Customer

A Defence Related Customer

Problem Statement/Requirements

The customer wanted a mechanism to render their optical fibre links to be intrusion proof with physical layer security solutions deployed on the fibre-optic networks to limit the risk of being exposed to data theft and to detect possible cable threats. The mechanism should also provide advance warning to prevent optical fibre cables getting cut or damaged inadvertently by construction equipment or due to digging which can cause network downtime, by gathering advance information about such prospective cable cuts. Additionally, it should provide continuous monitoring on the optical fibre infrastructure health and also perform proactive maintenance.

Solution Methodology

SFO developed the SecureLink FIPS unit which is a user friendly Centralized Management System with Tree View providing a complete view of all activity down to the individual level. A pair of FIPS is deployed to monitor a link of 65km and another pair for the next 65 km. The FIPS units are connected to the IP Network from where the data from the units flow to the EMS Servers thus allowing remote monitoring of real-time data. The EMS server is in turn linked to the Network Management System enabling the interaction between FIPS units and users. The EMS Servers reside at the Network Operating Centers (NOC) spread across the country. There is a central NOC and a Disaster Recovery NOC to provide central data management, redundancy and disaster recovery.

The FIPS units monitor the entire cable by monitoring a few dark (sensory) fibres. Pluggable AFM modules are available for monitoring active fibres (future upgrade). A laser beam is transmitted along the existing fibre optic communications cable, and the returned signal is automatically monitored and analyzed for disturbances. This same signal is then digitally processed to identify and remove nuisance alarms.

Key features of SecureLink FIPS are:

- 19" Rack Mountable, 8U Height; Optional Active Fibre Monitoring Module 4 U height
- Operates on 230V AC
- Secured User Access for configuration and device management
- Web access for clients
- SNMP V3 based remote management and control and hence compatible with third party NMS
- DCN connectivity through Ethernet
- Bit rate and protocol independent
- No electronics or power in the field
- User Configurable Thresholds and Alarm Settings
- Alarm notification through SMS/E-mail
- Dry contact alarm for external interface (Optional)
- Keeps log of alarms, trace data etc.
- Upgradable with hot pluggable feature.

Brief description of product:

A. Hardware

The FIPS system has two major components. The mainframe is a 6U sub rack with a CPU module that manages both the SecureLink subsystem as well as the Active Fibre Monitoring subsystem.

Secure Link Subsystem

The Secure Link subsystem is built on Industrial PC architecture. The key component of this system is the optical subsystem which implements the patented intrusion detection technology. This system uses three dark fibres per segment to facilitate the monitoring of an entire cable.

Active Fibre Monitoring Subsystem

The Active Fibre Monitoring Subsystem consists of 6 plug in modules, each with capability to monitor 8 data carrying fibres. This system shoots a laser that is well outside the band of the signals in use by the fibre, and detects the minute changes that happen due to intrusion activity.

Optical Time Domain Reflectometer (OTDR)

The OTDR module is a part of the AFM system. It is used to localize the intrusion, by measuring the optical distance to the anomaly in the fibre.

B. Software

The IPS system has the following software components:

CPU: The main CPU runs a custom built Linux operating system. It supports various communication protocols, including SNMP, Web Service, SSH and SFTP.

AFM: The AFM modules use a highly optimized RTOS to run the intrusion detection algorithms

Secure Link Module: This module runs on Windows operating system on an Industrial PC.

Impact

- 24/7 monitoring of illegal data tapping and advance warning about prospective cable damages.
- Highest levels of detection simultaneously with an extremely low Nuisance Alarm rate due to the intelligent event discrimination and analysis utilized.
- Locates the events with an accuracy of ±20m.

About SFO

SFO Technologies Pvt Ltd, the flagship arm of the diversified conglomerate, the NeST Group provides end-to-end design-engineering-software-manufacturing solutions to clients across geographies such as the USA, Canada, Europe, Middle East, South East Asia, Japan, Australia, and India. SFO has invested in building competence, scale and standards compliant process framework, in PCBA, fibre optics, Cable & wire Harness, Magnetics, High Level Assembly, VLSI design, embedded software development, etc. SFO's capabilities transcend the plain vanilla "Build-to-Spec or Build-to-Print" EMS and our ODM+ solutions are rapidly re-defining standards for the OEMs across Aerospace & Defence, Communications, Transportation, Healthcare and Energy & Industrial domains. .