NetworkIntegrity SYSTEMS

USE CASE

Long-haul Infrastructure Monitoring

Gaining control of your long-haul optical infrastructure

Executive Summary

Long-haul fiber-optic infrastructure has become the primary means for transmitting information around the world. The importance of monitoring this critical infrastructure cannot be understated, and neither can the risks of leaving the infrastructure unmonitored. Everything from the environment, to unapproved changes, to malicious intrusions can wreak havoc on the critical connections across a campus, a city, and beyond.

Newly developed Distributed Acoustic Sensing (DAS) technology in Network Integrity Systems' **VANGUARD FOCUS** infrastructure cyber security solution provides the remedy to these issues by giving you end-to-end, real-time visibility of your long-haul infrastructure health and security. By creating a sensor along the entire length of the cable, any event related to that cable is identified, tracked, and alarmed where necessary, reducing the potential risk for downtime or data security breaches.

Long-haul Infrastructure Challenges

Long-haul networks have faced a variety of risks related to the maintenance and security of the physical infrastructure. Those challenges come from a couple of different areas - people and processes.

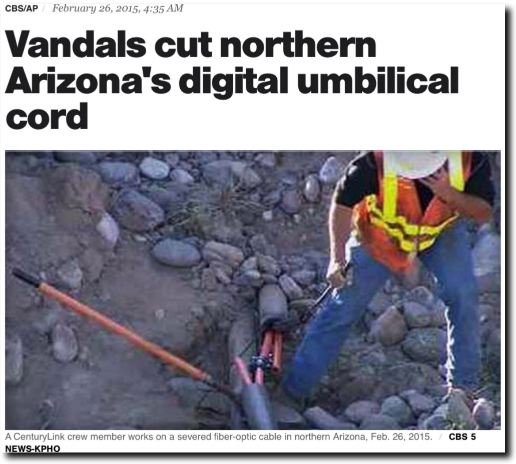
People-related risks:

- Malicious events - Events caused by things such as vandalism, tampering, or even terrorism.
- Unplanned events - Downtime caused by digging, maintenance errors, or construction.
- Criminal events - Outages caused by cable theft attempts, or data loss caused by tapping.

Process-related risks:

- Fault location issues - Inability to quickly identify the location of a failure.
- Documentation errors - Untracked or incorrectly documented changes.
- Environmental events - Unanticipated impacts to infrastructure from flooding, earthquakes, fires, etc...

With all of the risks facing long-haul infrastructure for public utilities and private companies alike, it's time to begin proactively monitoring and maintaining critical infrastructure paths to prevent or reduce the impacts of these events, which could have a catastrophic impact to your business and affect the lives of your customers.



CBS/AP / *February 26, 2015, 4:35 AM*

Vandals cut northern Arizona's digital umbilical cord

A CenturyLink crew member works on a severed fiber-optic cable in northern Arizona, Feb. 26, 2015. / **CBS 5 NEWS-KPHO**

An attack involving IT can take different forms. The IT itself can be the target. Or, a terrorist can either launch or exacerbate an attack by exploiting the IT infrastructure, or use IT to interfere with attempts to achieve a timely response. Thus, IT is both a target and a weapon.

Information Technology for Counterterrorism: Immediate Actions and Future Possibilities

What if you could predict an outage or intrusion before it happened?

Impacts of those Challenges

Some of the side effects of these challenges include the requirement for increased redundancy, which adds to the cost and complexity of the network. The long-haul nature of the network means that the simple process of verifying a proper cabling change requires a lot of time. Troubleshooting intermittent problems is nearly impossible, adding to the cost of operating the network.

Long-haul network outages are also extremely expensive. The all-hands-on-deck response required to resolve the outage distracts personnel from other tasks. During the outage, alternate circuit paths can become over-utilized, reducing the efficiency of the network. Resolution is often complex and finding the root cause is very difficult. In the end, outages can affect careers, income, performance objectives, and company value.

Distributed Acoustic Sensing is a Game-Changer

Until now, maintaining a long-haul fiber optic infrastructure has meant waiting for outages to occur and responding when that time comes - aside from routine visual inspections, there weren't any other options. Finding taps or other intrusions that put data at risk were left to chance. The critical nature of today's networks require a new solution.

While burying a cable and hoping for the best was the only option in the past, Distributed Acoustic Sensing is the future. DAS utilizes your existing fiber-optic infrastructure to create a system of sensors, leveraging the unique properties of optical fiber. This sensing system allows for continuous, automated monitoring of your layer one optical infrastructure.

The advantages of this type of monitoring solution are many:

- Immediately detect an event related to the cable AND/OR the surrounding area - Detect a backhoe as it starts to dig, not after it severs the cable.
- Differentiate between events - know the difference between a backhoe starting to dig and a lawn mower mowing the grass. The system will detect both, but will only alarm on the backhoe.
- Identify the exact location of the event - the precise resolution of the sensor allows you to immediately understand where the event is occurring.
- Prioritization of response - understanding the cause of the event and the precise location allows you to send the right people and assets in response.
- Detailed map of the cabling environment/path - Any Move/Add/Change work related to the monitored infrastructure will be detected and logged making undocumented changes a thing of the past.
- Virtual segmenting for different risk areas - assign different response priorities and methods to different segments of the monitored system.

Network Integrity Systems has the Solution

Network Integrity Systems' **VANGUARD FOCUS** is a network infrastructure cyber security solution utilizing state-of-the-art Distributed Acoustic Sensing (DAS) technology to provide long-range capability and pinpoint location of any physical disturbance to your communications cables, anywhere along those cables, up to 50km in length per segment.

Network Integrity Systems solutions are used to protect the most sensitive networks in the world from intrusion and tampering. With systems deployed all over the world, we are the leading experts in Physical Layer One security. Our systems have been tested against the most state-of-the-art, classified intrusion methods know to exist. Combined with our innovative technology, our advanced management console enables real-time monitoring without the false alarms that can plague other systems. Our world class customer support and responsiveness ensures that support is there when you need it. Contact us today to learn more!

> "On land, it's not nearly as difficult," said Tim Chovanak, a defense consultant who specializes in network taps and digital forensics. "The easiest thing to do would be to somehow get an agreement with a provider and just simply co-exist in a building, one of the main fiber stations, (peering) points or whatever. In other words, work out something with either a long-haul provider or with an employee."
>
> NSA eavesdropping: How it might work