(Available at: Affirm Product Specifications)

HOW IT WORKS

The INTERCEPTOR™ AFFIRM Automated Sensor Verification System is an integral component of the industry-leading INTERCEPTOR^{NX} Alarmed Carrier PDS solution. Engineered to automate the essential periodic testing of the system, INTERCEPTOR AFFIRM seamlessly integrates with our INSIGHT™ Alarm Management and Response software, conducting automatic tests for each zone without any human intervention. Its primary purpose is to validate the operational integrity of the sensing cables employed by the INTERCEPTOR system. This functionality meets the CNSSI 7003 requirement for zone verification testing. By automating this testing process, INTERCEPTOR AFFIRM significantly minimizes the need for manual oversight, streamlining operations while ensuring compliance with rigorous security standards.

Additionally, INSIGHT generates a comprehensive audit trail for periodic inspections, providing clear evidence that all required testing has been completed.

**FEATURES & BENEFITS****PRODUCT SPECIFICATIONS**

- ✓ **Automated Testing and Reduced Manual Oversight:** Automatically conducts periodic testing of the INTERCEPTOR™ Alarmed Carrier PDS system, minimizing the need for labor-intensive, manual testing processes.
- ✓ **Seamless Integration:** Works with INSIGHT™ Alarm Management and Response software for automated zone testing.
- ✓ **Operational Integrity Validation and Improved Security:** Verifies the functionality of sensing cables to ensure optimal performance.
- ✓ **Compliance Assurance:** Meets CNSSI 7003 standards for zone verification testing.
- ✓ **Audit Trail Documentation:** INSIGHT generates detailed records of completed inspections and tests.

(Available at: AFFIRM Product Page)

US Patent No.: 11,515,940 vs. Network Integrity System's Products

	Requirement	Solution
	Alarm System Approval and Functionality	INTERCEPTOR has been approved for PDS deployments across all military branches, government agencies, and defense contractors CONUS & OCONUS since 2003.
	Monitoring & Response	INTERCEPTOR NX integrates with INSIGHT alarm management software for centralized, remote monitoring, locally or worldwide. INSIGHT enforces SOPs, enabling a 15-minute alarm response.
	Testing and Maintenance	INTERCEPTOR NX meets PDS alarm verification requirements with AFFIRM, automating daily or weekly checks on a user-defined schedule.
	Standard Operating Procedures (SOP)	The INSIGHT Alarm Response and Management System utilizes customizable SOP's for each zone being monitored.

US Patent No.: 11,515,940 vs. *Network Integrity System's Products*

	<p>The CORA evaluates system security, including Alarmed PDS. While checklists vary, key areas typically assessed for CNSSI 7003 compliance include:</p> <ol style="list-style-type: none"> 1. Alarm System Approval and Functionality <ul style="list-style-type: none"> ◦ Confirm that the alarm system and sensors are approved by the relevant COMSEC and/or physical security authorities. ◦ Ensure the alarm system is integrated into an Intrusion Detection System (IDS) that meets Department of Defense (DoD) requirements. 2. Monitoring and Response <ul style="list-style-type: none"> ◦ Verify that alarm signals are transmitted to a continuously monitored station staffed by authorized personnel. ◦ Ensure security personnel can respond to any attempted penetration within 15 minutes of detection. 3. Testing and Maintenance <ul style="list-style-type: none"> ◦ Conduct regular functionality tests of the PDS alarm system, at least weekly, to ensure optimal performance. ◦ Maintain detailed records of all tests, inspections, and maintenance activities. 4. Standard Operating Procedures (SOP) <ul style="list-style-type: none"> ◦ Develop and maintain an SOP that includes procedures for: <ul style="list-style-type: none"> ▪ Verifying alarm functionality and performance. ▪ Responding to alarms within the specified timeframe. ▪ Inspecting the PDS to determine the cause of alarms. ▪ Defining actions to be taken regarding the termination of transmission. ▪ Initiating investigations of actual intrusion attempts. <p>(Available at: https://www.networkintegritysystems.com/cora-facts (hereinafter “CORA Facts”))</p>
<p>[9][c] wherein the optical fiber includes an input fiber length isolating the fiber disturbance actuator from the detection system.</p>	<p>The NIS products are installed such that the optical fiber includes an input fiber length isolating the fiber disturbance actuator from the detection system. For example, Distributed Acoustic Sensing (DAS) uses, <i>inter-alia</i>, reflection techniques to detect changes (e.g., in the monitor signal).</p> <p>“The fiber being monitored includes or has connected as part an input fiber length for isolation from the monitoring device of any connector reflections caused by connection of the fiber disturbance actuator. In many cases this also includes an exit fiber which again acts for isolation purposes. This isolation provided by the inlet and exit fiber portions is particularly important in the systems which rely on reflection techniques where</p>

any such reflections can be orders of magnitude greater than the signals to be detected.” See Col. 4, lines 26-35 of US 11,515,940.

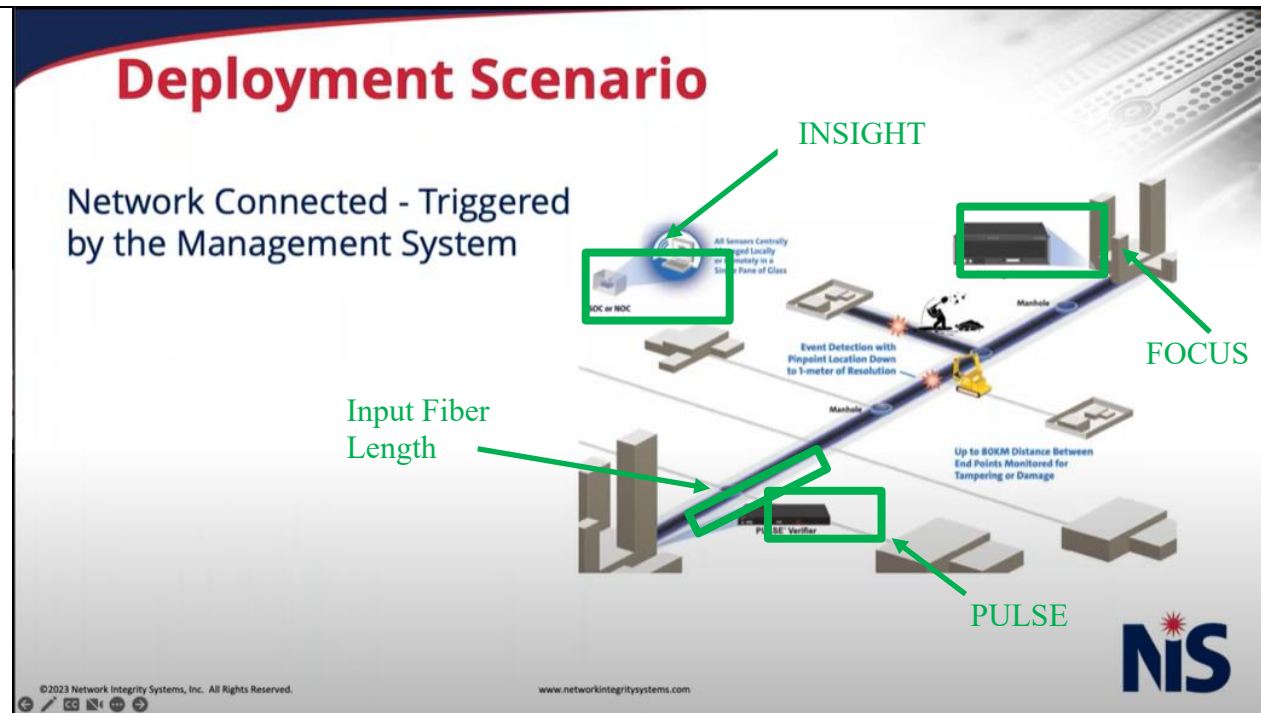
6. Summary

INTERCEPTOR FOCUS utilizes state-of-the-art Distributed Acoustic Sensing (DAS) technology to provide long-range capability and pinpoint location of any physical disturbance to your classified communications cable up to 40km in length. The system continuously monitors the entire cable and pathway to immediately detect and report the most sophisticated intrusion attempts, or even the subtlest tampering conducted for the purposes of data theft (eavesdropping) or denial of service.

Fully integrated with our proprietary CyberSecure software platform, the INTERCEPTOR FOCUS solution will centrally monitor and continually automate CNSSI 7003 required inspections and customized Standard Operating Procedures (SOP) for immediate response to any threat to your classified network. The INTERCEPTOR FOCUS can be rapidly deployed in new or existing network infrastructure to rapidly provide security to your physical layer.



(Available at: FOCUS Whitepaper)



(Available at: 19:55-20:30 FOSA Webinar)

Exhibit 9

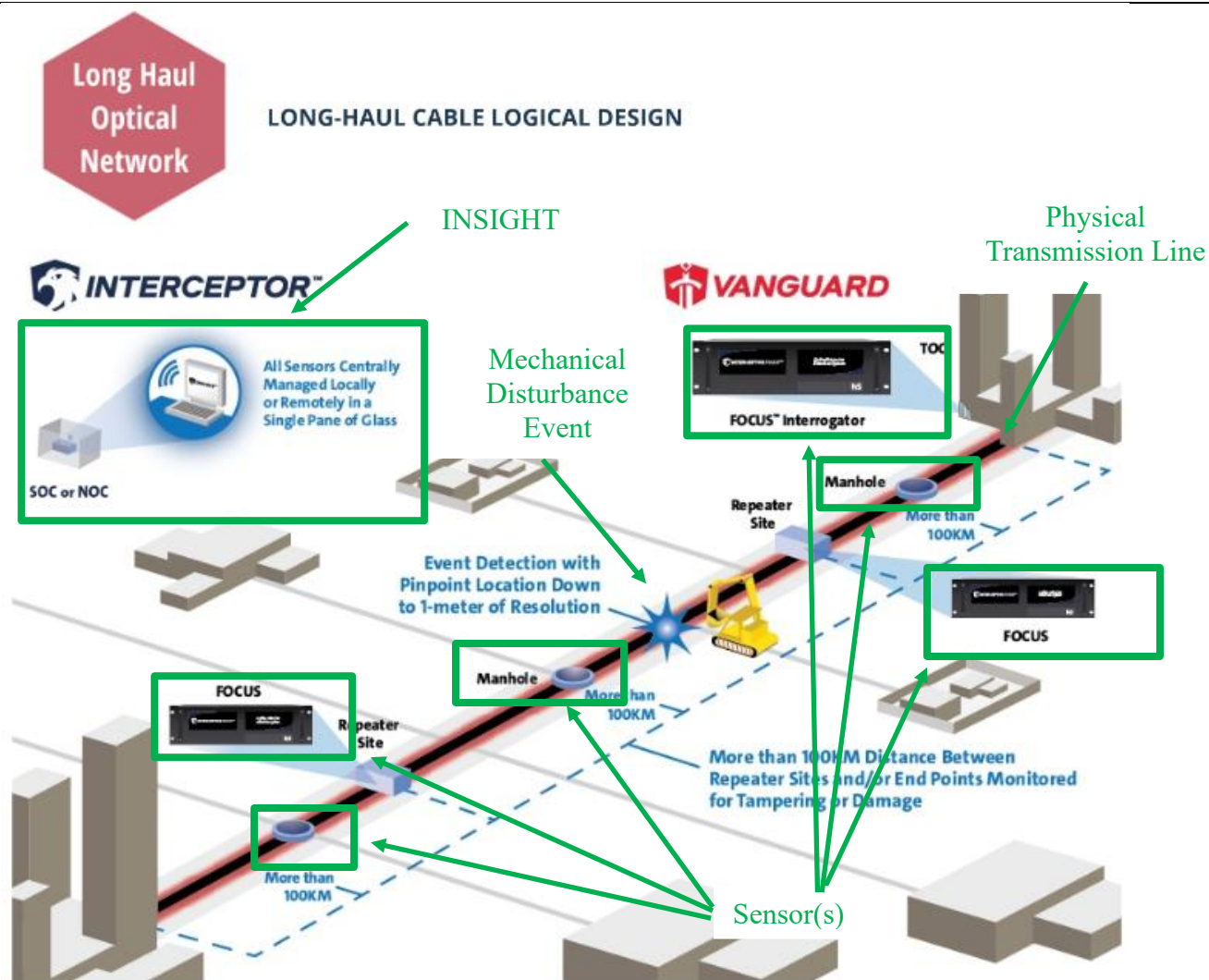
Claim	Support for Infringing Product(s) [Annotations in Green]
Claim 14	
<p>[14] One or more non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause operations comprising:</p>	<p>Network Integrity Systems (NIS) sells products that include one or more non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause operations.</p> <p>For example, NIS's INSIGHT runs on a computing device having one or more non-transitory computer-readable media storing instructions that, when executed by one or more processors, that cause operations.</p> <div data-bbox="674 493 1633 735">  <p>The logo for INSIGHT Alarm Response & Management System. It features a stylized black shield icon on the left containing a white target symbol. To the right of the icon, the word "INSIGHT" is written in a large, bold, italicized sans-serif font, followed by a trademark symbol (TM). Below "INSIGHT", the words "Alarm Response & Management System" are written in a smaller, bold, sans-serif font.</p> </div> <p>INSIGHT™ is an advanced alarm response and management application that integrates with NIS sensor solutions and other systems for comprehensive, efficient security management.</p> <hr/> <p>With INSIGHT™, you gain real-time visibility into your security posture and receive instant alarms and notifications, allowing you to stay informed and take immediate action when needed. This user-friendly interface, often called a "single pane of glass," consolidates all aspects of your security infrastructure, streamlining operations and enhancing your ability to respond quickly to security incidents.</p> <p>Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.</p> <p>For clients with existing alarm response infrastructure, we offer INTERLINK™, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.</p> <p>With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.</p> <p>INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.</p> <p>In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.</p> <p>(Available at: https://www.networkintegritysystems.com/INSIGHT (hereinafter "INSIGHT Product Page"))</p>

US Patent No.: 11,388,181 vs. Network Integrity System's Products

	<p>Licensing:</p> <p>In some cases, the purchase price of NIS products includes a license for INSIGHT™ or INTERLINK™ software. The license allows for the installation and operation of the current (as of installation date) production version of the described software. It does not cover future software upgrades or non-security-related patches. Software security-related patches for the licensed software version will be provided under this license for a period of three (3) years from date of delivery.</p> <p>NIS offers a Warranty and Support Program (WSP) that provides additional licensing for patches and/or version upgrades released during the WSP term, depending on the purchased options. NIS will never disable your software if you don't have a WSP subscription, but support will be limited to software security-related issues. For WSP program details, please refer to the Warranty and Support Program page.</p> <p>Customers without a WSP subscription can obtain a license for the latest software versions by purchasing a one-year WSP subscription at the Premium level.</p> <div style="border: 2px solid green; padding: 10px;"> <p>Minimum System Requirements:</p> <table border="1"> <tr> <td>Operating System</td><td>Windows – Windows 11; Windows Server 2019 or newer Linux – CentOS; Debian; Fedora; Ubuntu</td></tr> <tr> <td>CPU</td><td>64 bit, multi-core at 2.4 GHz</td></tr> <tr> <td>RAM¹</td><td>8 GB – 16 GB</td></tr> <tr> <td>Storage²</td><td>100 GB</td></tr> <tr> <td>Ports & Protocols³</td><td>Services = TCP 4000; HTTP= TCP 80; HTTPS= TCP 443</td></tr> </table> <p>Software Requirements: Docker Engine⁴ – Version 20.10.25 or newer 7-ZIP (Both Windows & Linux)</p> <p>¹May need to increase when connecting more than 50 devices to INSIGHT.</p> <p>²Storage capacity dependent on customer limitations. Above is the minimum recommendation for storage of logs (worker, server, install logs), Alarm Reports (and attachments), user profiles, Areas (with imagery), and Dashboards.</p> <p>³HTTP/HTTPS ports can be configured to a different TCP port if needed during installation of INSIGHT. Ports 80 and 443 are default.</p> <p>⁴If Docker Desktop is being used, the customer needs to follow requirements for running Docker Desktop within their organization.</p> </div> <p>(Available at: https://hub.networkintegritysystems.com/hubfs/INSIGHT%20Specification%20Sheet%20V5.pdf (hereinafter “INSIGHT Technical Specifications”))</p>	Operating System	Windows – Windows 11; Windows Server 2019 or newer Linux – CentOS; Debian; Fedora; Ubuntu	CPU	64 bit, multi-core at 2.4 GHz	RAM ¹	8 GB – 16 GB	Storage ²	100 GB	Ports & Protocols ³	Services = TCP 4000; HTTP= TCP 80; HTTPS= TCP 443
Operating System	Windows – Windows 11; Windows Server 2019 or newer Linux – CentOS; Debian; Fedora; Ubuntu										
CPU	64 bit, multi-core at 2.4 GHz										
RAM ¹	8 GB – 16 GB										
Storage ²	100 GB										
Ports & Protocols ³	Services = TCP 4000; HTTP= TCP 80; HTTPS= TCP 443										
<p>[14][a][1] obtaining, from multiple sensors associated with a physical transmission line, sensor data</p>	<p>INSIGHT obtains sensor data, from multiple sensors (e.g., NIS FOCUS, manhole cover sensors, etc.) associated with a physical transmission line (e.g., an optical fiber line), sensor data related to a mechanical disturbance event on the physical transmission line.</p>										

US Patent No.: 11,388,181 vs. Network Integrity System's Products

related to a mechanical disturbance event on the physical transmission line,



LONG-HAUL CABLE CYBER PROTECTION

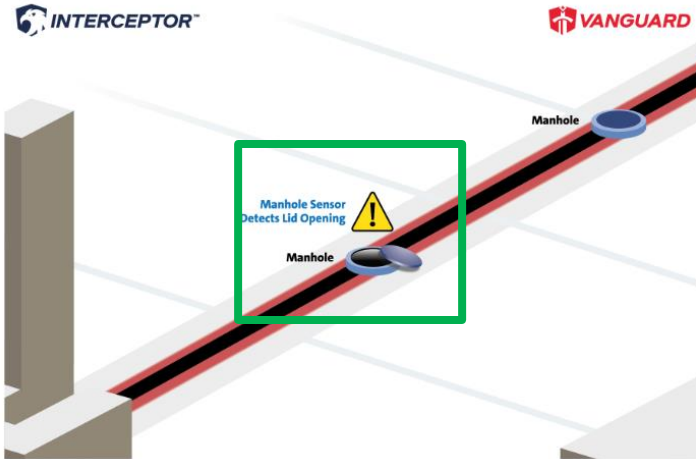
Cable downtime is costly but monitoring thousands of kilometers of cable is challenging. Distributed Acoustic Sensing technology (DAS) allows you to confidently monitor your cables in real time and detect risks to within 1 meter of resolution. Using DAS technology, our FOCUS NX system monitors a single strand of SM cable in long-haul cables and pathways) and pinpoints the exact location of events such as impact to conduit or tampering with the cable. This reduces the risk of downtime or data security breaches. Through daisy-chaining practices, the protection of any cable length can be achieved.

The FOCUS NX seamlessly integrates with our INSIGHT Alarm Response Management software, giving you a comprehensive view of your security posture. This integration allows for effortless monitoring and management of your security systems.

The U.S. Government and Military uses INTERCEPTOR FOCUS NX to protect their classified network infrastructure, and the VANGUARD FOCUS NX is available for the commercial market to protect their network infrastructure.

(Available at: Slide 86 of <https://prezi.com/view/ofYkUmoJdl3b1X4WlETk/?hsCtaTracking=0b289cce-8dbb-46ec-8647-7885d8c1659e%7Cc64c2891-b4f8-4165-b5f4-d5d179a8f53f> (hereinafter "Prezi"))

US Patent No.: 11,388,181 vs. Network Integrity System's Products



While our INTERCEPTOR or VANGUARD products actively protect cabling system assets, areas of likely ingress, such as maintenance manholes or other maintenance points, are often unprotected and should be monitored to detect unauthorized entry as a second layer of protection.

Our Maintenance Hole Protection System was designed to provide real time monitoring of network infrastructure access points such as maintenance-holes and hand-holes over long distances utilizing zero-power fiber optic sensors. Each sensor can detect Open/Close conditions, fiber loss (dB), and fiber cuts at each sensor location.

(Available at: Prezi, slide 87)

Q. How does Interceptor™ detect an intrusion into a fiber optic cable?

A: Interceptor launches a monitoring signal into a pair of fibers of the optical cable being protected, which turns the entire cable (up to 144 fibers) into a sensor. When any component of the cable is abnormally handled, for instance during an intrusion attempt, the monitored fibers sense the disturbance and Interceptor reports the event.

(Available at: <https://www.networkintegritysystems.com/blog/2010/01/22/fact-friday-1> (hereinafter “Fact Friday”))

US Patent No.: 11,388,181 vs. Network Integrity System's Products



INSIGHT™ is an advanced alarm response and management application that integrates with NIS sensor solutions and other systems for comprehensive, efficient security management.

With **INSIGHT™**, you gain real-time visibility into your security posture and receive instant alarms and notifications, allowing you to stay informed and take immediate action when needed. This user-friendly interface, often called a "single pane of glass," consolidates all aspects of your security infrastructure, streamlining operations and enhancing your ability to respond quickly to security incidents.

(Available at: INSIGHT Product Page)



Product Specifications

Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.

For clients with existing alarm response infrastructure, we offer INTERLINK™, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.

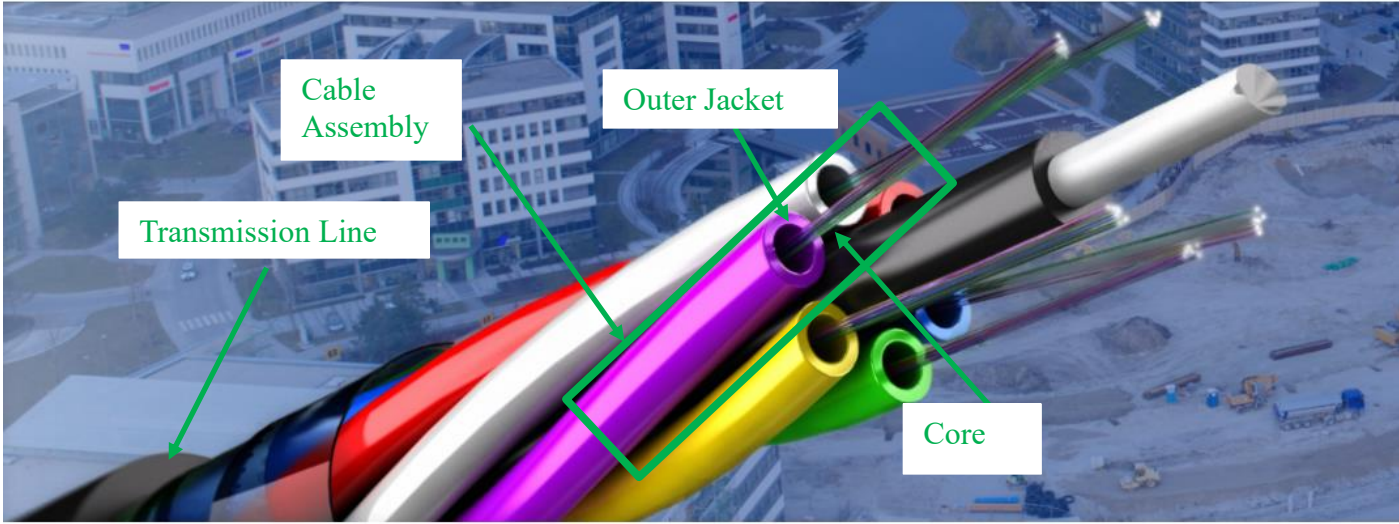
With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.

INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.

In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.

(Available at: INSIGHT Technical Specifications)

US Patent No.: 11,388,181 vs. *Network Integrity System's Products*

<p>[14][a][2] wherein the physical transmission line comprises one or more cable assemblies, the one or more cable assemblies comprising a cable assembly having an outer jacket and a core;</p>	<p>INSIGHT receives sensor data related to mechanical disturbance events on the physical transmission line (e.g., the optical fiber line). The physical transmission line comprises one or more cable assemblies, where the one or more cable assemblies comprise a cable assembly having an outer jacket and a core.</p> <p>See <i>supra</i> [14]-[14][a][1];</p>  <p>(Available at: https://www.networkintegritysystems.com/interceptor-products-3 (hereinafter “Interceptor Product Page”))</p>
<p>[14][b][1] determining a type of the mechanical disturbance event on the physical transmission</p>	<p>INSIGHT determines a type of the mechanical disturbance event on the physical transmission line based on one or more mechanical disturbance event signatures.</p>

US Patent No.: 11,388,181 vs. Network Integrity System's Products

line based on one or more mechanical disturbance event signatures,

Q. How does Interceptor™ detect an intrusion into a fiber optic cable?

A: Interceptor launches a monitoring signal into a pair of fibers of the optical cable being protected, which turns the entire cable (up to 144 fibers) into a sensor. When any component of the cable is abnormally handled, for instance during an intrusion attempt, the monitored fibers sense the disturbance and Interceptor reports the event.

(Available at: Fact Friday)



FEATURES & BENEFITS



- Long-Haul Alarmed Carrier System
- Monitors events along cables up to 100km in length
- Capable of detecting conduit contact, cable manipulation, and other activity near the cable path such as digging or drilling *
- Identifies, within as close as 1 meter, the location of the event
- Detects and locates simultaneous events at multiple locations
- No bandwidth bottlenecks or degradation of network performance
- NIS offers a dual-system solution combined with our Machine Learning that offers a robust level of both redundancy and resiliency, delivering the most uptime possible for critical security requirements.

**Depending on cable type and deployment environment*

Click Below to Learn More About
INTERCEPTOR FOCUS NX

[https://
www.networkintegritysystems.com
/interceptor-products:3](https://www.networkintegritysystems.com/interceptor-products:3)

(Available at: Prezi slide 133)

ALARM RESPONSE MANAGEMENT

SENTINEL integrates with our INSIGHT Alarm Response Management software, offering a comprehensive, real-time view of your security posture. In another industry first, INSIGHT's Event Processor takes event information from multiple sensors and other devices and analyzes the order and severity to provide intelligent alarms based on more than a single factor. SENTINEL scales effortlessly from single to multi-site installations to meet any security need.

(Available at: <https://www.networkintegritysystems.com/sentinel-std> (hereinafter "Sentinel Product Page"))

HOW IT WORKS

SENTINEL FOCUS^{NX} employs Distributed Acoustic Sensing (DAS) technology to monitor optical fibers that are covertly buried and/or fence or wall-mounted along borders and facility perimeters. When physical intrusions create vibrations that reach the optical fibers, the interrogator discerns changes in the light. Then, machine learning-based AI instantly and simultaneously classifies the type of intrusion, such as walking, tunneling, climbing or fence cutting, and pinpoints the location of the intrusion with an accuracy of up to 1-meter resolution.

ALARM RESPONSE MANAGEMENT

SENTINEL FOCUS^{NX} integrates with our INSIGHT Alarm Response Management software, offering a comprehensive, real-time view of your security posture. In another industry first, INSIGHT's Event Processor takes event information from multiple sensors and other devices and analyzes the order and severity to provide intelligent alarms based on more than a single factor. SENTINEL scales effortlessly from single to multi-site installations to meet any security need.

(Available at: <https://www.networkintegritysystems.com/sentinel-focus> (hereinafter "Sentinel FOCUS Product Page"))

US Patent No.: 11,388,181 vs. *Network Integrity System's Products*

	<p>INTERCEPTOR FOCUS^{NX} is our next generation long-haul sensing technology that immediately detects and identifies any threat to your classified network infrastructure, while pinpointing its exact location.</p> <p>The Network Integrity Systems INTERCEPTOR FOCUS^{NX} Optical Intrusion Detection System utilizes Distributed Acoustic Sensing (DAS) technology to monitor long-haul cables and pathways, up to 100km per device, with pinpoint location of any disturbances to your network communications cables, to 1-meter of resolution. INTERCEPTOR FOCUS^{NX} utilizes Phase DAS technology with an improved noise floor and machine learning for accurate event detection.</p> <p>(Available at: https://hub.networkintegritysystems.com/hubfs/INTERCEPTOR%20FOCUS%20NX%20Spec%20sheet%20V2%201.pdf (hereinafter "Interceptor Focus NX Specification Sheet"))</p> <p>The INTERCEPTOR Optical Network Security System has Information Assurance Analytics embedded in its protection schema and logical design. INTERCEPTOR records and logs detailed threat information and the associated alarms, allowing IA personnel to perform thorough analysis to identify emerging trends, as well as to optimize the protection provided by the INTERCEPTOR.</p> <p>In addition, the intrusion signatures used by the INTERCEPTOR to identify threats to the network are continuously updated and expanded to ensure that <i>any</i> threat to the physical network can be identified and detected <i>before</i> the network is degraded or National Security Information is compromised.</p> <p>(Available at: https://www.networkintegritysystems.com/blog/2011/11/09/interceptor-provides-information-assurance-analytics (hereinafter "Information Assurance Article"))</p>
[14][b][2] the one or more mechanical disturbance event signatures being derived from one or more prior mechanical	<p>INSIGHT determines a type of the mechanical disturbance event on the physical transmission line based on one or more mechanical disturbance event signatures, where the one or more mechanical disturbance event signatures [are] derived from one or more prior mechanical disturbance events.</p>

disturbance
events,

Q. How does Interceptor distinguish between true intrusions and everyday events that may cause nuisance alarms?

A: Interceptor incorporates a patented Smart Filtering™ technology to “auto-configure” itself and learn a baseline of normal, routine, benign, non-threatening affects upon the cable system. These normal events are thereafter ignored resulting in the elimination of false alarms.

(Available at: Fact Friday)



INSIGHT™ is an advanced alarm response and management application that integrates with NIS sensor solutions and other systems for comprehensive, efficient security management.

With **INSIGHT™**, you gain real-time visibility into your security posture and receive instant alarms and notifications, allowing you to stay informed and take immediate action when needed. This user-friendly interface, often called a "single pane of glass," consolidates all aspects of your security infrastructure, streamlining operations and enhancing your ability to respond quickly to security incidents.

Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.

For clients with existing alarm response infrastructure, we offer **INTERLINK™**, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.

With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.

INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.

In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.

(Available at: INSIGHT Product Page)

6. Artificial Intelligence in Distributed Acoustic Sensing

Artificial Intelligence (AI) is a branch of computer science that aims to create systems capable of performing tasks that usually require human intelligence. These tasks include learning from experience, understanding natural language, recognizing patterns, and making decisions. Machine Learning (ML) is a specialized field of Artificial Intelligence (AI) that enables computer systems to learn autonomously from data and improve their performance over time without being explicitly programmed. It involves algorithms and statistical models that computers use to perform tasks by leveraging patterns and inferences. These algorithms can process vast amounts of data, identify patterns and make decisions with minimal human intervention, thereby enhancing system efficiency and accuracy.

Interpreting the vast amount of acoustic data generated by DAS systems can be complex and requires advanced analysis techniques. This is where Machine Learning (ML) comes into play. ML, a subset of artificial intelligence, allows computers to learn from and make decisions based on data. In the context of DAS, machine learning can be used to analyze the acoustic signal data for pattern recognition, anomaly detection, and predictive analysis. For example, ML algorithms can be trained on a set of data where the outcomes are known (supervised learning) to create a model that can predict the outcomes when new data is input.

right ©2023 Network Integrity Systems, Inc. All Rights Reserved. Proprietary and Confidential.

Page 5 of

Here's how it works: The ML algorithm is first trained on a dataset that includes both normal and anomalous signals. This 'training phase' allows the algorithm to understand and learn the characteristics of both types of signals. Once the algorithm is trained, it can be used to monitor real-time data from the DAS system. As new data comes in, the ML algorithm processes it and identifies whether the signals are normal or anomalous based on what it has learned.

This application of ML in DAS offers numerous benefits. It can significantly reduce the time and resources required to monitor and interpret DAS data, enabling faster and more accurate responses to potential issues. It also allows for predictive maintenance, as the ML algorithm can recognize patterns that indicate a potential future issue, allowing preventative measures to be taken before a problem occurs.

In summary, the application of machine learning in distributed acoustic sensing enables more efficient and accurate data interpretation, real-time monitoring, anomaly detection, and predictive maintenance, which can lead to significant cost savings and improved operational efficiency in many deployment scenarios.

(Available at: <https://hub.networkintegritysystems.com/hubfs/DAS%20in%20the%20Age%20of%20AI.pdf> (hereinafter "DAS in the Age of AI")

US Patent No.: 11,388,181 vs. *Network Integrity System's Products*

	<p>The INTERCEPTOR Optical Network Security System has Information Assurance Analytics embedded in its protection schema and logical design. INTERCEPTOR records and logs detailed threat information and the associated alarms, allowing IA personnel to perform thorough analysis to identify emerging trends, as well as to optimize the protection provided by the INTERCEPTOR.</p> <p>In addition, the intrusion signatures used by the INTERCEPTOR to identify threats to the network are continuously updated and expanded to ensure that <i>any</i> threat to the physical network can be identified and detected <i>before</i> the network is degraded or National Security Information is compromised.</p> <p>(Available at: Information Assurance Article)</p>
<p>[14][b][3] wherein the mechanical disturbance event is determined to be (i) a first event type in response to the first and second sensor data being similar to a first signature and (ii) a second event type in response to the first and second sensor data being similar to a second signature; and</p>	<p>INSIGHT determines a mechanical disturbance event to be (i) a first event type in response to [the] first and second sensor data being similar to a first signature and (ii) a second event type in response to the first and second sensor data being similar to a second signature.</p> <p><i>See supra</i> [14][b][1]-[14][b][2].</p>

[14][c] causing an action to be performed such that (ii) the action is a first action in response to the mechanical disturbance event being the first event type and (ii) the action is a second action in response to the mechanical disturbance event being the second event type.

INSIGHT causes an action to be performed such that (i) the action is a first action in response to the mechanical disturbance being the first event type and (ii) the action is a second action in response to the mechanical disturbance being the second event type.

See supra [14][b][1]-[14][b][2].

For example, INSIGHT would (i) generate an alarm in response to a disturbance being a non-ambient event and (ii) prevent nuisance alarms (e.g., prevent generation of an alarm) and instead simply logging the disturbance in response to an ambient event.



INSIGHT™ is an advanced alarm response and management application that integrates with NIS sensor solutions and other systems for comprehensive, efficient security management.

With **INSIGHT™**, you gain real-time visibility into your security posture and receive instant alarms and notifications, allowing you to stay informed and take immediate action when needed. This user-friendly interface, often called a "single pane of glass," consolidates all aspects of your security infrastructure, streamlining operations and enhancing your ability to respond quickly to security incidents.

Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.

For clients with existing alarm response infrastructure, we offer **INTERLINK™**, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.

With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.

INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.

In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.

(Available at: INSIGHT Product Page)

US Patent No.: 11,388,181 vs. Network Integrity System's Products

Q. How does Interceptor distinguish between true intrusions and everyday events that may cause nuisance alarms?

A: Interceptor incorporates a patented Smart Filtering™ technology to “auto-configure” itself and learn a baseline of normal, routine, benign, non-threatening affects upon the cable system. These normal events are thereafter ignored resulting in the elimination of false alarms.

(Available at: Fact Friday)

With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.

Feature Comparison (v1.1)	INSIGHT	INTERLINK
User configuration	✓	
• User	✓	
• Team	✓	
• Organization	✓	
• Custom Roles	✓	
Administrator roles for full user management	✓	
Fully customizable map/image display with path overlay	✓	
Fully customizable Dashboard display per user	✓	
Widgets library for personalized experience	✓	
Alarm notification (visual with optional audio)	✓	
Alarm investigation and reporting	✓	
Customizable alarm response procedures	✓	
Dark/Light modes	✓	✓
Bespoke event processing engine	✓	✓
Event broker (up and down stream)	✓	✓
Full logging of all activity with sortable display	✓	✓
Automated & On-Demand Zone Testing	✓	✓
Email notifications	✓	✓
Device integration management	✓	✓
Multi-device management and upgrades	✓	✓
Notifications for license renewal and upgrades	✓	✓
Flexible licensing	✓	✓
Runs on Windows or Linux platforms	✓	✓
Contextual help available on screen	✓	✓

US Patent No.: 11,388,181 vs. *Network Integrity System's Products*

	<p>(Available at: https://www.networkintegritysystems.com/INSIGHT/interlink-features-comparison (hereinafter “INSIGHT-Interlink Feature Comparison”))</p> <p>The INTERCEPTOR Optical Network Security System has Information Assurance Analytics embedded in its protection schema and logical design. INTERCEPTOR records and logs detailed threat information and the associated alarms, allowing IA personnel to perform thorough analysis to identify emerging trends, as well as to optimize the protection provided by the INTERCEPTOR.</p> <p>In addition, the intrusion signatures used by the INTERCEPTOR to identify threats to the network are continuously updated and expanded to ensure that <i>any</i> threat to the physical network can be identified and detected <i>before</i> the network is degraded or National Security Information is compromised.</p> <p>(Available at: “Information Assurance Article”)</p>
--	---

Exhibit 10

Claim	Support for Infringing Product(s) [Annotations in Green]
Claim 1	
[1] A method for managing a protective distribution system, comprising:	<p>Network Integrity Systems (NIS) sells products that manage a protective distribution system.</p> <p>The NIS INSIGHT product is an alarm response and management application (e.g., software). INSIGHT manages a protective distribution system.</p> <div style="text-align: center;">  <p>INSIGHT™ Alarm Response & Management System</p> </div> <p>INSIGHT™ is an advanced alarm response and management application that integrates with NIS sensor solutions and other systems for comprehensive, efficient security management.</p> <hr/> <p>With INSIGHT™, you gain real-time visibility into your security posture and receive instant alarms and notifications, allowing you to stay informed and take immediate action when needed. This user-friendly interface, often called a "single pane of glass," consolidates all aspects of your security infrastructure, streamlining operations and enhancing your ability to respond quickly to security incidents.</p> <p>Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.</p> <p>For clients with existing alarm response infrastructure, we offer INTERLINK™, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.</p> <p>With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.</p> <p>INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.</p> <p>In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.</p> <p>(Available at: https://www.networkintegritysystems.com/INSIGHT (hereinafter "INSIGHT Product Page"))</p>
[1][a] monitoring a	INSIGHT monitors a fiber optic information transmission line.

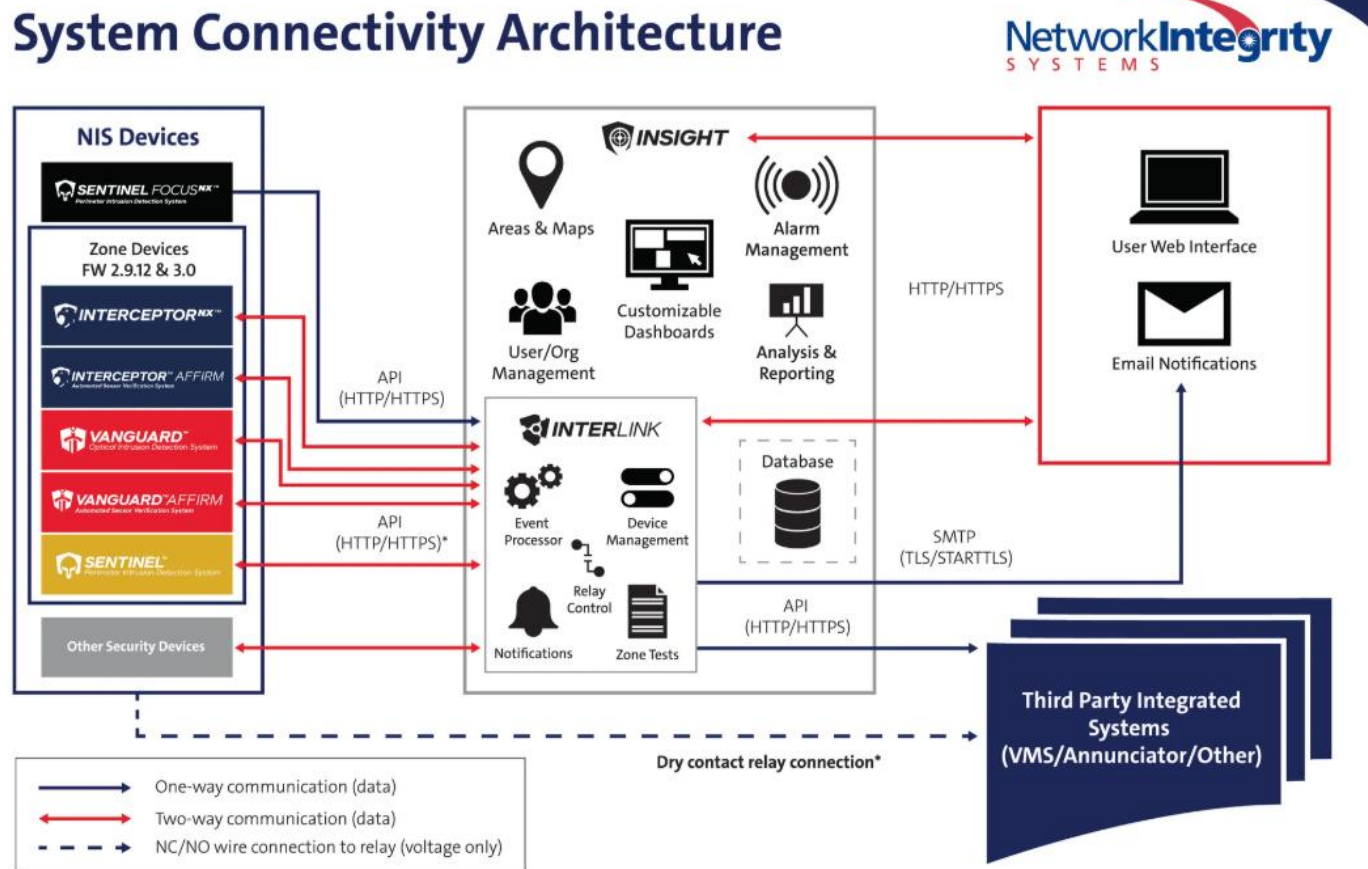
US Patent No.: 9,455,999 vs. *Network Integrity System's Products*

fiber optic
information
transmission
line;



(Available at: <https://www.networkintegritysystems.com/interceptor-products-3> (hereinafter "Interceptor Product Page"))

US Patent No.: 9,455,999 vs. Network Integrity System's Products



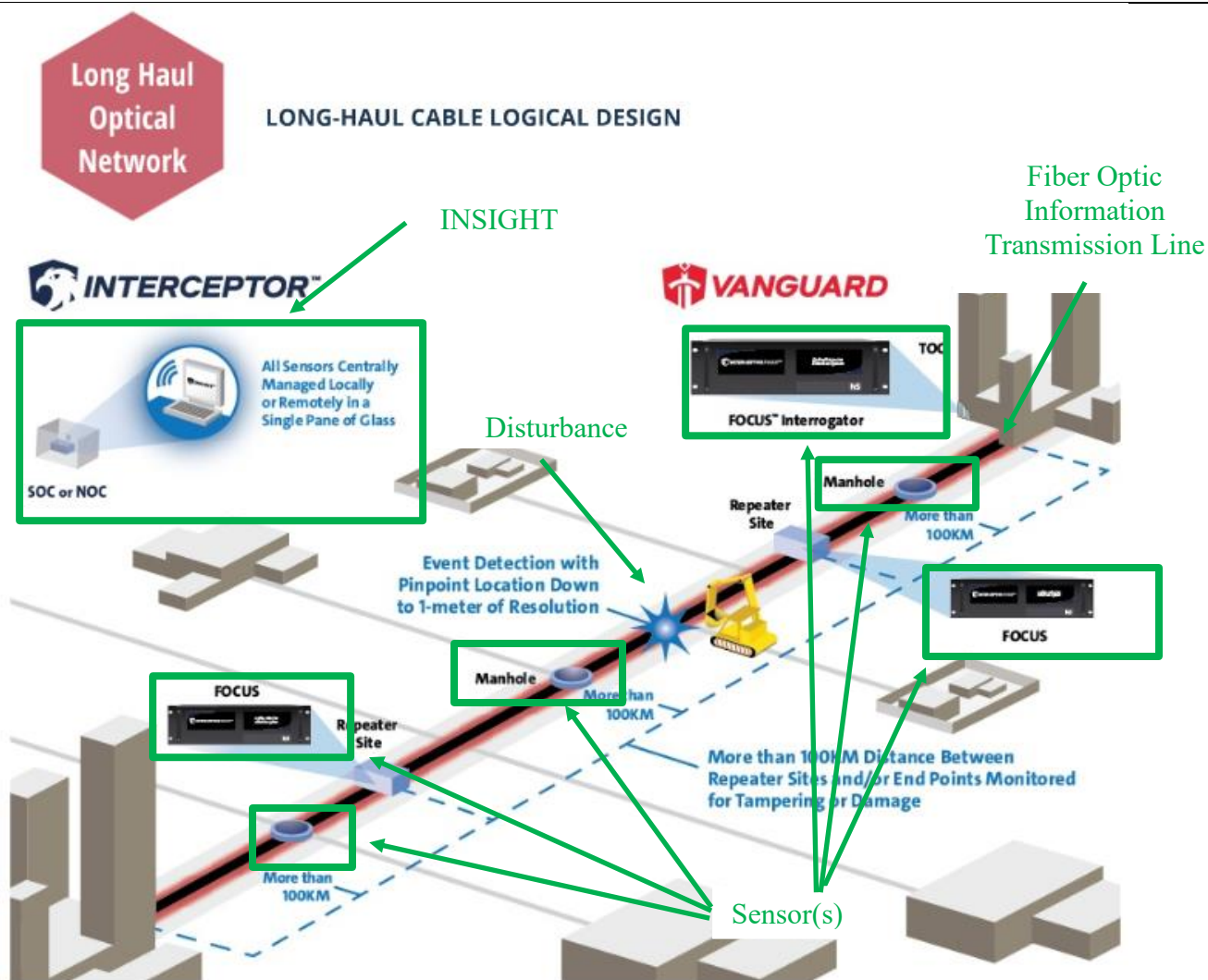
(Available at: INSIGHT Product Page)

[1][b][1]
detecting, via
one or more
sensors, a
disturbance on
the fiber optic
information

INSIGHT detects, via one or more sensors, a disturbance on the fiber optic information transmission line. For example, INSIGHT obtains sensor data, from one or more sensors (e.g., NIS FOCUS, manhole cover sensors, etc.), to detect disturbance(s) on the fiber optic information transmission line.

US Patent No.: 9,455,999 vs. Network Integrity System's Products

transmission
line,



LONG-HAUL CABLE CYBER PROTECTION

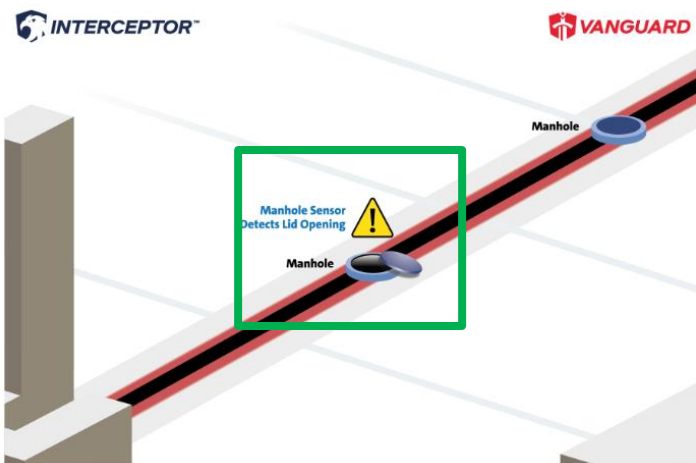
Cable downtime is costly but monitoring thousands of kilometers of cable is challenging. Distributed Acoustic Sensing technology (DAS) allows you to confidently monitor your cables in real time and detect risks to within 1 meter of resolution. Using DAS technology, our FOCUS NX system monitors a single strand of SM cable in long-haul cables and pathways) and pinpoints the exact location of events such as impact to conduit or tampering with the cable. This reduces the risk of downtime or data security breaches. Through daisy-chaining practices, the protection of any cable length can be achieved.

The FOCUS NX seamlessly integrates with our INSIGHT Alarm Response Management software, giving you a comprehensive view of your security posture. This integration allows for effortless monitoring and management of your security systems.

The U.S. Government and Military uses INTERCEPTOR FOCUS NX to protect their classified network infrastructure, and the VANGUARD FOCUS NX is available for the commercial market to protect their network infrastructure.

(Available at: Slide 86 of <https://prezi.com/view/ofYkUmoJdl3b1X4WlETk/?hsCtaTracking=0b289cce-8dbb-46ec-8647-7885d8c1659e%7Cc64c2891-b4f8-4165-b5f4-d5d179a8f53f> (hereinafter "Prezi"))

US Patent No.: 9,455,999 vs. Network Integrity System's Products



While our INTERCEPTOR or VANGUARD products actively protect cabling system assets, areas of likely ingress, such as maintenance manholes or other maintenance points, are often unprotected and should be monitored to detect unauthorized entry as a second layer of protection.

Our Maintenance Hole Protection System was designed to provide real time monitoring of network infrastructure access points such as maintenance-holes and hand-holes over long distances utilizing zero-power fiber optic sensors. Each sensor can detect Open/Close conditions, fiber loss (dB), and fiber cuts at each sensor location.

(Available at: Prezi, slide 87)

Q. How does Interceptor™ detect an intrusion into a fiber optic cable?

A: Interceptor launches a monitoring signal into a pair of fibers of the optical cable being protected, which turns the entire cable (up to 144 fibers) into a sensor. When any component of the cable is abnormally handled, for instance during an intrusion attempt, the monitored fibers sense the disturbance and Interceptor reports the event.

(Available at: <https://www.networkintegritysystems.com/blog/2010/01/22/fact-friday-1> (hereinafter “Fact Friday”))

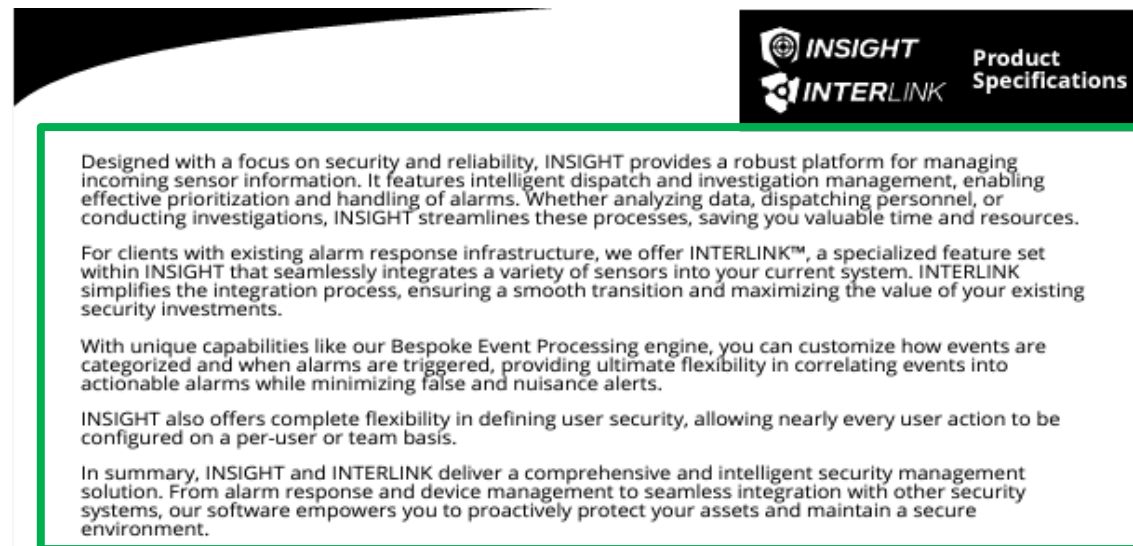
US Patent No.: 9,455,999 vs. Network Integrity System's Products



INSIGHT™ is an advanced alarm response and management application that integrates with NIS sensor solutions and other systems for comprehensive, efficient security management.

With INSIGHT™, you gain real-time visibility into your security posture and receive instant alarms and notifications, allowing you to stay informed and take immediate action when needed. This user-friendly interface, often called a "single pane of glass," consolidates all aspects of your security infrastructure, streamlining operations and enhancing your ability to respond quickly to security incidents.

(Available at: INSIGHT Product Page)

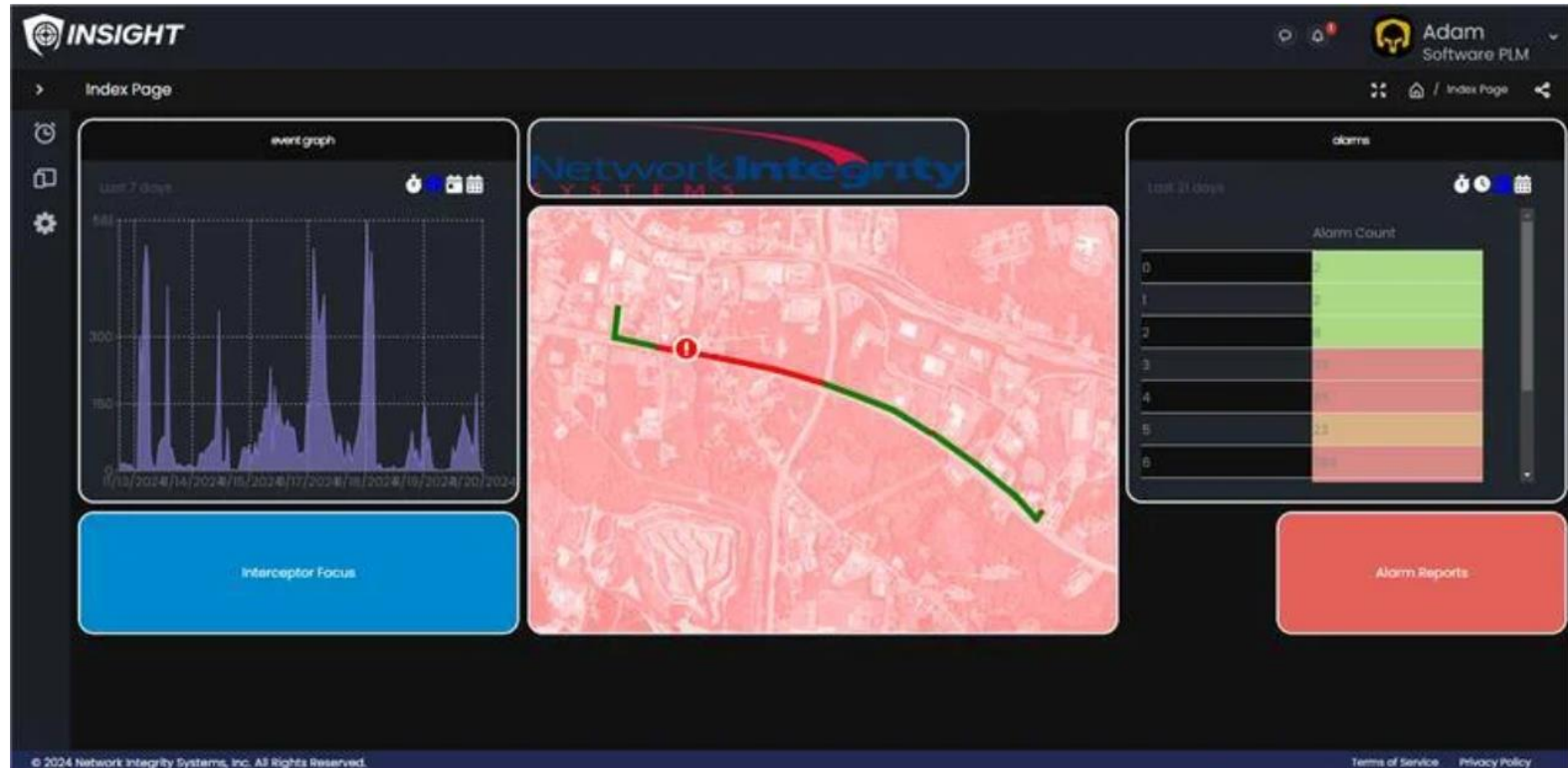


(Available at: <https://hub.networkintegritysystems.com/hubfs/INSIGHT%20Specification%20Sheet%20V1.1.pdf> (hereinafter "INSIGHT Technical Specifications"))

[1][b][2]
wherein the
detected
disturbance
does not exceed
a first preset
threshold for
triggering alerts
of a first alert
type based on
detected
disturbances,

INSIGHT detects a disturbance, where the detected disturbance does not exceed a first preset threshold triggering alerts of a first alert type based on detected disturbances. For example, as shown below a detected disturbance results in an “Alarm Count,” but does not generate an alarm (e.g., red alerts or a red exclamation mark or).

See supra [1][b][1].



(Available at: <https://www.networkintegritysystems.com/interceptor-products-3> (hereinafter “Interceptor Product Page”))

[1][b][3] and
wherein the one
or more sensors
comprise at

The one or more sensors (e.g., NIS FOCUS, manhole cover sensors, etc.) comprise at least one of a vibration sensor, a frequency sensor, an acoustic sensor, and reflective sensor.

least one of a vibration sensor, a frequency sensor, an acoustic sensor, and reflective sensor.

2. DAS Capabilities

The Network Integrity Systems INTERCEPTOR™, SENTINEL™ and VANGUARD™ FOCUS Optical Intrusion Detection Systems utilize Distributed Acoustic Sensing (DAS) technology to provide long range detection capability along with pinpoint location of any physical disturbances to an optical fiber, either one installed as a dedicated sensor cable or or a fiber intrinsic to an optical communications network. By pulsing light down a single-mode optical fiber, the FOCUS solutions can detect events caused by vibrational disturbances created by abnormal activities such as cable handling, tampering, environmental changes, vehicle or foot traffic, heavy machinery, climbing, cutting or lifting of fence fabric, and tunneling under barriers. Identification of these disturbances can be detected anywhere along the cable up to 100km in length. Also, multiple disturbances, no matter how close or how far to each other, can be detected and located simultaneously.

(Available at: <https://hub.networkintegritysystems.com/hubfs/DAS%20in%20the%20Age%20of%20AI.pdf> (hereinafter “DAS in the Age of AI”))

2. Optical Time Domain Reflectometry

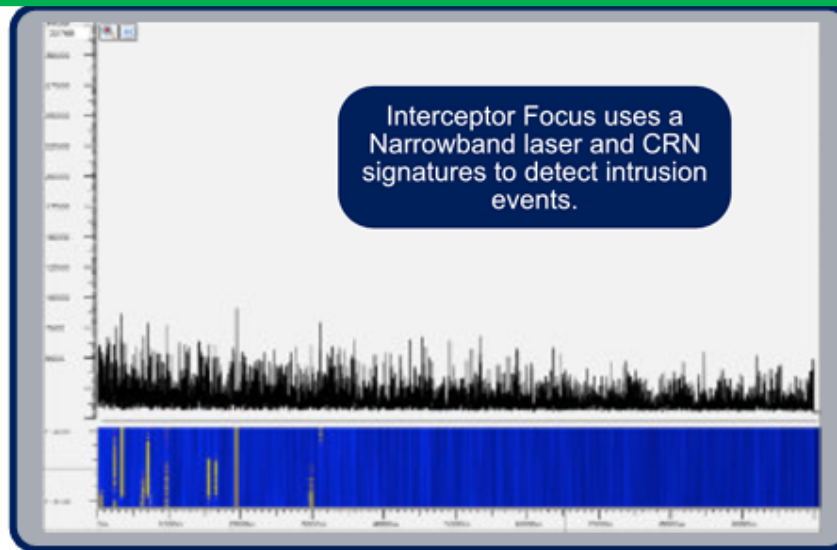
Distributed optical fiber sensors typically use a technique called Optical Time Domain Reflectometry (OTDR) to achieve the spatial resolving function mentioned above. This technique is very similar to radar, in that it uses variations in backscatter from intense, short pulses of radiation launched into an optical fiber.

	<p>Conventional OTDR instruments are commonly used to measure attenuation profiles of optical fibers in the telecommunication industry. Since optical attenuation does not change rapidly in a fiber, these instruments do not need to respond quickly. They are also optimized to read smoothly from point to point along the fiber under test. This latter aspect of performance requires low noise in the detection system. Instrumental noise arises from two main causes. The first is due to thermal noise in the electronics. The effects of this can be minimized by averaging the results from many interrogation pulses, as well as by increasing the sensitivity of the optical receiver to weak optical signals. The second source of noise that needs to be minimized in conventional OTDR systems is caused by the randomness of the molecular structure of glass fiber, in combination with the narrow relative frequency spread of laser sources. This type of noise is known as Coherent Rayleigh Noise (CRN) and repeats exactly between successive interrogation pulses when the laser and the fiber are stable during the interrogation period. This determinism in the noise precludes any improvement from averaging over repeated pulses and is instead overcome by employing lasers with Wideband optical emission.</p>
--	---

3. Distributed Optical Fiber Vibration Sensing

Vibration sensing can be achieved in OTDR systems by shortening the time needed to accurately record the optical backscatter signature of a fiber and by exploiting, rather than minimizing, the CRN signature. Ideally, the backscatter signature should be accurately recorded after a single laser pulse. A narrowband optical source is used to make CRN a large part of the response.

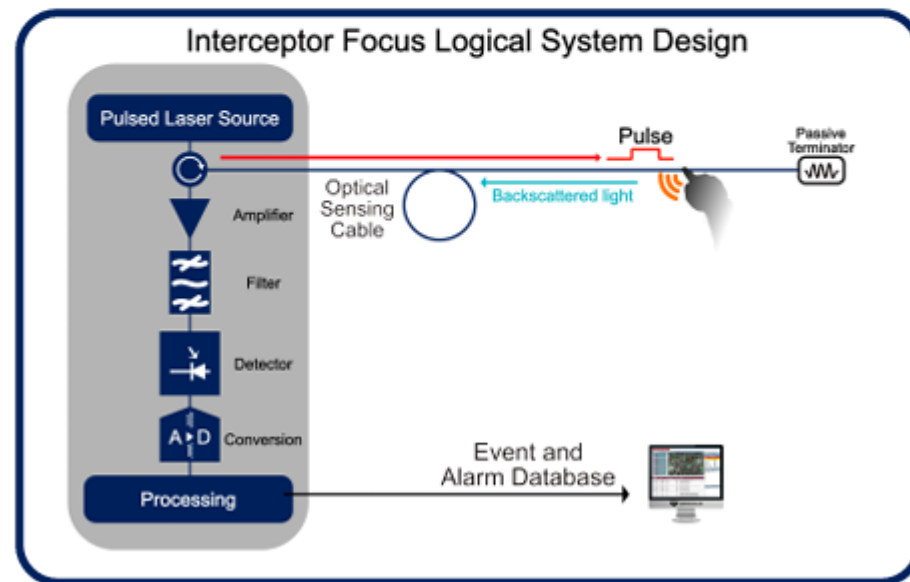
CRN is produced by interference between the backscattered contributions from different parts of the traveling pulse of radiation. The received signal is stable if the fiber is undisturbed. INTERCEPTOR FOCUS measures changes in the CRN pattern. Detection noise is minimized by using optical amplification, narrowband optical filtering, and low-pass electronic filtering.



Any changes in the fiber occurring before the next pulse will then lead to associated changes in the backscatter signature from the fiber. The locations of these changes can then be identified in the time domain and converted to known locations. The magnitudes of the changes depend on the strength and type of disturbance acting on the fiber. In order to provide for discrimination of small changes in backscatter signature over distances shorter than the minimum practical pulse length, the data acquisition system in the

4. Spatial Resolution and Vibration Sensitivity

The instantaneous intensity of the CRN is generated by self-interference between all of the reflected signal components from every part of the propagating optical pulse, so the physical length of the pulse limits the spatial resolution of the system. The shorter the pulse is made, the finer the spatial detail. However, shortening the pulse also reduces the mean intensity of the backscatter, making it harder to record the backscatter signature without suffering from random receiver noise. This introduces a tradeoff between spatial resolution and vibration sensitivity. In practice, laser pulses only one or two meters in length can be used to detect mechanical vibrations having amplitudes much smaller than an optical wavelength, thus providing a very good combination of sensitivity and spatial resolution. Helios GS systems offer spatial resolution down to one meter by using optical pulses of only 10 ns duration.



One other advantage of adopting the OTDR method for distributed detection of vibration is that once the backscattered light has left the sensing region, no

(Available at: <https://hub.networkintegritysystems.com/hubfs/Documents/Brochures/White%20Paper%20-%20INTERCEPTOR%20FOCUS%20Technology.pdf> (hereinafter “FOCUS Whitepaper”))

[1][c]
determining,
responsive to
the detection via
the one or more
sensors, a count
for the number
of disturbances
within a preset
time period that
do not exceed
the first preset
threshold;

INSIGHT determines, responsive to the detection via the one or more sensors, a count for the number of disturbances within a preset time period that do not exceed the first preset threshold.

ALARM RESPONSE MANAGEMENT

SENTINEL integrates with our INSIGHT Alarm Response Management software, offering a comprehensive, real-time view of your security posture. In another industry first, INSIGHT's Event Processor takes event information from multiple sensors and other devices and analyzes the order and severity to provide intelligent alarms based on more than a single factor. SENTINEL scales effortlessly from single to multi-site installations to meet any security need.

(Available at: <https://www.networkintegritysystems.com/sentinel-std> (hereinafter "Sentinel Product Page"))

ALARM RESPONSE MANAGEMENT

SENTINEL FOCUS^{NX} integrates with our INSIGHT Alarm Response Management software, offering a comprehensive, real-time view of your security posture. In another industry first, INSIGHT's Event Processor takes event information from multiple sensors and other devices and analyzes the order and severity to provide intelligent alarms based on more than a single factor. SENTINEL scales effortlessly from single to multi-site installations to meet any security need.

(Available at: <https://www.networkintegritysystems.com/sentinel-FOCUS> (hereinafter "Sentinel FOCUS Product Page"))

Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.

For clients with existing alarm response infrastructure, we offer **INTERLINK™**, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.

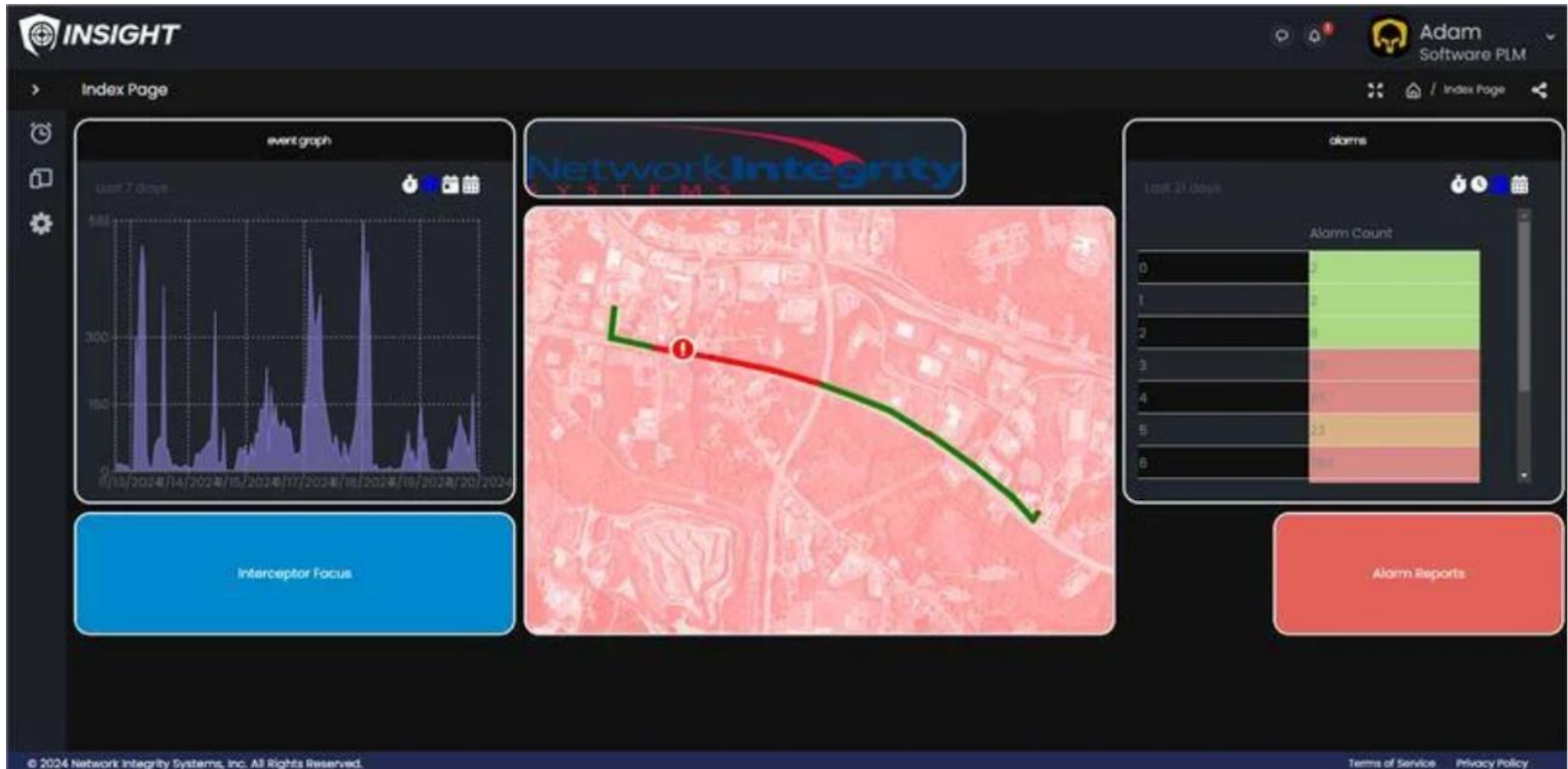
With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.

INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.

In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.

(Available at: INSIGHT Product Page)

For example, INSIGHT displays an “Alarm Count.” Depending on the “Alarm Count,” INSIGHT uses color codes, such as green, orange, and red (on the right below). In addition, INSIGHT annotates an alarm with a red exclamation point (in the center below).



(Available at: Interceptor Product Page)

[1][d][1]
determining
whether the
count, for the

INSIGHT determines whether the count, for the number of disturbances that do not exceed the first preset threshold, exceeds a second preset threshold for triggering alerts of the first alert type.

US Patent No.: 9,455,999 vs. *Network Integrity System's Products*

number of disturbances that do not exceed the first preset threshold, exceeds a second preset threshold for triggering alerts of the first alert type,

Q. How does Interceptor distinguish between true intrusions and everyday events that may cause nuisance alarms?

A: Interceptor incorporates a patented Smart Filtering™ technology to “auto-configure” itself and learn a baseline of normal, routine, benign, non-threatening affects upon the cable system. These normal events are thereafter ignored resulting in the elimination of false alarms.

(Available at: Fact Friday)



INSIGHT™ is an advanced alarm response and management application that integrates with NIS sensor solutions and other systems for comprehensive, efficient security management.

With **INSIGHT™**, you gain real-time visibility into your security posture and receive instant alarms and notifications, allowing you to stay informed and take immediate action when needed. This user-friendly interface, often called a “single pane of glass,” consolidates all aspects of your security infrastructure, streamlining operations and enhancing your ability to respond quickly to security incidents.

Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.

For clients with existing alarm response infrastructure, we offer **INTERLINK™**, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.

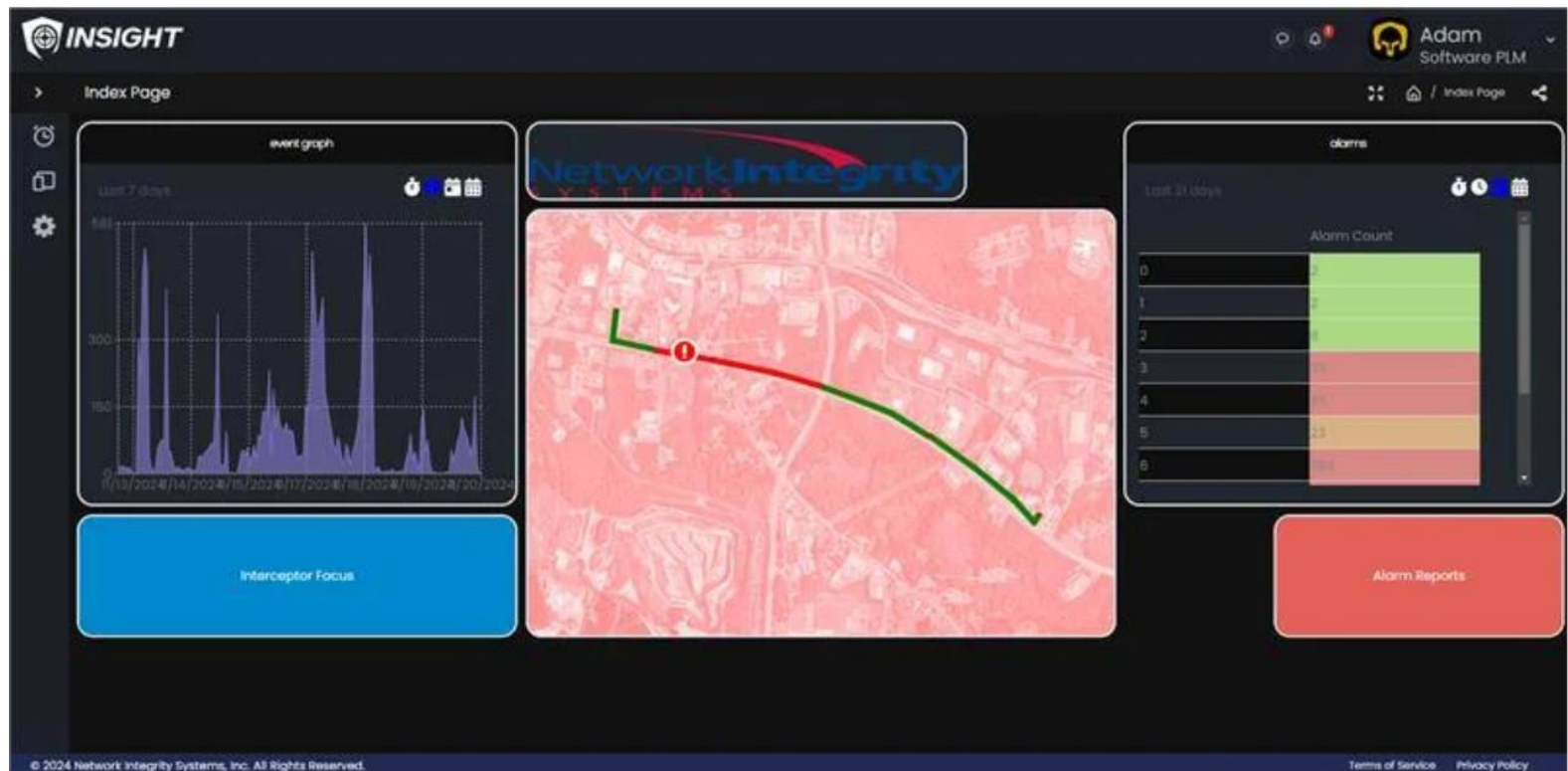
With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.

INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.

In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.

(Available at: INSIGHT Product Page)

For example, INSIGHT displays an “Alarm Count.” Depending on the “Alarm Count,” INSIGHT uses color codes, such as green, orange, and red (on the right below). In addition, INSIGHT annotates an alarm with a red exclamation point (in the center below).



(Available at: [Interceptor Product Page](#))

[1][d][2]
wherein the
second preset
threshold
corresponds to a
preset number

The second preset threshold corresponds to a preset number of allowable disturbances not exceeding the first preset threshold and within the preset time period before one or more alerts of the first alert type are to be triggered.

See supra [1][d][1].

of allowable disturbances, not exceeding the first preset threshold and within the preset time period, before one or more alerts of the first alert type are to be triggered; and	The second preset threshold annotated above (<i>See supra</i> [1][d][1]) shows a red color. Such red color corresponds to a preset number of allowable disturbances (e.g., not exceeding the first preset threshold and within the preset time period) before one or more alerts of the first alert type are to be triggered. Prior to the second preset threshold being exceeded, the color may be green. As such, once the second preset threshold is exceeded, the color changes to red and the first alert type is triggered.
[1][c] triggering an alert of the first alert type responsive to a determination that the count exceeds the second preset threshold.	INSIGHT triggers an alert of the first alert type responsive to a determination that the count exceeds the second preset threshold. <i>See supra</i> [1][d][1]-[1][d][2].

Exhibit 11

US Patent No.: 11,367,342 vs. *Network Integrity System's Products*

Claim	Support for Infringing Product(s) [Annotations in Green]
Claim 17	
[17] One or more non-transitory, computer-readable media storing instructions that, when executed by one or more processors, effectuate operations comprising:	<p>Network Integrity Systems (NIS) sells products that include one or more non-transitory, computer-readable media storing instructions that, when executed by one or more processors, effectuate operations.</p> <p>For example, NIS's INSIGHT runs on a computing device having one or more non-transitory, computer-readable media storing instructions that, when executed by one or more processors, effectuate operations.</p> <div style="text-align: center;">  <p>INSIGHT™ Alarm Response & Management System</p> </div> <p>INSIGHT™ is an advanced alarm response and management application that integrates with NIS sensor solutions and other systems for comprehensive, efficient security management.</p> <hr/> <p>With INSIGHT™, you gain real-time visibility into your security posture and receive instant alarms and notifications, allowing you to stay informed and take immediate action when needed. This user-friendly interface, often called a "single pane of glass," consolidates all aspects of your security infrastructure, streamlining operations and enhancing your ability to respond quickly to security incidents.</p> <p>Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.</p> <p>For clients with existing alarm response infrastructure, we offer INTERLINK™, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.</p> <p>With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.</p> <p>INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.</p> <p>In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.</p> <p>(Available at: https://www.networkintegritysystems.com/insight (hereinafter "INSIGHT Product Page"))</p>

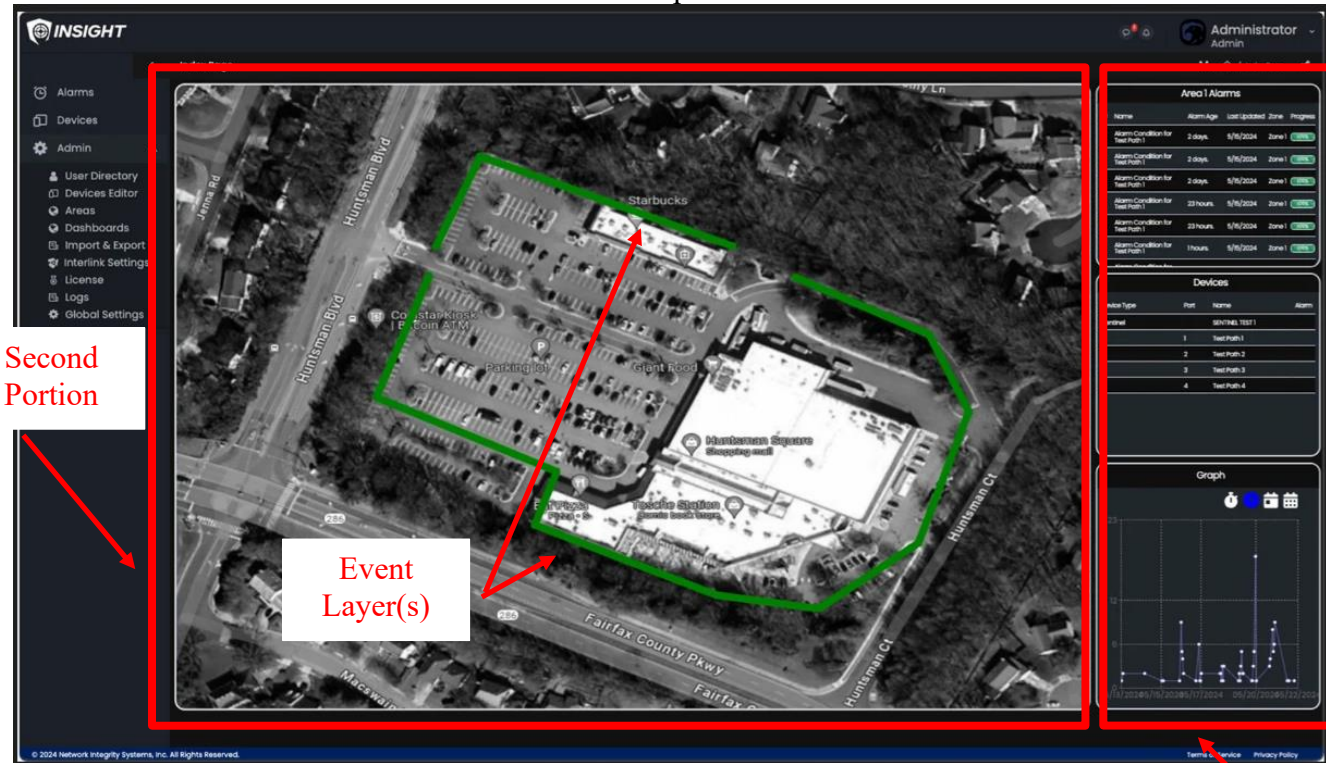
US Patent No.: 11,367,342 vs. Network Integrity System's Products

	<p>Licensing:</p> <p>In some cases, the purchase price of NIS products includes a license for INSIGHT™ or INTERLINK™ software. The license allows for the installation and operation of the current (as of installation date) production version of the described software. It does not cover future software upgrades or non-security-related patches. Software security-related patches for the licensed software version will be provided under this license for a period of three (3) years from date of delivery.</p> <p>NIS offers a Warranty and Support Program (WSP) that provides additional licensing for patches and/or version upgrades released during the WSP term, depending on the purchased options. NIS will never disable your software if you don't have a WSP subscription, but support will be limited to software security-related issues. For WSP program details, please refer to the Warranty and Support Program page.</p> <p>Customers without a WSP subscription can obtain a license for the latest software versions by purchasing a one-year WSP subscription at the Premium level.</p> <div style="border: 2px solid green; padding: 10px;"> <p>Minimum System Requirements:</p> <table border="1"> <tr> <td>Operating System</td><td>Windows – Windows 11; Windows Server 2019 or newer Linux – CentOS; Debian; Fedora; Ubuntu</td></tr> <tr> <td>CPU</td><td>64 bit, multi-core at 2.4 GHz</td></tr> <tr> <td>RAM¹</td><td>8 GB – 16 GB</td></tr> <tr> <td>Storage²</td><td>100 GB</td></tr> <tr> <td>Ports & Protocols³</td><td>Services = TCP 4000; HTTP= TCP 80; HTTPS= TCP 443</td></tr> </table> <p>Software Requirements: Docker Engine⁴ – Version 20.10.25 or newer 7-ZIP (Both Windows & Linux)</p> <p>¹May need to increase when connecting more than 50 devices to INSIGHT.</p> <p>²Storage capacity dependent on customer limitations. Above is the minimum recommendation for storage of logs (worker, server, install logs), Alarm Reports (and attachments), user profiles, Areas (with imagery), and Dashboards.</p> <p>³HTTP/HTTPS ports can be configured to a different TCP port if needed during installation of INSIGHT. Ports 80 and 443 are default.</p> <p>⁴If Docker Desktop is being used, the customer needs to follow requirements for running Docker Desktop within their organization.</p> </div> <p style="text-align: center;">(Available at: https://hub.networkintegritysystems.com/hubfs/INSIGHT%20Specification%20Sheet%20V5.pdf (hereinafter “INSIGHT Technical Specifications”))</p>	Operating System	Windows – Windows 11; Windows Server 2019 or newer Linux – CentOS; Debian; Fedora; Ubuntu	CPU	64 bit, multi-core at 2.4 GHz	RAM ¹	8 GB – 16 GB	Storage ²	100 GB	Ports & Protocols ³	Services = TCP 4000; HTTP= TCP 80; HTTPS= TCP 443
Operating System	Windows – Windows 11; Windows Server 2019 or newer Linux – CentOS; Debian; Fedora; Ubuntu										
CPU	64 bit, multi-core at 2.4 GHz										
RAM ¹	8 GB – 16 GB										
Storage ²	100 GB										
Ports & Protocols ³	Services = TCP 4000; HTTP= TCP 80; HTTPS= TCP 443										
[1][a][1] providing a user interface including (i) a first portion configured	INSIGHT provides a user interface including (i) a first portion configured to present a set of events and (ii) a second portion configured to present a playback of events in accordance with event detection times and a set of event layers for the playback.										

US Patent No.: 11,367,342 vs. Network Integrity System's Products

to present a set of events and (ii) a second portion configured to present a playback of events in accordance with event detection times and a set of event layers for the playback,

Example 1:



First Portion

US Patent No.: 11,367,342 vs. Network Integrity System's Products



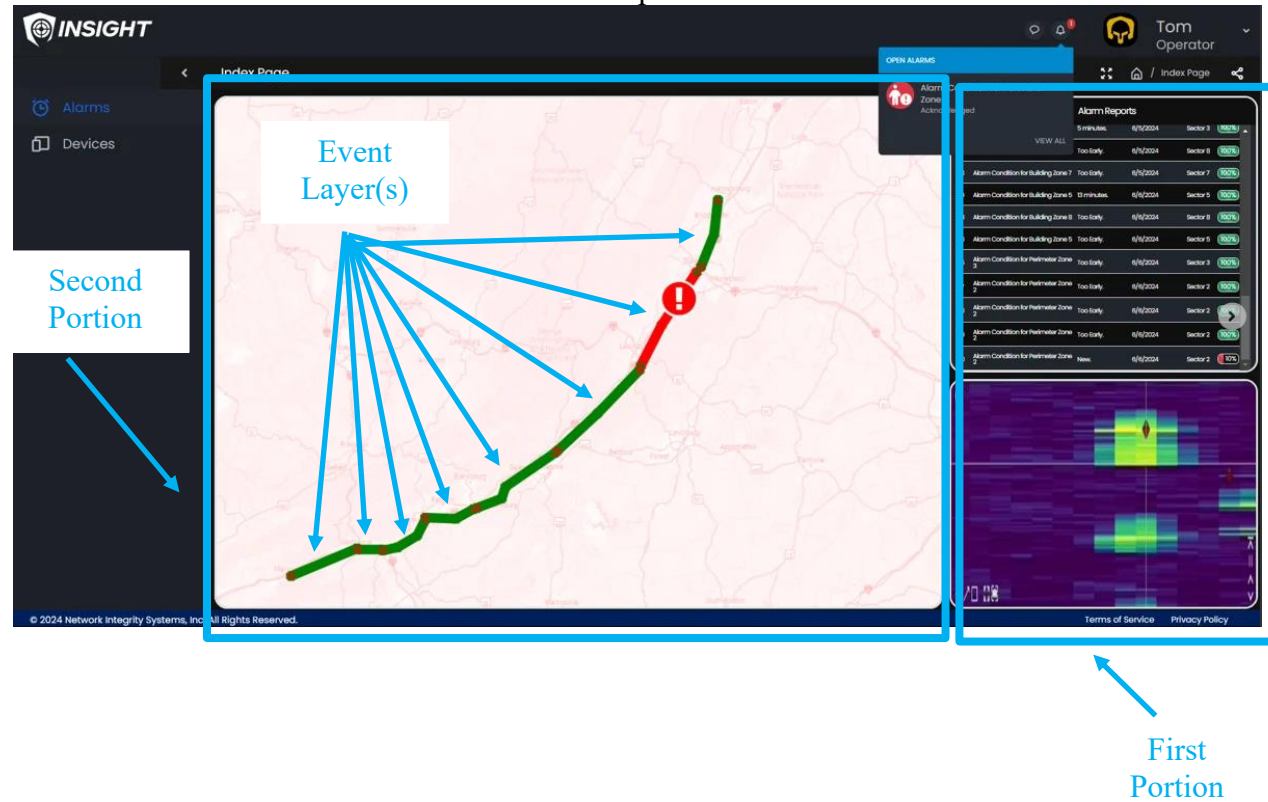
Expanded view of
First Portion
showing:

- Events and
- Event detection times

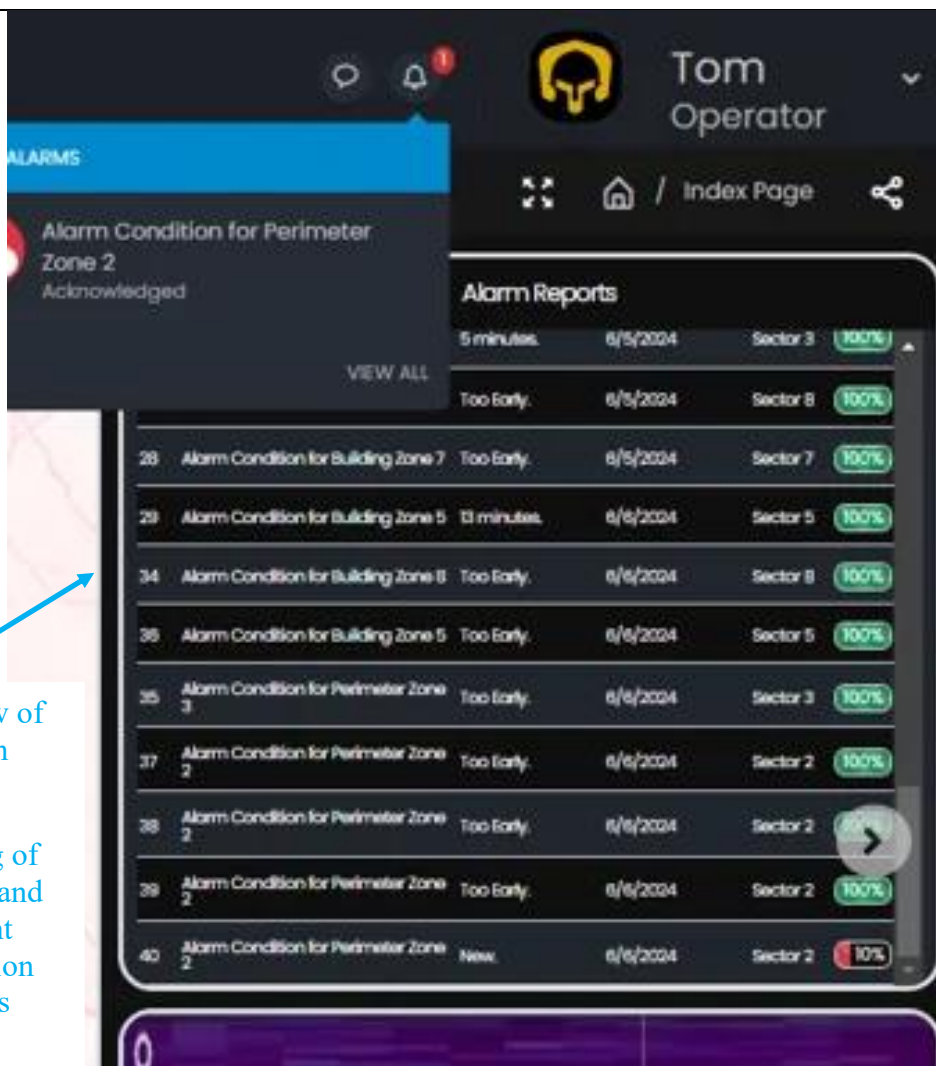
(Available at: INSIGHT Product Page)

(Note: Annotations in red for the above user interface)

Example 2:



US Patent No.: 11,367,342 vs. Network Integrity System's Products



Expanded view of
First Portion
showing:

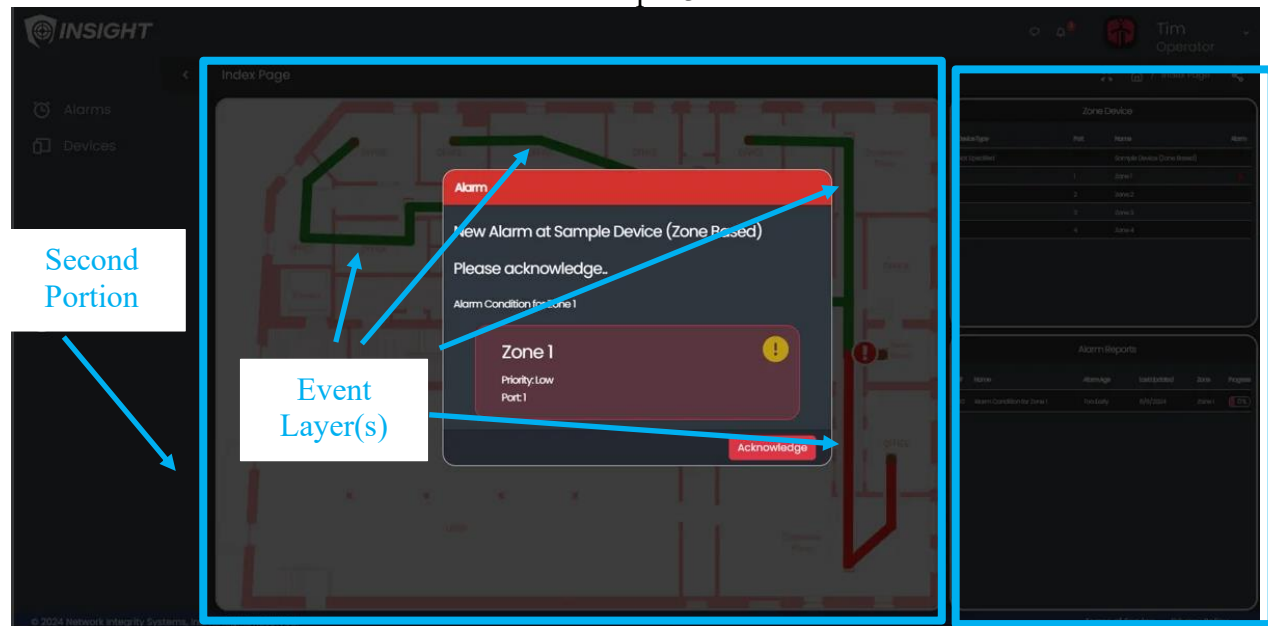
- Listing of events and
- Event detection times

(Available at: INSIGHT Product Page)

(Note: Annotations in blue for the above user interface)

US Patent No.: 11,367,342 vs. *Network Integrity System's Products*

Example 3:



First Portion

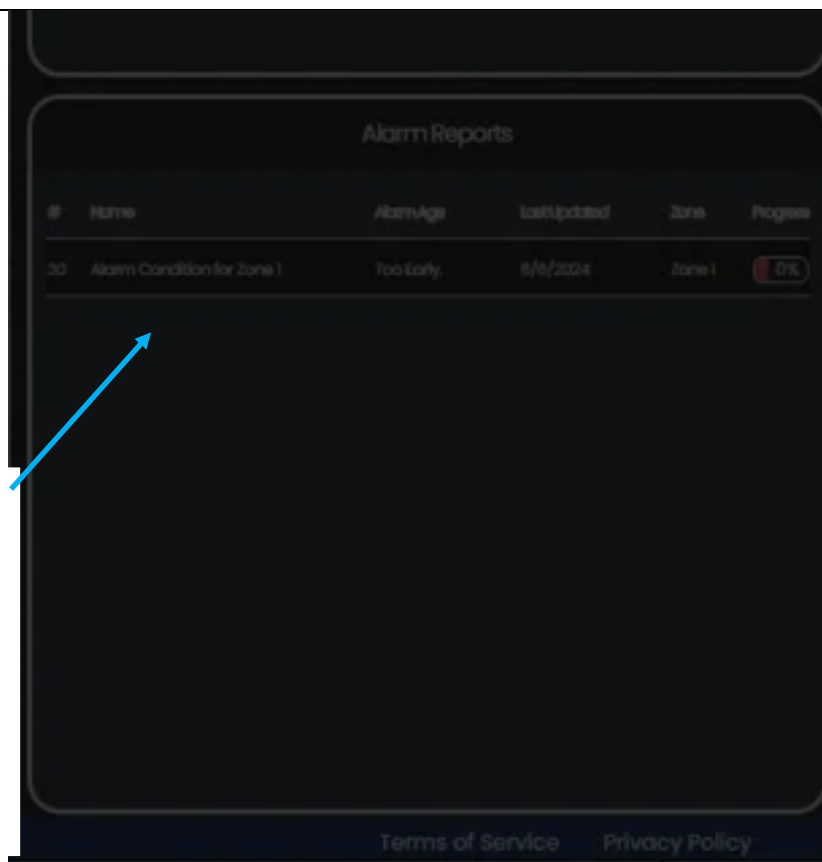
Second Portion

Event Layer(s)

US Patent No.: 11,367,342 vs. *Network Integrity System's Products*

Expanded view of
First Portion
showing:

- Listing of events and
- Event detection times



(Available at: INSIGHT Product Page)

(Note: Annotations in blue for the above user interface)

Our system provides a detailed map of the cabling environment/path and virtual segments of different risk areas. It can detect an event related to the cable and/or the surrounding area, differentiate between events, identify its location, and mobilize the appropriate response.

(Available at: <https://www.networkintegritysystems.com/li-landing-page> (hereinafter “Eliminate Downtime Page”))

US Patent No.: 11,367,342 vs. Network Integrity System's Products

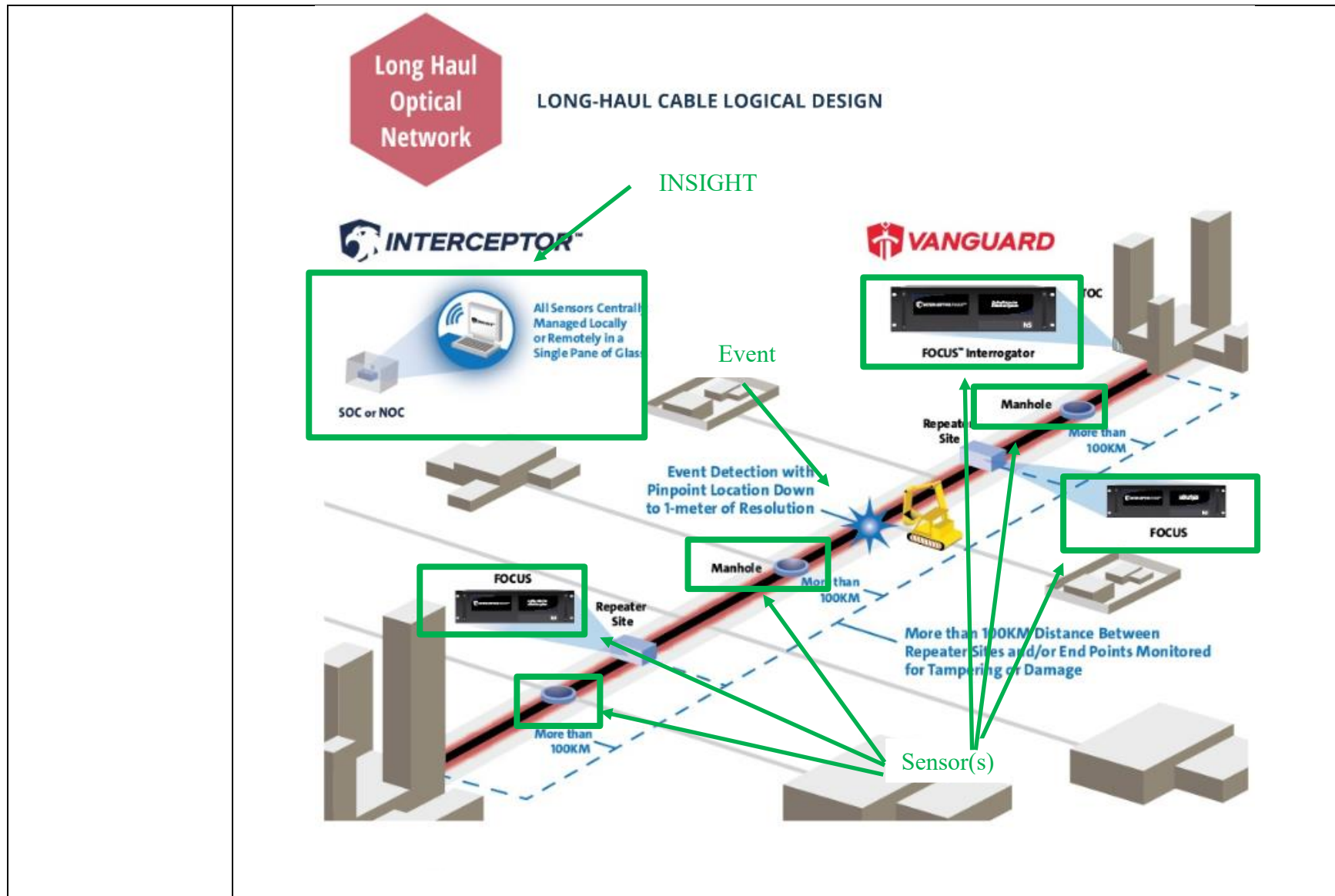
Feature Comparison (v1.1)			
User configuration		✓	
• User		✓	
• Team		✓	
• Organization		✓	
• Custom Roles		✓	
Administrator roles for full user management		✓	
Fully customizable map/image display with path overlay		✓	
Fully customizable Dashboard display per user		✓	
Widgets library for personalized experience		✓	
Alarm notification (visual with optional audio)		✓	
Alarm investigation and reporting		✓	
Customizable alarm response procedures		✓	
Dark/Light modes		✓	✓
Bespoke event processing engine		✓	✓
Event broker (up and down-stream)		✓	✓
Full logging of all activity with sortable display		✓	✓
Automated & On-Demand Zone Testing		✓	✓
Email notifications		✓	✓
Device integration management		✓	✓
Multi-device management and upgrades		✓	✓
Notifications for license renewal and upgrades		✓	✓
Flexible licensing		✓	✓
Runs on Windows or Linux platforms		✓	✓
Contextual help available on screen		✓	✓

(Available at: <https://www.networkintegritysystems.com/insight/interlink-features-comparison> (hereinafter “INSIGHT-INTERLINK Features Comparison”))

US Patent No.: 11,367,342 vs. *Network Integrity System's Products*

<p>[1][a][2] each layer of the set of layers indicating one or more events related to alerts generated by sensors based on an event detection;</p>	<p>Each layer of the set of layers (e.g., presented in the second portion) indicate one or more events related to alerts generated by sensors based on an event detection. For example, INSIGHT obtains sensor data (e.g., alerts generated by sensors) from multiple sensors (e.g., NIS FOCUS, manhole cover sensors, etc.).</p> <p>See <i>supra</i> [1][a][1];</p> <p>Note: Although Examples 1-3 (e.g., of the user interface) have been provided above, for sake of brevity, support of infringement for any of the following claim feature(s) may be shown with respect to any one of the Examples 1-3 as indicated above.</p>
--	---

US Patent No.: 11,367,342 vs. Network Integrity System's Products



LONG-HAUL CABLE CYBER PROTECTION

Cable downtime is costly but monitoring thousands of kilometers of cable is challenging. Distributed Acoustic Sensing technology (DAS) allows you to confidently monitor your cables in real time and detect risks to within 1 meter of resolution. Using DAS technology, our FOCUS NX system monitors a single strand of SM cable in long-haul cables and pathways) and pinpoints the exact location of events such as impact to conduit or tampering with the cable. This reduces the risk of downtime or data security breaches. Through daisy-chaining practices, the protection of any cable length can be achieved.

The FOCUS NX seamlessly integrates with our INSIGHT Alarm Response Management software, giving you a comprehensive view of your security posture. This integration allows for effortless monitoring and management of your security systems.

The U.S. Government and Military uses INTERCEPTOR FOCUS NX to protect their classified network infrastructure, and the VANGUARD FOCUS NX is available for the commercial market to protect their network infrastructure.

(Available at: Slide 86 of <https://prezi.com/view/ofYkUmoJdl3b1X4WlETk/?hsCtaTracking=0b289cce-8dbb-46ec-8647-7885d8c1659e%7Cc64c2891-b4f8-4165-b5f4-d5d19a8f53f> (hereinafter "Prezi"))

US Patent No.: 11,367,342 vs. Network Integrity System's Products



While our INTERCEPTOR or VANGUARD products actively protect cabling system assets, areas of likely ingress, such as maintenance manholes or other maintenance points, are often unprotected and should be monitored to detect unauthorized entry as a second layer of protection.

Our Maintenance Hole Protection System was designed to provide real time monitoring of network infrastructure access points such as maintenance-holes and hand-holes over long distances utilizing zero-power fiber optic sensors. Each sensor can detect Open/Close conditions, fiber loss (dB), and fiber cuts at each sensor location.

(Available at: Prezi, slide 87)

Q. How does Interceptor™ detect an intrusion into a fiber optic cable?

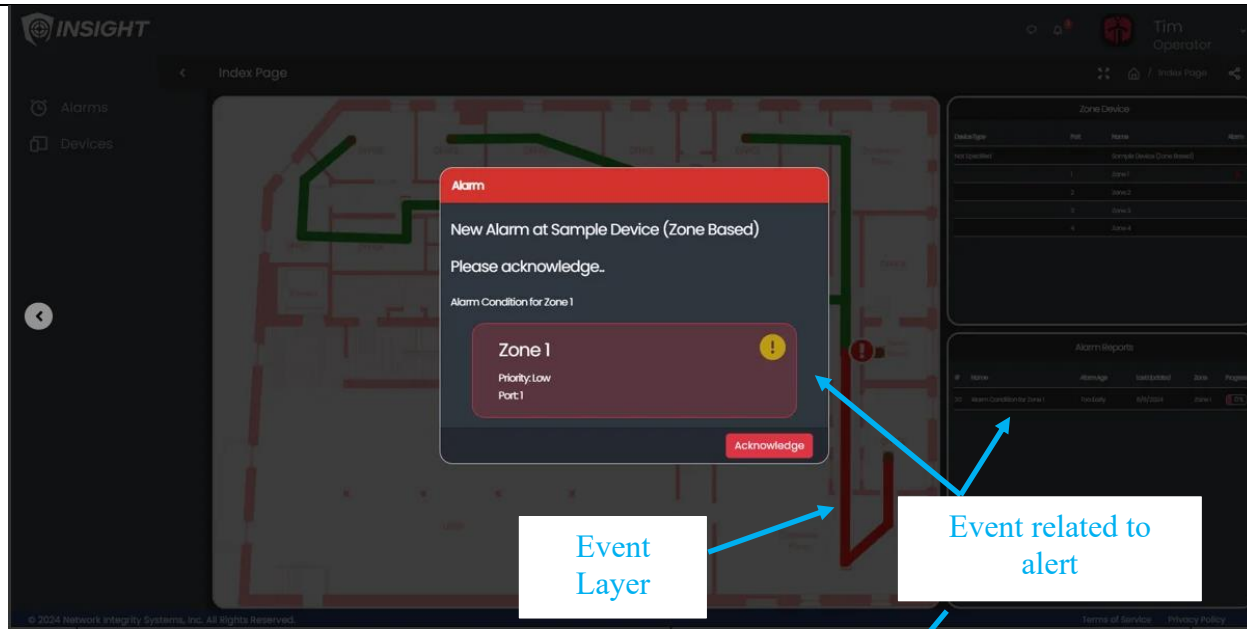
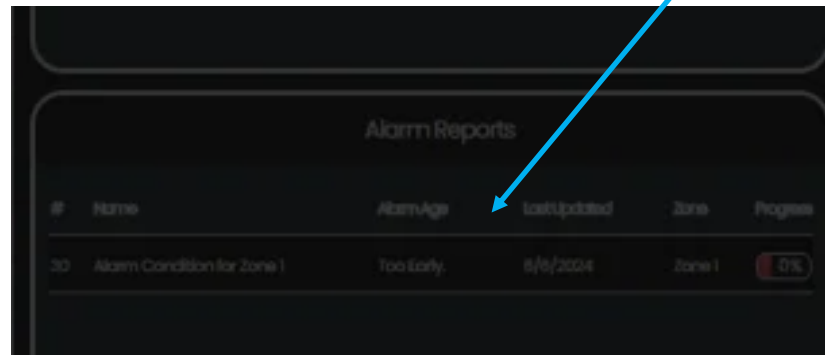
A: Interceptor launches a monitoring signal into a pair of fibers of the optical cable being protected, which turns the entire cable (up to 144 fibers) into a sensor. When any component of the cable is abnormally handled, for instance during an intrusion attempt, the monitored fibers sense the disturbance and Interceptor reports the event.

(Available at: <https://www.networkintegritysystems.com/blog/2010/01/22/fact-friday-1> (hereinafter “Fact Friday”))

US Patent No.: 11,367,342 vs. *Network Integrity System's Products*

	<div data-bbox="1346 191 1799 323">  Product Specifications </div> <div data-bbox="638 334 1745 769" style="border: 2px solid green; padding: 10px;"> <p>Designed with a focus on security and reliability, INSIGHT provides a robust platform for managing incoming sensor information. It features intelligent dispatch and investigation management, enabling effective prioritization and handling of alarms. Whether analyzing data, dispatching personnel, or conducting investigations, INSIGHT streamlines these processes, saving you valuable time and resources.</p> <p>For clients with existing alarm response infrastructure, we offer INTERLINK™, a specialized feature set within INSIGHT that seamlessly integrates a variety of sensors into your current system. INTERLINK simplifies the integration process, ensuring a smooth transition and maximizing the value of your existing security investments.</p> <p>With unique capabilities like our Bespoke Event Processing engine, you can customize how events are categorized and when alarms are triggered, providing ultimate flexibility in correlating events into actionable alarms while minimizing false and nuisance alerts.</p> <p>INSIGHT also offers complete flexibility in defining user security, allowing nearly every user action to be configured on a per-user or team basis.</p> <p>In summary, INSIGHT and INTERLINK deliver a comprehensive and intelligent security management solution. From alarm response and device management to seamless integration with other security systems, our software empowers you to proactively protect your assets and maintain a secure environment.</p> </div> <p style="text-align: center;">(Available at: INSIGHT Technical Specifications)</p>
--	--

US Patent No.: 11,367,342 vs. Network Integrity System's Products



(Available at: INSIGHT Product Page)

(Note: Annotations in blue for the above user interface)

US Patent No.: 11,367,342 vs. Network Integrity System's Products

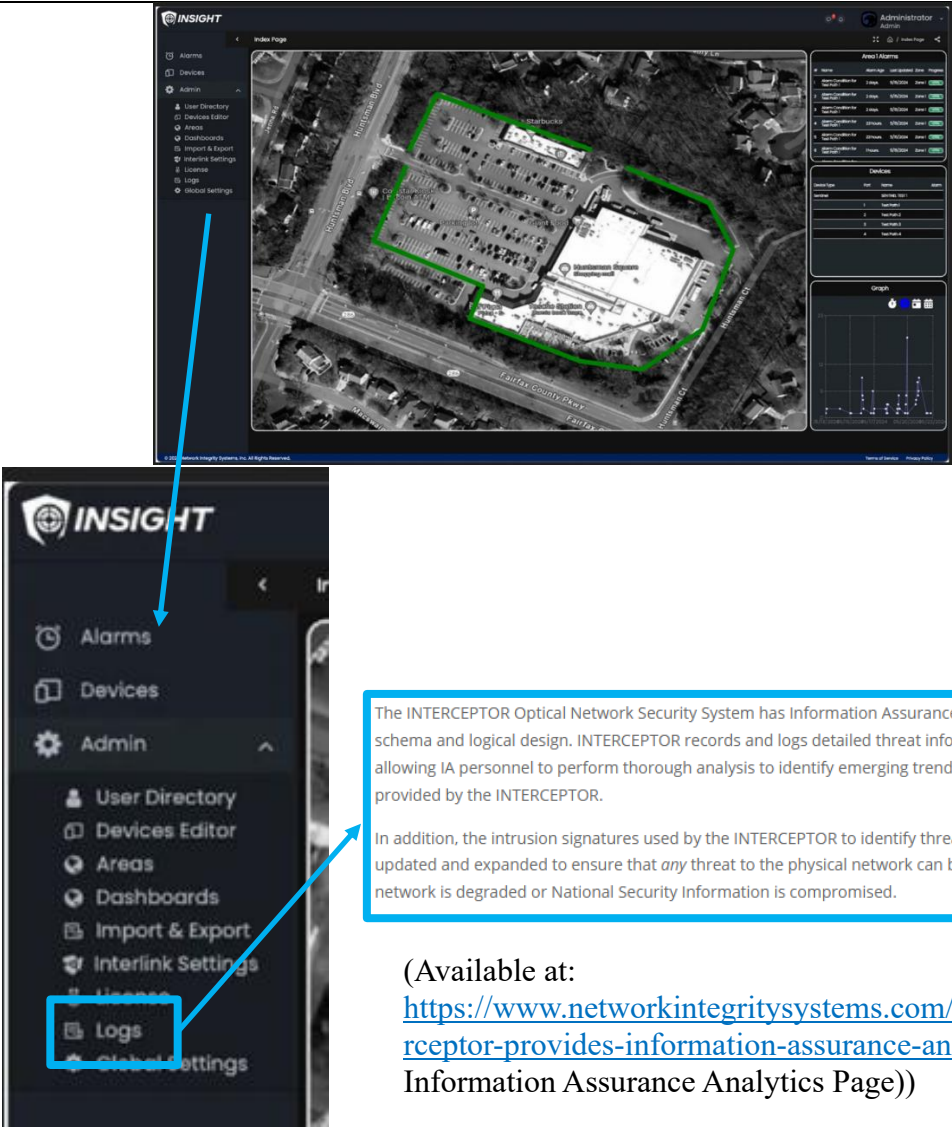
[1][b] obtaining, during the playback, a user selection of events via the user interface, the user selection indicating a subset of events to be presented in the playback;

INSIGHT provides functionality that during the playback, INSIGHT obtains a user selection of events via the user interface. The user selection indicates a subset of events to be presented in the playback.

Feature Comparison (v1.1)		INSIGHT	INTERLINK
User configuration		✓	
• User		✓	
• Team		✓	
• Organization		✓	
• Custom Roles		✓	
Administrator roles for full user management		✓	
Fully customizable map/image display with path overlay		✓	
Fully customizable Dashboard display per user		✓	
Widgets library for personalized experience		✓	
Alarm notification (visual with optional audio)		✓	
Alarm investigation and reporting		✓	
Customizable alarm response procedures		✓	
Dark/Light modes		✓	✓
Bespoke event processing engine		✓	✓
Event broker (up and down stream)		✓	✓
Full logging of all activity with sortable display		✓	✓
Automated & On-Demand Zone Testing		✓	✓
Email notifications		✓	✓
Device integration management		✓	✓
Multi-device management and upgrades		✓	✓
Notifications for license renewal and upgrades		✓	✓
Flexible licensing		✓	✓
Runs on Windows or Linux platforms		✓	✓
Contextual help available on screen		✓	✓

(Available at: INSIGHT-INTERLINK Features Comparison)

US Patent No.: 11,367,342 vs. Network Integrity System's Products



The top screenshot shows the INSIGHT web interface. The main area displays a map of a building complex with a green outline. The left sidebar contains a menu with items: Alarms, Devices, Admin, User Directory, Devices Editor, Areas, Dashboards, Import & Export, Interlink Settings, Licenses, Logs, and Global Settings. The right sidebar shows 'Area 1 Alarms' and 'Dashboards'.

The bottom screenshot is a close-up of the sidebar menu. The 'Logs' item is highlighted with a blue box. A blue arrow points from the 'Logs' item in the bottom screenshot to the 'Logs' item in the top screenshot.

The INTERCEPTOR Optical Network Security System has Information Assurance Analytics embedded in its protection schema and logical design. INTERCEPTOR records and logs detailed threat information and the associated alarms, allowing IA personnel to perform thorough analysis to identify emerging trends, as well as to optimize the protection provided by the INTERCEPTOR.

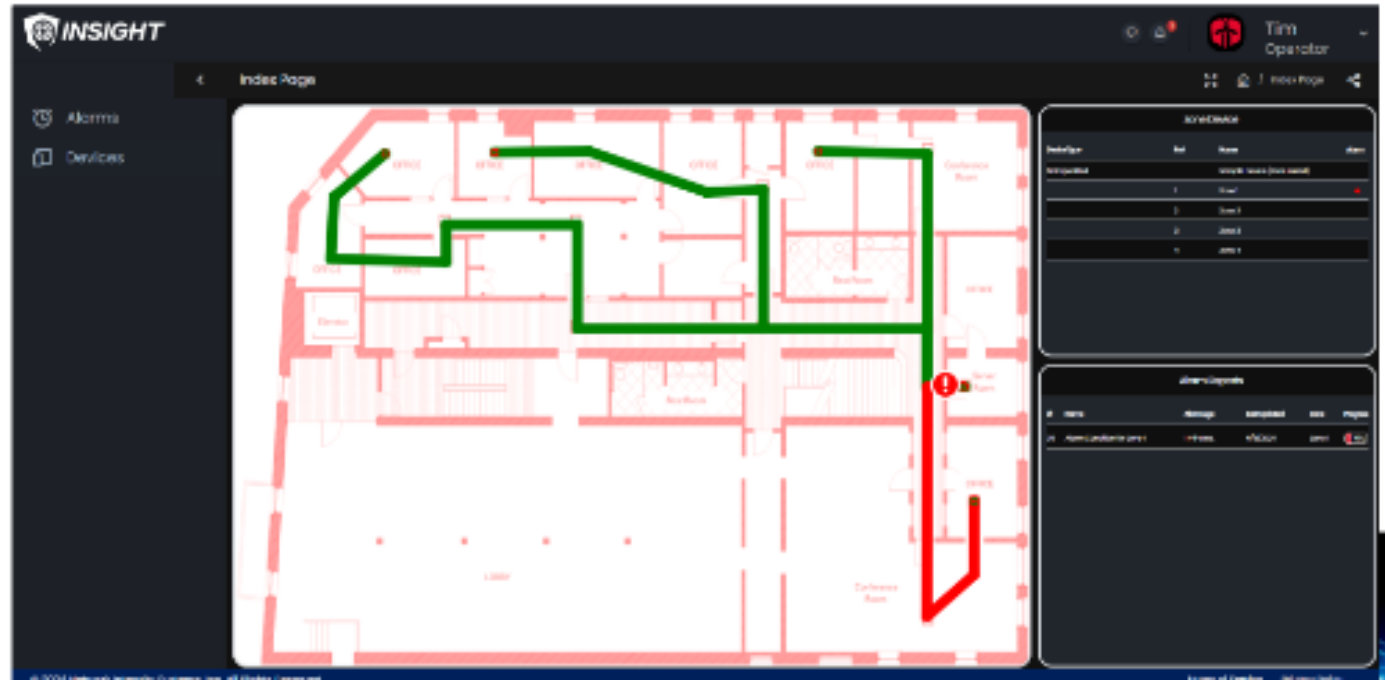
In addition, the intrusion signatures used by the INTERCEPTOR to identify threats to the network are continuously updated and expanded to ensure that *any* threat to the physical network can be identified and detected *before* the network is degraded or National Security Information is compromised.

(Available at:
<https://www.networkintegritysystems.com/blog/2011/11/09/interceptor-provides-information-assurance-analytics> (hereinafter: Information Assurance Analytics Page))

(Available at: INSIGHT Product Page)

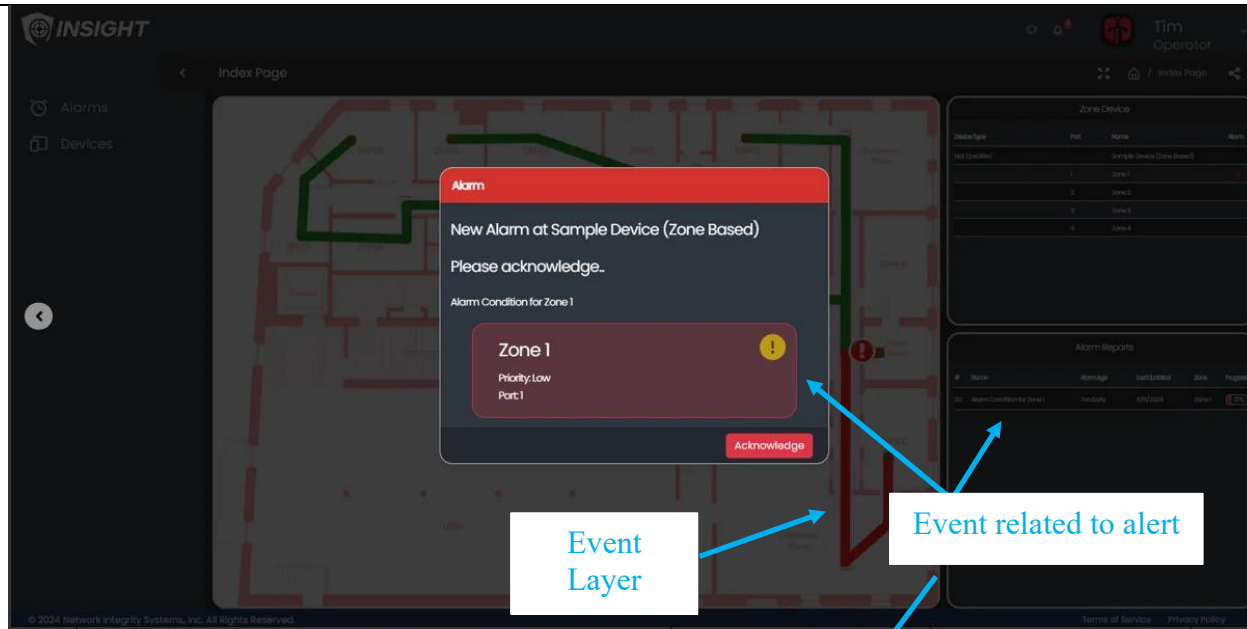
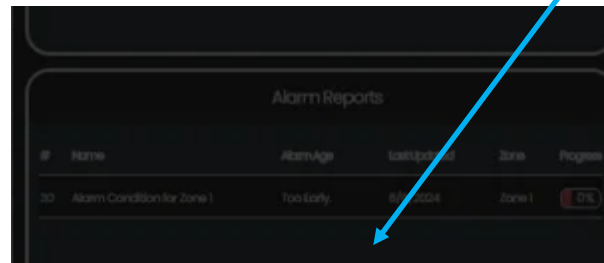
(Note: Annotations in blue for the above user interface)

US Patent No.: 11,367,342 vs. Network Integrity System's Products



(Available at: Prezi, slide 134)

US Patent No.: 11,367,342 vs. *Network Integrity System's Products*

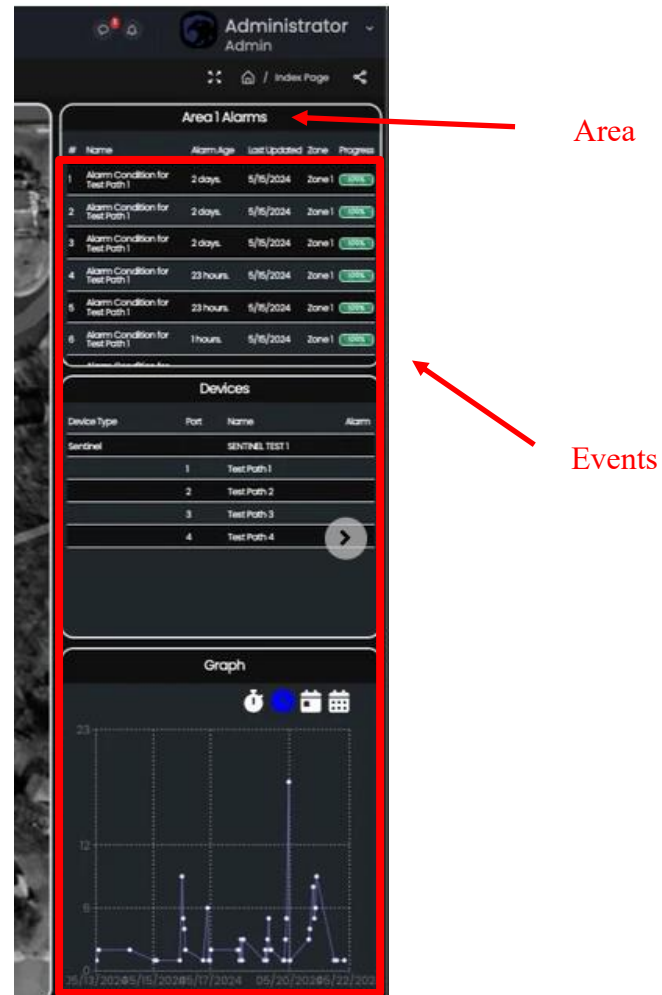


(Available at: INSIGHT Product Page)

(Note: Annotations in blue for the above user interface)

For example, as INSIGHT “records and logs detailed threat information and associated alarms,” a user may select events via the user interface, indicating a subset of events to be presented in the playback.

As another example, INSIGHT displays views of different “Area(s)” (e.g., Area 1 Alarms). As such, a user may select an Area associated with events – hence, a user selection of events via the user interface indicating a subset of events to be presented in the playback.



(Available at: INSIGHT Product Page)

(Note: Annotations in red for the above user interface)

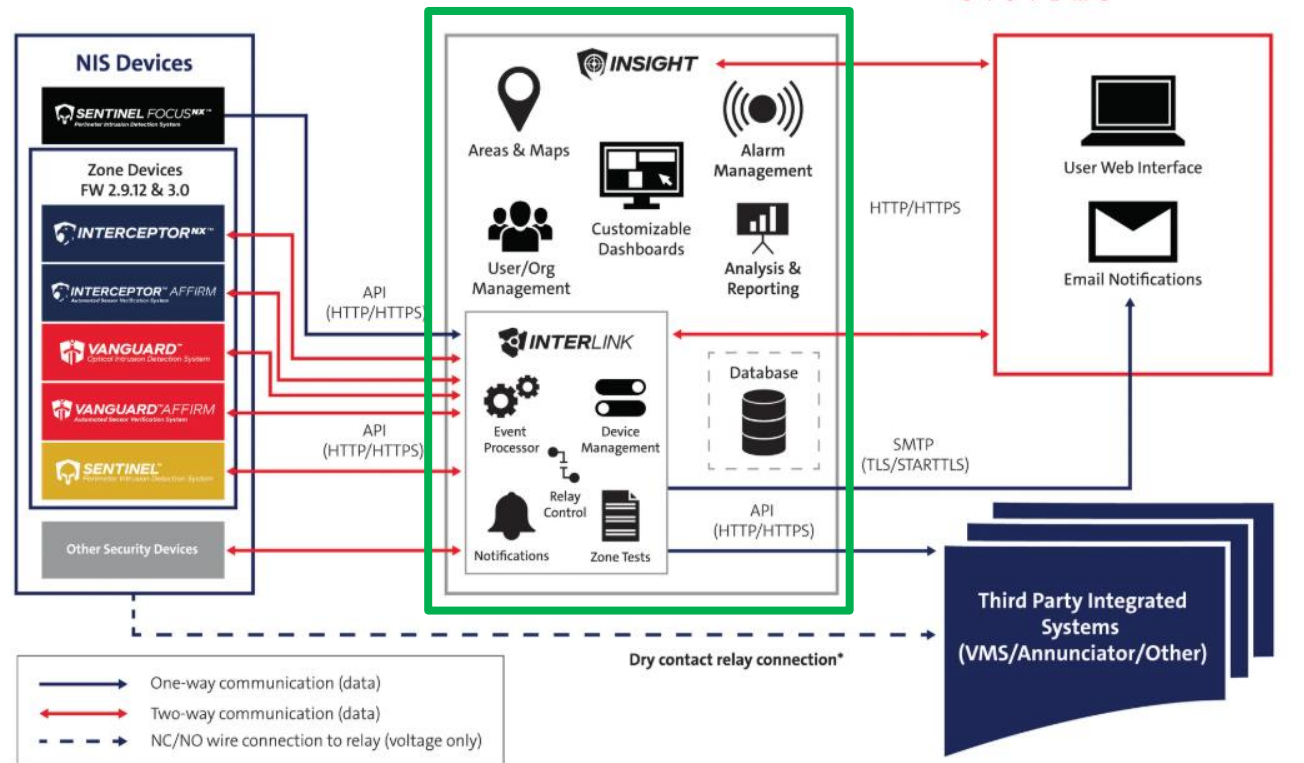
US Patent No.: 11,367,342 vs. Network Integrity System's Products

[1][c] modifying, during the playback, a set of layers for the playback based on the user selection such that layers corresponding to the subset of events are added to the event playback; and

INSIGHT modifies, during the playback, a set of layers for the playback based on the user selection such that layers corresponding to the subset of events are added to the event playback.

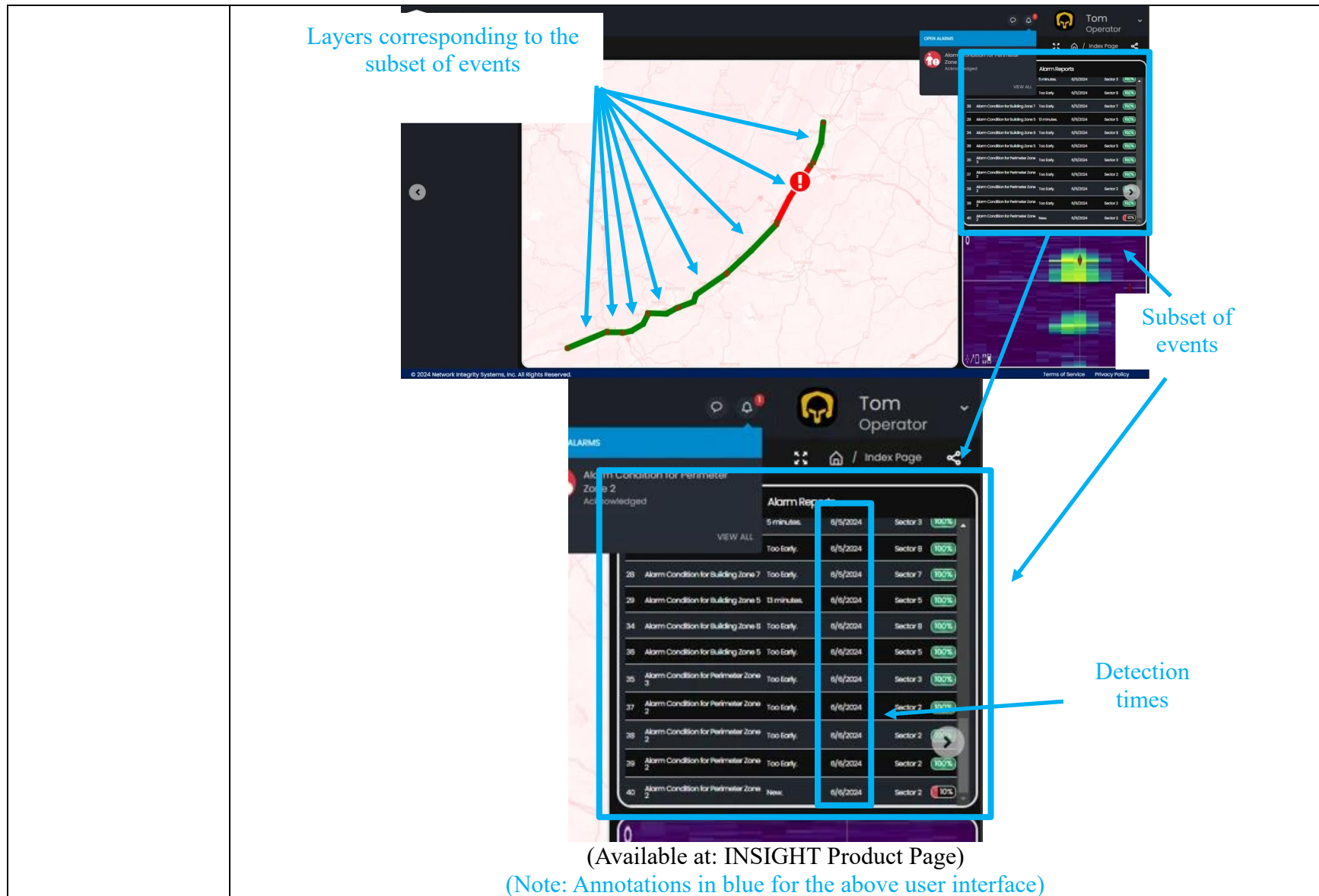
See *supra* [1][b].

System Connectivity Architecture



(Available at: INSIGHT Product Page)

US Patent No.: 11,367,342 vs. Network Integrity System's Products



US Patent No.: 11,367,342 vs. Network Integrity System's Products

[1][d] causing the layers corresponding to the subset of events to be overlaid on the second portion of the user interface based on the modification of the set of layers such that the subset of events is presented based on detection times associated with the subset of events.

INSIGHT causes the layers corresponding to the subset of events to be overlaid on the second portion of the user interface based on the modification of the set of layers such that the subset of events is presented based on detection times associated with the subset of events.

See *supra* [1][c].

Our system provides a detailed map of the cabling environment/path and virtual segments of different risk areas. It can detect an event related to the cable and/or the surrounding area, differentiate between events, identify its location, and mobilize the appropriate response.

(Available at: Eliminate Downtime Page)

Feature Comparison (v1.1)	INSIGHT	INTERLINK
User configuration	✓	
• User	✓	
• Team	✓	
• Organization	✓	
• Custom Roles	✓	
Administrator roles for full user management	✓	
Fully customizable map/image display with path overlay	✓	
Fully customizable Dashboard display per user	✓	
Widgets library for personalized experience	✓	
Alarm notification (visual with optional audio)	✓	
Alarm investigation and reporting	✓	
Customizable alarm response procedures	✓	
Dark/Light modes	✓	✓
Bespoke event processing engine	✓	✓
Event broker (up and down-stream)	✓	✓
Full logging of all activity with sortable display	✓	✓
Automated & On-Demand Zone Testing	✓	✓
Email notifications	✓	✓
Device integration management	✓	✓
Multi-device management and upgrades	✓	✓
Notifications for license renewal and upgrades	✓	✓
Flexible licensing	✓	✓
Runs on Windows or Linux platforms	✓	✓
Contextual help available on screen	✓	✓

(Available at: INSIGHT-INTERLINK Features Comparison)