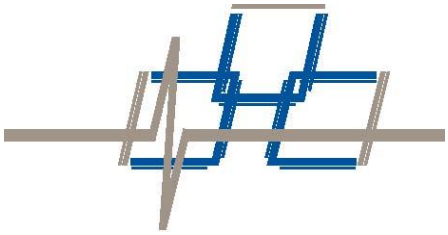
Fiber SenSys
DATA SECURITY

Protective Distribution Systems for Passive Optical Networks



Introduction

Protected Distribution Systems (PDS)[1] are designed to deter and/or detect intruders that are attempting physical access to the communications infrastructure (predominantly fiber optic) carrying national security information and other types of sensitive and important data. Performance standards for PDS are stipulated to provide adequate safeguards to permit the transmission of unencrypted classified information over PDS protected systems.[2] This document describes the use of Fiber SenSys' SecurLAN products in PDS involving passive optical networks (PON).[3]

SecurLAN Technology

SecurLAN® is a technology invented by Fiber SenSys, Inc. (FSI) in 1996 that senses accidental or intentional intruders that are trying to access a fiber-optic cable (at the physical cable layer) in order to engage in physical (layer one) tampering. SecurLAN also plays an important role in overall network uptime and service level discussions. The technology works by using a spare fiber inside the multi-strand cable as a distributed sensor. When an intruder attempts to cut into the fiber-optic cable they introduce tiny amounts of strain in the sensing fiber. This strain is detected by specialized electro-optical SecurLAN equipment, which alerts the Head End (and appropriate network security managers) to take appropriate measures such as investigating the cause of the intrusion and rerouting data away from the suspected intrusion.

Fiber SenSys manufactures SecurLAN equipment for protecting optical networks that use either single-mode (SM) or multimode (MM) fiber, in virtually any type of cable and virtually any type of optical network.[4] Because SecurLAN uses spare fibers, the data rates, protocols, and other performance specifics of the optical network data stream are irrelevant; only the specific type of optical fiber matters. When specifying a SecurLAN product, it is recommended that designers and specifiers make sure to indicate whether the fiber is SM or MM.

Passive Optical Networks

In addition to various topological configurations, optical networks also differ in the way they route signals. In active networks, signals are electronically detected and converted from photons to electrons. They are then conditioned, buffered, switched (as necessary) and re-transmitted over another fiber-optic circuit.

---

[1] PDS is commonly used to protect SIPRNet and JWICS networks. Standards for PDS are found in NSTISSI 7003, which describes the requirements for systems in the U.S. and for sites subject to low-medium threat outside the U.S.

[2] A complete protected distribution system protects more than just the transmission media (typically optical fiber) and includes additional systems such as subscriber/terminal equipment.

[3] SecurLAN is a generic technology than can be used in PON as well as all other fiber-optic networks.

[4] The cable must have at least one un-used optical fiber, however. This un-used optical fiber is what SecurLAN uses as the intrusion sensor.

Active networks are highly flexible and configurable but they tend to be expensive because of the cost of the active components and the need for maintenance. Passive optical networks have a lower cost and more reliable because they route signals passively, without using powered electronic network elements. Figure 3 illustrates the basic kernel of a passive optical network (PON). In a PON, an optical line terminal (OLT) transmits through a passive splitter to multiple optical network units (ONUs) located near end users. A PON is thus a point-to-multipoint network that uses passive (unpowered) optical splitters to enable a single optical fiber to serve multiple users.

As can be seen in figure 3, downstream signals are broadcast to the ONUs. The ONU can also broadcast upstream signals, which are combined using a multiple access protocol like time-division multiplexing (the OLT stipulates time slot assignments for upstream communication in order to prevent data collisions).

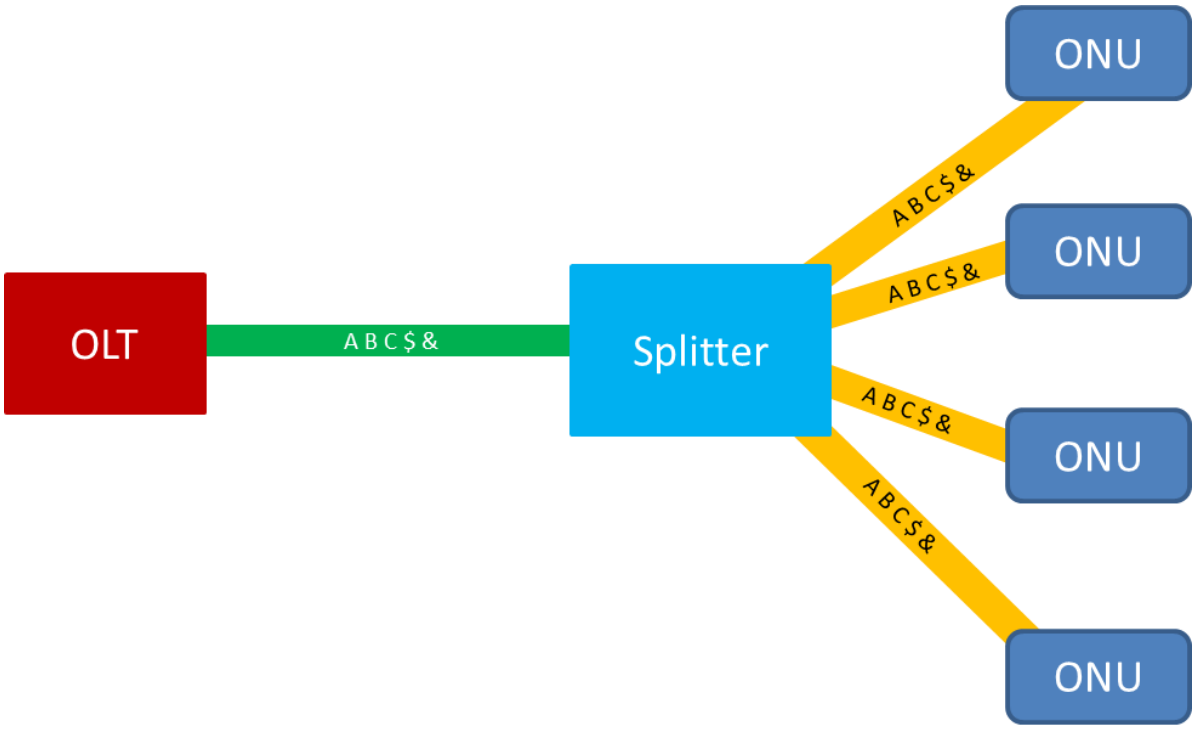


Figure 1. Basic kernel of a PON.

Installing SecurLAN in a PON

SecurLAN is a versatile physical network sensor that is enabled using several deployment options. For a complete overview of SecurLAN for PDS, please visit the FSI website (www.fibersensys.com).

SecurLAN for PON technology involves dark (unused) fibers in optical cables that are used as distributed sensors in order to determine if an intruder is trying to cut into the cable, tap the fiber-optic network, or otherwise physically intrude upon the infrastructure. It is also used to ensure network uptime and detect either intentional or accidental physical network intrusions by protecting the physical cable. SecurLAN is designed to detect small amounts of strain that are transferred to the sensing fiber when the cable is accessed. When the electro-optical alarm processing unit (APU) senses an intrusion, it signals an alarm, allowing the investigation of the intrusion or the shut-down or re-routing of secure data.

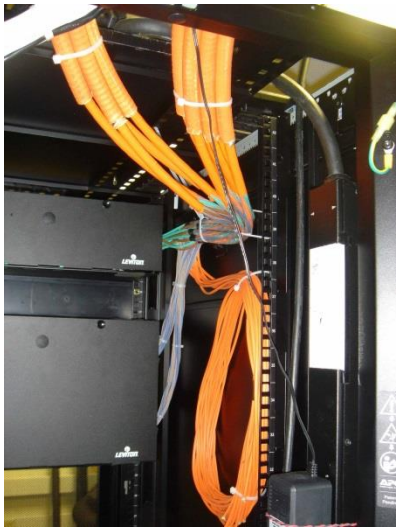
Since SecurLAN uses dark fiber (where no data is transmitting through the spare fiber), it is unaffected by data protocols or bandwidth in the PON. The only distinguishing feature of the PON (that is of importance to SecurLAN) is the type of sensing fiber (SM or MM) in the cable that houses the PON transmission fibers.

Because of the modal characteristics of MM optical fibers, splitters are made almost exclusively of SM fiber. SM fiber is also desirable for high-speed data transmission, as dispersion and loss are both lower in SM fiber than in MM fiber. For all these reasons, PON is almost exclusively constructed with SM fiber. Still, it may be desirable to construct the PON with some MM sensing fibers in the PON cables, so that these fibers can be used as sensors in the PDS.

Generally it's preferable to have independent zones for each ONU, as this makes location and identification of intruders quicker and easier. However, if it is not necessary that each ONU be protected by an individual/independent zone, then it's possible to use the SL508-SM to secure many different PON splitters, as shown in figure 4.

Observe that the configuration in figure 4 uses two SM fibers in each of the cables that run between each ONU and the PON splitter. These fibers are spliced[5] together at the ONU and the splitter, as shown in the diagram, creating a single length of sensing fiber that runs all the way from the SL508-SM to the end-termination unit in the PON splitter box. Using this configuration, one SL508-SM could be used to protect up to 8 PON splitters, each supporting up to 32 ONUs. The total number of ONUs protected in this scenario is 256.

[5] Fiber-optic connectors might also be used, but since splices are more reliable, and have lower optical loss, they are preferable to the use of connectors.



Single-mode sensing fibers in the cables that go from the PON splitter to the various ONU

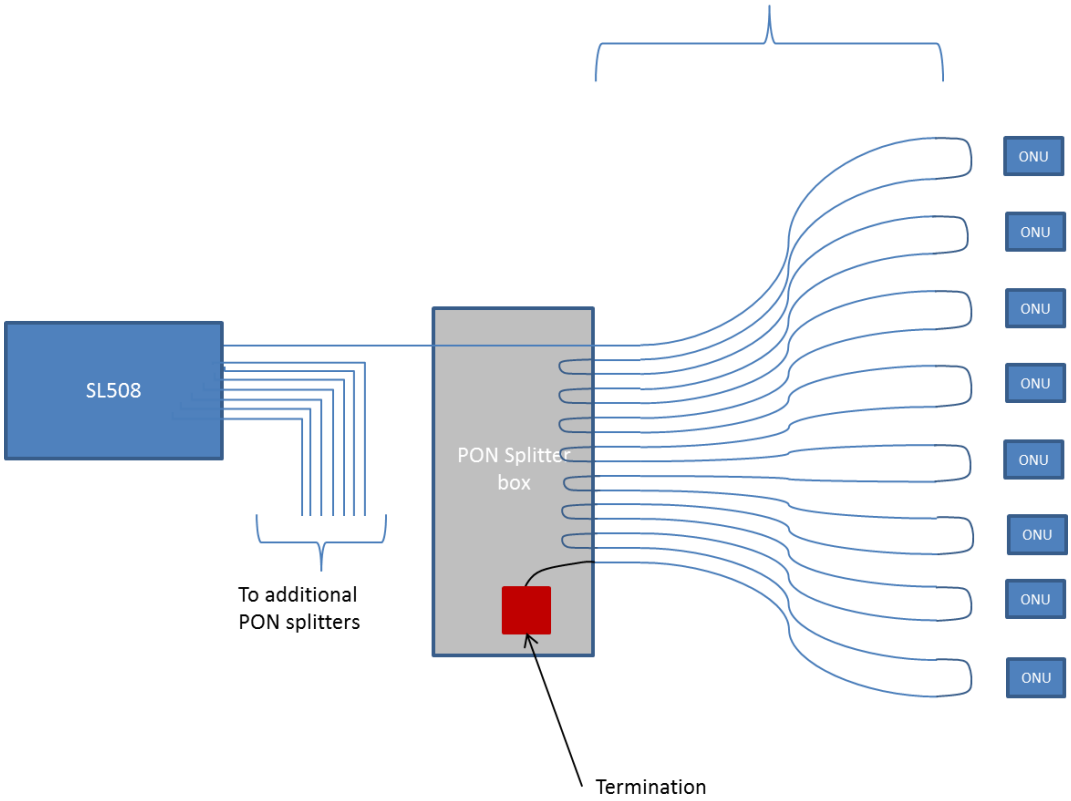


Figure 4. SL508-SM deployed in a PDS PON. All fibers are SM. In this configuration, the cable between the OLT and splitter, as well as all the cables between the splitter and all the ONUs, are one zone. A similar configuration could be used with PON architecture having 1-by-32 splitters.

Depending on the application, it may be desirable to place the APU near the PON splitter. This can be done using either the SL508-SM or the 25-zone capable FD525 APU. In some environments, it may be desirable to have independent ONU zones. However, if the ONUs share zones, then one SL508-SM can always be configured to protect each PON splitter box and associated OLT and ONU.

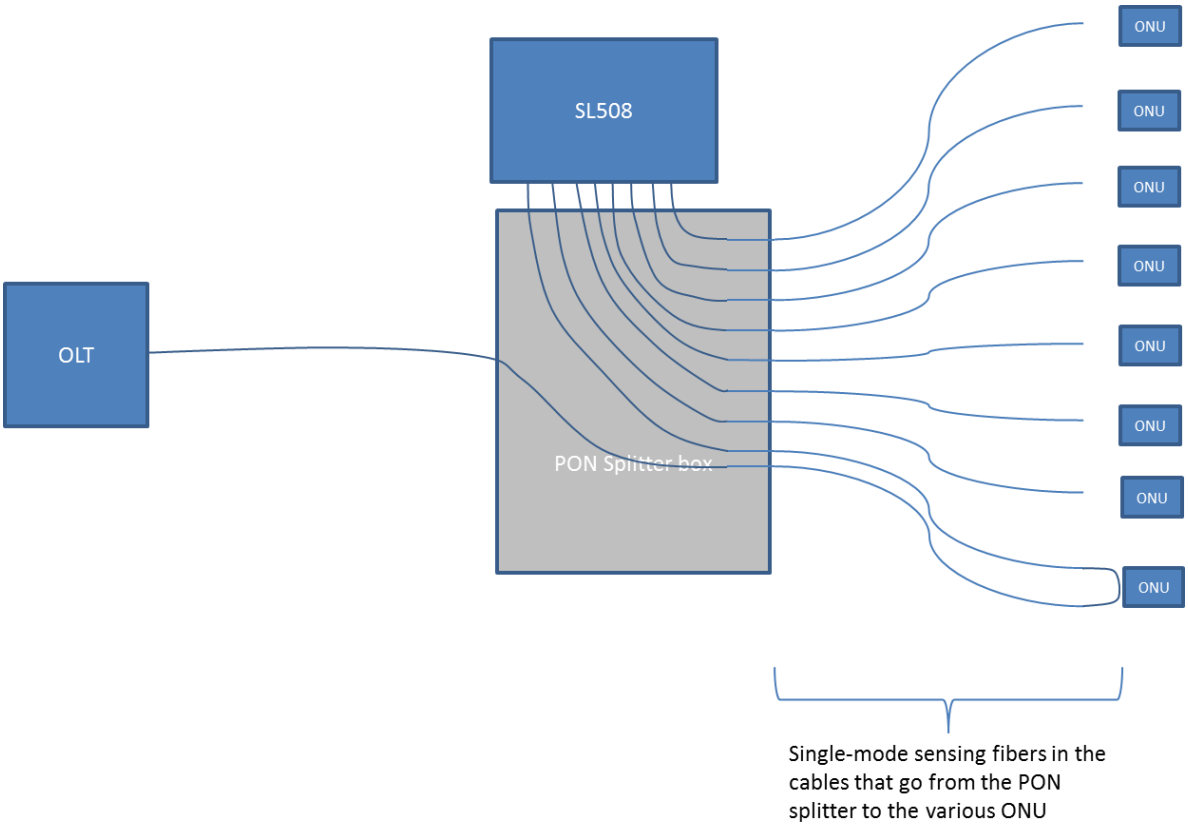


Figure 5. Protecting the PON with an SL508-SM at the splitter box.

Conclusions

As shown in this whitepaper, a wide array of design options are available for the protection of PON installations, depending on the specific intrusion detection response requirements at each project location. With this technology, individual ONUs or groups of ONUs are configured for maximum SIPRNET or JWICS physical protection.

Fiber SenSys offers several solutions under the category of “SecurLAN” to deliver NSTISSI 7003 Compliant Voice, Video & Data over a secure PON fiber infrastructure. In particular, the FD5XX/SL5XX series of APUs is based on a time-domain multiplexed configuration that uses the same topology as PON, and overlays PON networks seamlessly and efficiently, providing high-security solutions for physical protection of the network. Furthermore, SecurLAN does not utilize the same fibers that are used to transmit data over the PON, so it can never interfere with data transmission. And, because it uses dark fiber, SecurLAN protects all fiber-optic networks; whether ATM, BPON/, OC-12, GPON, etc. SecurLAN provides full physical-layer protection regardless of data protocols or bandwidth.

As with any alarm system, minimizing the nuisance alarm rate (NAR) is critical to efficient use and high security. Toward this goal, SecurLAN provides sophisticated, tunable digital signal processing algorithms that provide optimum probability of detecting attempted intrusions, while minimizing the nuisance alarm rate. Each zone is manually tuned to address the environmental conditions of each specific environment. Solutions are also available within the software to tune multiple zones that have identical environmental conditions.

In a typical fiber-to-the-desktop (FTTD) PON, the OLT provides service for 32 ONU and a PON with multiple OLT can support hundreds ONU. Because of its high zone count per APU (up to 25 in the FD525), SecurLAN can overlay the PON architecture, providing individual zone protection for each ONU in systems where competing solutions may sometimes only provide one zone per OLT. This document outlines a small sample of possible configurations using the SL508-SM in PDS PON, and there are additional configurations based on new products that are planned for Q2 2014 and beyond.

About Fiber Sensys, Inc.

Fiber SenSys, Inc., an Optex Group Company, is the market leading manufacturer of intrusion detection solutions for commercial, government and military installations, including airports, oil refineries, solar power generation farms, electrical substations, nuclear power plants, secure government networks, secure commercial facilities, and other critical infrastructure facilities.

For more information, contact us at:
info@fibersensys.com
Tel: +1(503)692-4430
Toll free (US) +1(800)641-8150

Fiber SenSys
High Performance – High Reliability – High Security