White Paper

Distributed Acoustic Sensing in the Age of AI

For two decades, Network Integrity Systems has been at the forefront of the fiber optic sensing industry, constantly pushing the boundaries of innovation. Over the past five years, we have actively participated in the advancements of Distributed Acoustic Sensing (DAS), with a focus on Security and Critical Infrastructure Protection, With our groundbreaking FOCUS^{NX} solutions, equipped with cutting-edge Machine Learning technology, we have taken detection capabilities to a whole new level. Discover the power of DAS and how harnessing Artificial Intelligence can significantly enhance your security posture.

Table of Contents

1. Introduction

As optical fiber technologies continue to proliferate on several fronts, one of the most interesting areas of development has been around the use of optical fibers as sensors. The most advanced technology in this arena is called Distributed Acoustic Sensing or DAS. Network Integrity Systems' (NIS) portfolio includes products which incorporate DAS technology, which further extends our leadership position in the field of optical sensing. By utilizing optical fibers either in existing optical communication cabling infrastructure or within dedicated sensing cables, NIS DAS solutions can monitor amongst other critical assets, long-haul communications networks, private trunk cable routes interconnecting disparate locations, fence lines surrounding high-profile facilities, borders and much more. DAS technology not only detects when an intrusion occurs but moreover pinpoints with extreme accuracy the location of these events. Furthermore, DAS accomplishes this without the need for separate networks of sensors and switches.

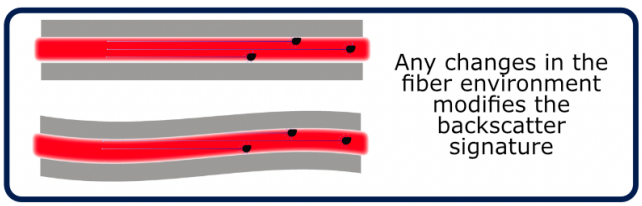
Machine Learning is revolutionizing DAS by enhancing data interpretation and anomaly detection. ML algorithms can process and analyze massive amounts of acoustic data generated by DAS systems, identifying patterns and correlations that might be missed by human analysis alone. This enables more precise real-time monitoring, predictive maintenance, and improved decision-making in industries like security, oil and gas, and infrastructure, where DAS is commonly used.

2. DAS Capabilities

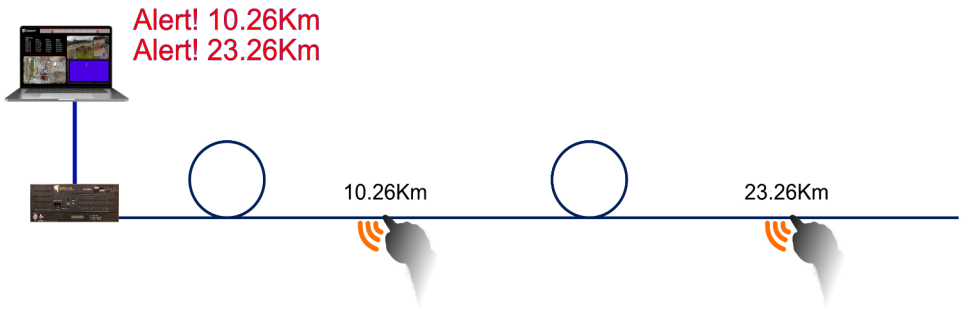
The Network Integrity Systems INTERCEPTOR™, SENTINEL™ and VANGUARD™ FOCUS Optical Intrusion Detection Systems utilize Distributed Acoustic Sensing (DAS) technology to provide long range detection capability along with pinpoint location of any physical disturbances to an optical fiber, either one installed 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.

3. DAS Technology

DAS technology is an advanced type of fiber optic sensing that works on the principle of measuring backscattered light resulting from launched probe light propagating along an interrogated fiber. In essence, DAS is Phase-Sensitive Optical Time-Domain Reflectometry. The FOCUS unit sends pulsed laser light into a single strand of single-mode optical fiber and monitors the Rayleigh backscatter from the reflected light. The Rayleigh backscatter pattern changes with acoustic and vibrational energy. Once the reflected pattern is received, it is processed and analyzed by advanced algorithms to determine the type of event.



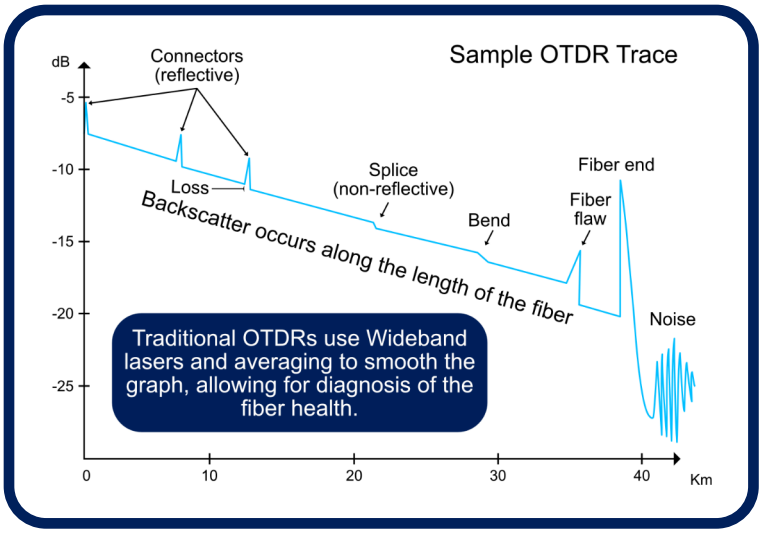
The solution is comprised of three components: the optical fiber interrogator (FOCUS hardware), a sensing fiber (single strand of single-mode optical fiber) and optionally, a response management software application operating on a local or remote server or in the Cloud. In communication network security monitoring applications, the sensing fiber is typically a spare or "dark" strand of fiber within the network cabling. In physical security applications such as perimeter fence monitoring, the sensing fiber is contained within a dedicated cable installed either on the fence or buried in the ground along the perimeter.



4. Optical Time Domain Reflectometry (OTDR)

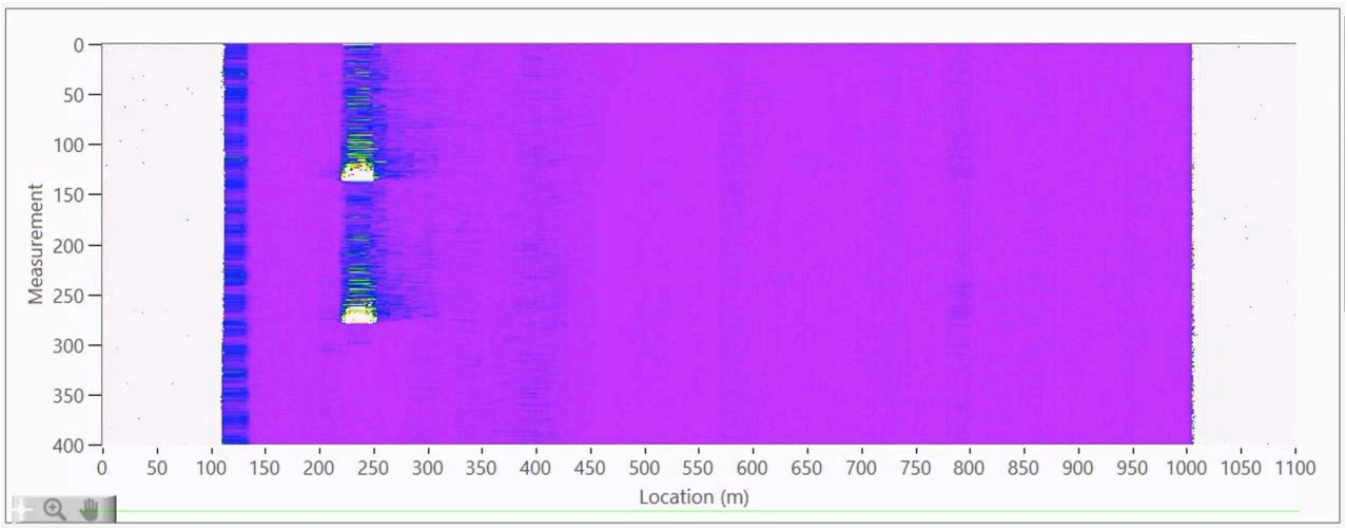
Distributed optical fiber sensors typically use a technique called Optical Time Domain Reflectometry (OTDR) to achieve the spatial resolving function mentioned above. This technique is very similar to radar, in that it uses variations in backscatter from intense, short pulses of radiation launched into 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.



5. DAS Sensing Principles

Measurable spatially localized properties of the backscattered light will vary proportionally to localized applied strain. In other words, as the fiber is strained, characteristics of the back-scattered light will vary proportionally, and can be measured. Applied strain will result from several fiber perturbations, including strain, pressure, vibrations, and acoustics. Backscatter traces are acquired as a function of intensity and time. Each individual Backscatter intensity trace is digitized at a sampling frequency of 250 MHz,. This results in a spatial sampling resolution of ~0.8m. The raw data is first digitized and stored in memory. This process is repeated for successive backscatter traces.



The resulting data sets are resolved into two dimensions: Time and Distance. Each sample point behaves like a two-path interferometer. The signal is then passed through ML signal processing algorithms for event generation. This processing allows for precise identification of the location and type of threat.

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.

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.

7. DAS Benefits

The Network Integrity Systems FOCUS solutions have several inherent benefits over existing infrastructure security options. Benefits include:

- Long distance – The low attenuation in the optical fiber enables the light to propagate over an optical fiber with a large length. If the fiber is used as the sensing medium, the sensor range can be up to 100km.
- High sensitivity – minute variations in the optical signal (such as the nanometer-level changes of wavelength or micro radian of phase) caused by slight environment disturbance can be detected.
- Low latency – The signal travels at the speed of light inside the fiber and can be detected in real-time.
- Compact and light weight – The physical characteristics of optical fiber, such as small diameters and no metal parts, make the sensing fiber compact and lightweight.
- Non-line of sight – Since the optical fiber is flexible and can be bent or curled, the fiber sensing path does not require line of sight, unlike most free-space optical sensors.
- Immunity to electromagnetic interference – Since there is no metal in the optical fiber, it does not experience electromagnetic interferences, and does not present a shock hazard during lightning.
- Robustness – The optical fiber can be deployed in harsh environments and has very good fatigue durability.

Besides the benefits in general fiber optic-based sensing solutions, DFOS solutions offer additional benefits:

- Large number of sensing points – The entire optical fiber acts as the sensor, making it equivalent to hundreds or thousands of sensors in succession, so the total capital expenditure (CAPEX) is significantly reduced compared to equivalent numbers of discrete sensors.
- Passive field requirement – All the active elements that require electricity in the DFOS system are located at the interrogator, which is usually installed at the central office, and the signal is communicated through the sensing fiber itself. Therefore, the need for communication

hardware and power supply in the field is eliminated, and operation expenditure (OPEX) for power consumption, is greatly reduced.

- Intrinsic synchronization – Since signals received from these individual sensing points are generated by common input pulses, these signals are intrinsically synchronized. This is unlike other integrated sensor systems that require complex synchronization schemes.
- Ability to localize the event – By performing the time-of-flight calculation on the backscattering signals, DFOS can pinpoint the location of every detected event.
- Ability to detect multiple events – Since these sensors are detected individually and independently, multiple events can be identified and localized simultaneously.
- Use standard fiber – Unlike some fiber optic sensors that require grating fabrication or chemical transducer coating, the DFOS can operate on standard communication-grade optical fiber without special physical or chemical modification.

8. DAS Applications

NIS DAS solutions consist of three major product groups, two of which are designed for data network monitoring and one for security applications such as perimeter monitoring:

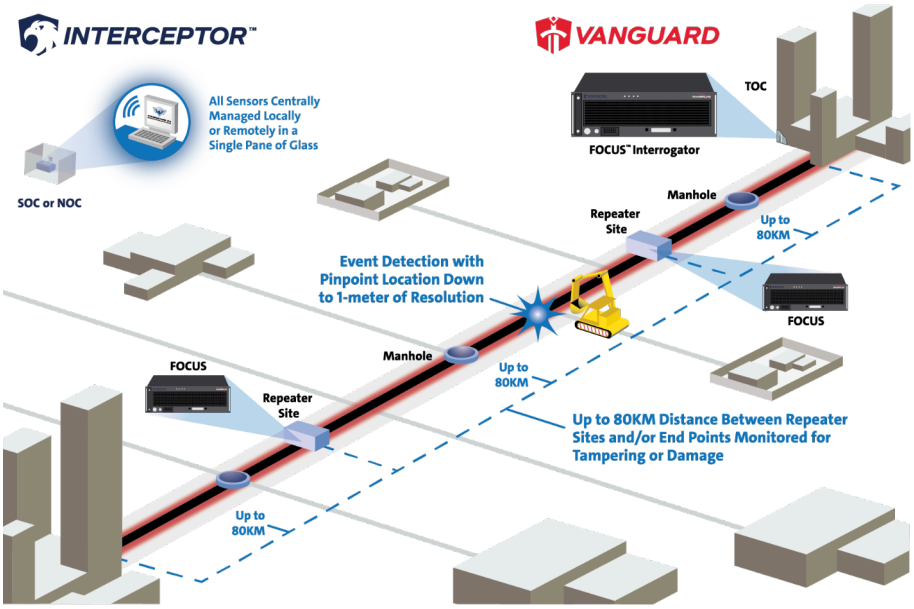
INTERCEPTOR FOCUS$^{NX™}$ – For U.S. Government data network monitoring.

VANGUARD FOCUS$^{NX™}$ – For private enterprise data network monitoring.

SENTINEL FOCUS$^{NX™}$ – For perimeter, border, critical facility, critical asset intrusion detection monitoring

8.1 Data Network Monitoring

Thanks to the technology innovation and feature enhancement in the NIS FOCUS product suite, many new or improved application solutions are available. These applications improve operational efficiency for the network operators and create new capabilities for the existing network infrastructures, bringing new business opportunities and revenues for the network owners.



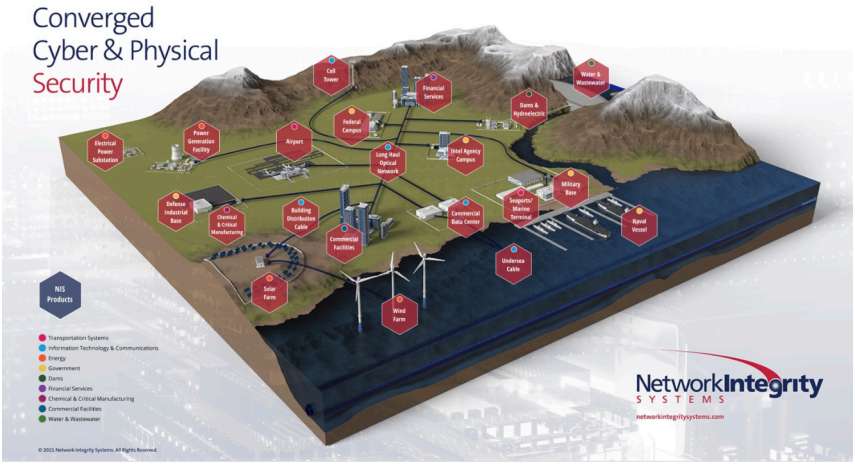
8.2 Fiber Cable Cut Prevention

Cable cut is a common problem for network operators. Not only does it cause service interruption, but it also requires costly repair efforts. Cable cut usually occurs when some unauthorized construction activity occurs around buried optical cables. Existing solutions, such as OTDR monitoring, can only detect a cable cut after it occurs. The NIS FOCUS solutions can provide early warning to network operators before the accident occurs. This is achieved by constantly analyzing activities along the cable routes to detect any abnormal activities—such as when a construction machine starts operation—and identifying possible events at those locations. The network operators will be notified and can take appropriate action before cable damage occurs.

8.3 Facility Security & Critical Infrastructure Monitoring

NIS DAS allows continuous monitoring over the perimeter of critical facilities and campuses with accurate location reports. The ML-based analytic software can classify events accurately and quickly. The user can also customize event alerts, designating what events to be alerted and what events to be treated as normal. With their long-distance sensing capability, NIS DAS products can deliver a wide range of security monitoring solutions, ranging from the perimeter of a 5G wireless tower to a data center site to harbors and national borders.

Visit NIS' Solutions Landscape virtual environment for details on specific applications:



9. Summary

NIS DAS suite of products uses a toolset of distributed vibration and acoustic sensing technologies. Applied to existing fiber optic network infrastructures or a dedicated fiber optic sensing network, it monitors various types of environmental conditions and events. A user-friendly and customizable GUI denotes the location of events-of-interest and provides actionable data in real-time. When an environment disturbance like physical movements, temperature variations, or acoustic vibrations reach the optical fibers, the sensor interrogator instantly detects and locates the signal. The solution's ML-based AI analytic engine simultaneously analyzes and classifies the multiple physical events. Integrated software immediately triggers silent or audible alarms and/or sends actionable alerts. Actionable data, such as date, time, location, and event classification can be stored locally or remotely for future reference and data analysis.

Overall, NIS DAS solutions can interrogate a long section of optical fiber, providing fine spatial resolution and the ability to localize each event accurately and instantly. These features enable

many new applications that make fiber cable network operations more efficient and yield additional network value and uses, such as smart cities, smart transportation, smart power distribution. When NIS FOCUS solutions are applied to a fiber optic communication network, the entire network becomes a giant sensor for various applications and actualizes the new Network-as-a-Sensor paradigm.

Finally, NIS DAS solutions are CAPEX friendly, as they are compatible with existing deployed infrastructure; they are OPEX friendly, because they reduce or replace large amounts of manual labor and; they are environmentally friendly, thanks to the low energy consumption of DAS compared to the use of hundreds of discrete sensors.

1937 Tate Boulevard, SE
Hickory, North Carolina, 28602,USA
Call 877.NIS.4PDS(877.647.4737)
www.networkintegritysystems.com

Network Integrity SYSTEMS