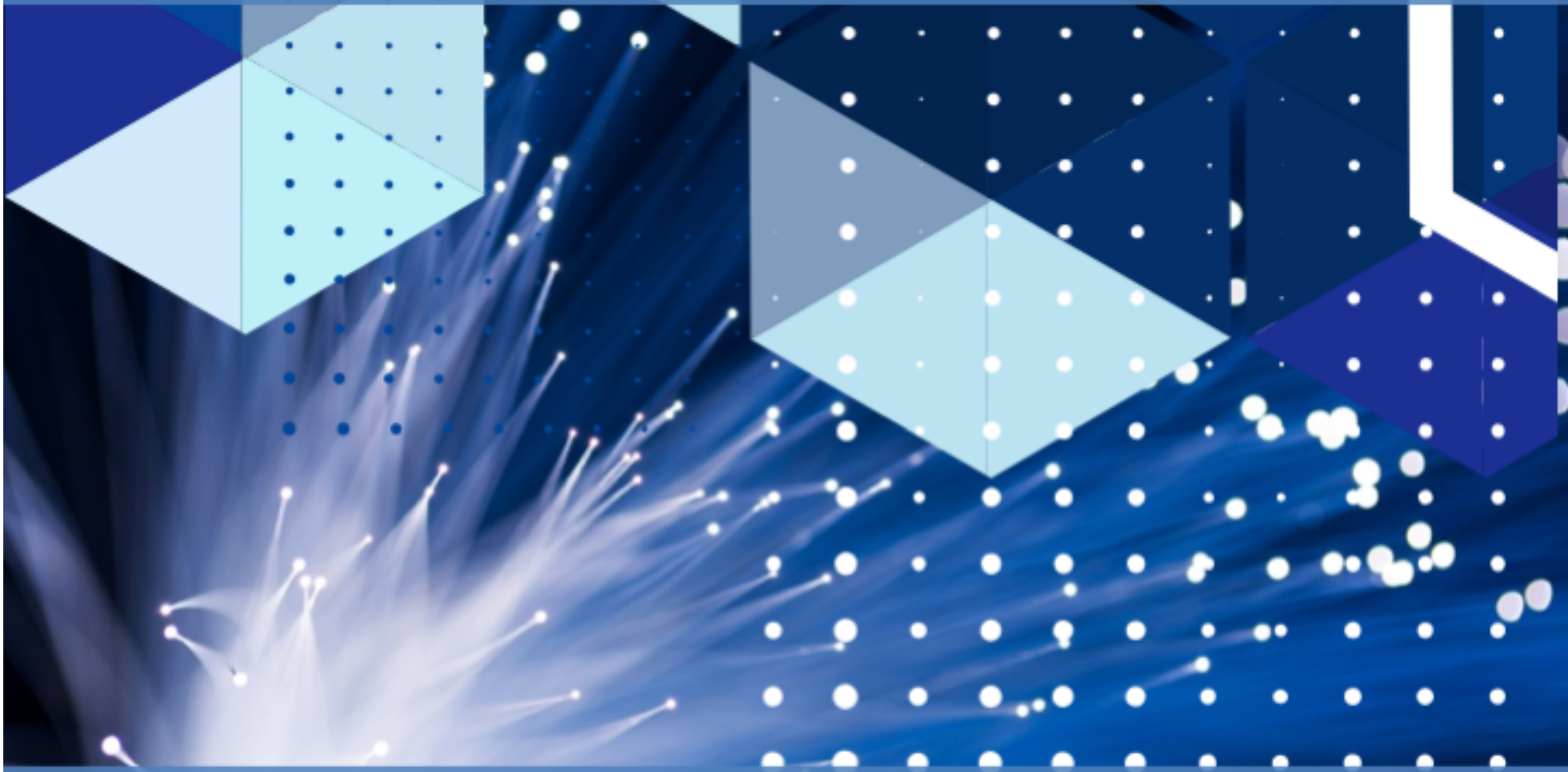
Distributed Acoustic Sensing

Distributed Acoustic Sensing technology and the impact on infrastructure security.



NetworkIntegrity
SYSTEMS

We Bring Security To Light™

Introduction

As optical fiber technologies continue to proliferate on several fronts, one of the most interesting areas of development has been in using optical fiber as a sensor. The most advanced technology in this arena is Distributed Acoustic Sensing (DAS). Network Integrity Systems' (NIS) portfolio of products now includes DAS technology, further-extending our leadership in the monitoring and security of critical network infrastructure. By making the cable a sensor, NIS DAS products now have the ability to monitor long-haul networks and pinpoint the location of security events without the need for separate networks of sensors and switches.

DAS Technology

In long-haul or outside plant (OSP) applications, high performance detection capabilities as well as pinpoint location information is required to alert operators of a real time, cable intrusion attempt and promptly direct the response team to the accurate location to quickly find and eliminate the threat.

The Network Integrity Systems INTERCEPTOR™ FOCUS Optical Intrusion Detection System utilizes Distributed Acoustic Sensing (DAS) technology to provide long range detection capability along with pinpoint location of any physical disturbances to your classified communications cable. By pulsing light down a single-mode telecommunication fiber, the Interceptor Focus will detect events caused by vibrational disturbances, such as cable handling or tampering, anywhere along that cable, up to 40km in length.

DAS technology is an extremely advanced type of fiber optic sensing that works on the principle of measuring backscattered light resulting from launched probe light that propagates along an interrogated fiber. In essence, DAS is Phase-Sensitive Optical Time-Domain Reflectometry. The INTERCEPTOR FOCUS 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, such as digging near buried conduit, cutting into conduit, and physical handling of the cable. The system will also provide precise location along the cable and monitor the event over time.

The solution is comprised of two components, the optical fiber interrogator (INTERCEPTOR FOCUS hardware) and the sensing fiber (single strand of single-mode optical fiber). The sensing fiber is typically a spare or "dark" strand of fiber located inside the customer's data cable.

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 backscattered light will vary proportionally, and can be measured. Applied strain will result from a number of 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 150Mhz, giving one sample every 6.67ns. This results in a spatial sampling resolution of ~.67m.

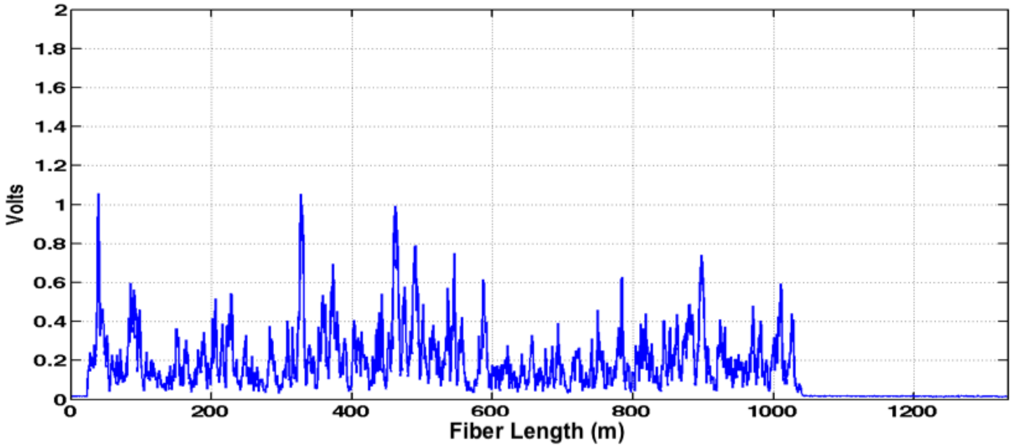


Figure 1: Single Backscatter Trace

The raw data is first digitized and stored in memory. This process is repeated for successive backscatter traces.

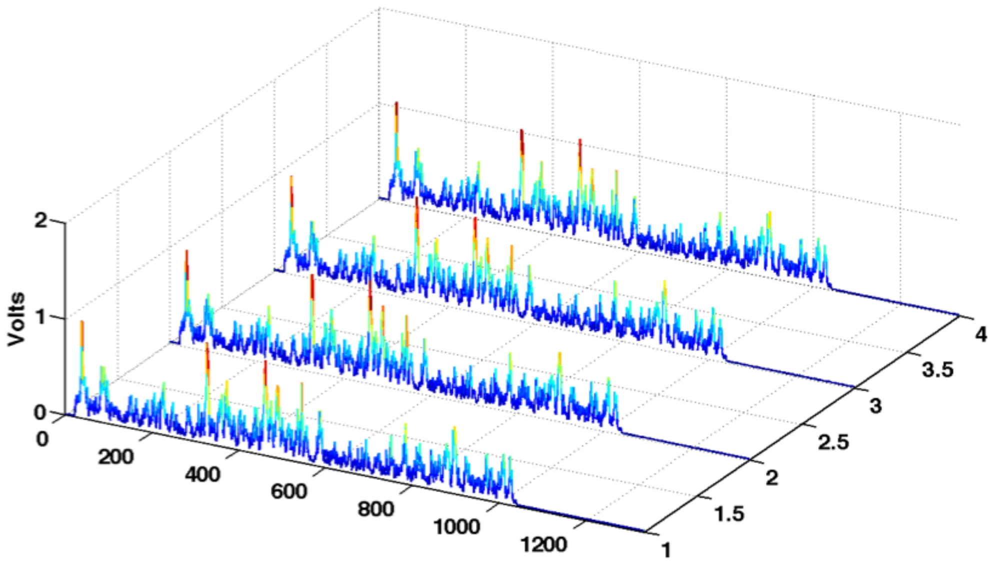
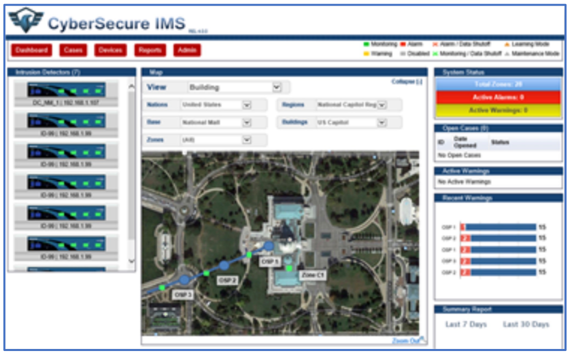


Figure 2: Successive Backscatter Traces – Waterfall Plot

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 novel signal processing algorithms for event generation. This processing allows for precise identification of the location and type of threat.

Event Handling

All of Network Integrity Systems' solutions utilize a single platform for event notification and tracking; the industry-leading CyberSecure IMS platform. CyberSecure IMS is the first application certified by the US Government to monitor and protect physical network infrastructure. This ensures that all of your infrastructure monitoring and response is handled by a single console.



DC_NM_1 | 192.168.1.107
ID-99 | 192.168.1.99
ID-99 | 192.168.1.99
ID-99 | 192.168.1.99
ID-99 | 192.168.1.99
ID-99 | 192.168.1.99

View: Building
Nations: United States
Regions: National Capitol Reg
Base: National Mall
Buildings: US Capitol
Zones: (All)

Total Zones: 20
Active Alarms: 0
Active Warnings: 0

ID	Date Opened	Status
No Open Cases		

No Active Warnings

Summary

The Network Integrity Systems INTERCEPTOR FOCUS solution has several inherent benefits over existing long-haul infrastructure security options:

- Utilizes existing fiber optic infrastructure
- Real-time threat sensing with pinpoint location
- No powered devices in the field
- High performance w/ low maintenance
- Consistent sensing over long distances
- Immune to EMI, RFI, and lightning
- Cost effective security solution