Fiber SenSys Alarm Processors

Fiber SenSys manufactures reliable, high-performance fiber-optic intrusion detection solutions for a wide variety of markets: government and military installations, airports, oil refineries, electrical substations, nuclear power plants, water purification and storage, corporate headquarters, manufacturing facilities, palaces and residential facilities are only a few common examples.

Fiber SenSys is the world leader in its market, with its fiber optic intrusion detection systems deployed at hundreds of sites around the globe. Electromagnetic and radio interference, traffic, lightning, and other common sources of nuisance alarms do not affect these systems. Installation is straightforward, using only simple hand tools, and the sensor systems require almost no maintenance. These products are economical, reliable, and effective. In addition to keeping intruders out, Fiber SenSys intrusion detection systems can be used to protect one of the most important resources – information.

Fiber SenSys offers two product families; *The Fiber Defender*® *models* can be used in indoor/outdoor applications and can be configured as fence sensors, wall cap sensors, or buried/ground sensors. *The* SecurLAN® *system* protects data flowing between computers through conduits and cabling trays, stopping potential security breaches that many IT managers may not be aware of. The Optical Cutoff Switch is an optional accessory for the SecurLAN® system. The Optical Cutoff Switch removes or diverts the flow of optical data through a network data cable that has been compromised by physical intrusion.

For more information, go to: www.fibersensys.com

Brian Burnett, MRV Communications

Intelligent Alarm Management using the MRV LX Series.

The MRV LX out-of-band network (**OOBN**) manager has given Fiber SenSys a complimentary solution to their **Alarm Processor Units (APU)** with a higher level of intelligence, remote monitoring and configuration, and automatic actions based on the LX's user configurable triggers and SNMP notification. With the solution in place, Security managers, utilizing these sophisticated optical fiber sensors and LX OOBN for high security facilities can now tailor the overall solution to meet their own security needs.

Fiber Sensys Spectraview manager and the LX

The Fiber SenSys APU is offered in different models for different physical installations like: Fences, Walls, Buried, Ground mats, cable conduits, etc). Some installations span a number of miles and accessing the APU's is time consuming and sometimes, not practical. Until the introduction of the LX, trained personnel had to calibrate and configure each unit in the field with a hand held device or a laptop running the Fiber SenSys *Spectraview Manager Software Application*. Things like wind, vibration, shockwaves, and other conditions can trigger false alarms. With the LX units set up to support remote access to the APUs, Security personnel can now connect to any of the APU's utilizing the *Spectraview* application from a central location. This remote access provides for real-time monitoring and calibration of the remote APU without the security personnel having to go into the field.

Megavision Pro, the LX, and SNMP

The existing management platform messaging was proprietary and is not as scalable as the LX used in conjunction with SNMP and Megavision Pro. Additionally, the solution was bulky and took up significant rack space for large installations. Now alarms can be passed over the network using SNMP, and the security personnel have a real-time, event horizon alarm notification system that contains real-time data as well as the ability to retain historical data for reporting, trending, and auditing purposes. A greater number of installations can be supported in a smaller overall footprint. Megavision Pro also gives the security personnel visual alarm notification on their desktop screens so they can quickly and efficiently react to alarms and events.

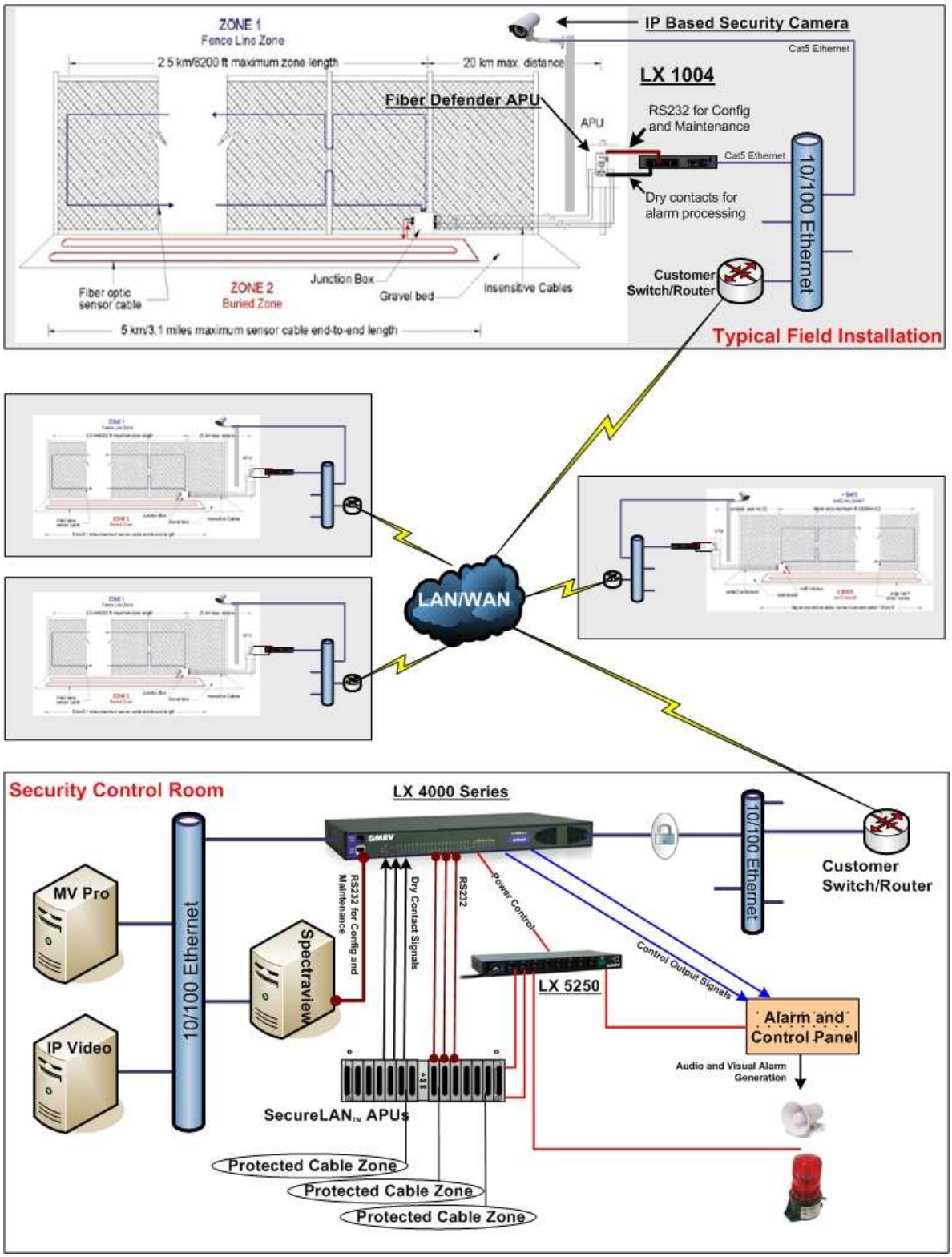

Figure 1-Typical APU/LX Configuration

Brian Burnett, MRV Communications

How the solution works:

Each APU will alert the remote LX of different alarm conditions (Critical, Warning, Tamper Switch) based on "Form-C" dry contact closures. Until the MRV LX product was introduced, security managers had to transmit alarm conditions on 2 or 4 wire copper extenders, or by modems to the alarm control panel in the main security control room. This solution poses numerous challenges and the information is not secure. Fiber SenSys enlisted the help of MRV Communications to help solve their problem.

Since the MRV LX is a network based security appliance, it allows for network based, encrypted TCP/IP communications to a central site or numerous operation centers simultaneously.
The applications that are supported in the combined MRV / Fiber Sensys installation are:

1) The Fiber SenSys APU's dry contact events are recognized by the remote LX and then the remote LX sends those alarm conditions via customized SNMP messages to a centralized MRV Megavision Pro Server. This utilizes a customer owned and operated standard TCP/IP network. The components required to build the network are readily available in the marketplace from vendors like MRV. Because the LX is network based, it allows the security managers to use a variety of different networking topologies including switches, routers, wireless access points, free space optics, etc.

2) The LX "Clustering" feature is implemented and it allows for the remote LX 1000 units to send control output commands over the network to the central LX 4000 connected to an alarm control panel for audio and visual alarms. By asserting or deasserting voltage on the control output pins, the alarm control panel can then power external notification alarms such as horns, buzzers, sirens, strobe lights, etc. Utilizing the MRV LX clustering feature also allows for shared parameters and software updates to the LX for management efficiency.

3) The MRV Megavision Pro server will initiate two different applications depending on a specific alarm condition reported. Configuring specific alarm actions within the Megavision Pro Server, allows the security personnel to automatically launch specific applications for surveillance and camera control.
    i. Critical - In a critical alarm condition, Megavision Pro will call up the customer's video security application with the node id of the camera that matches the area under surveillance by the Fiber SenSys APU. The security personnel then can visually monitor the zone where the alarm condition occurred without manually

having to react first to the Megavision alarm and then second to navigate to an external application to call up the camera. This saves valuable time when responding to a critical alarm condition.

ii. Warning - The remote LX will initiate a script to change the destination for the Spectraview application. This is done using the clustering and scripting capabilities of the LX and the "TCPPIPE" feature. Megavision Pro will launch the customer's SpectraView application and automatically connect the application to the APU where the warning message occurred. The security personnel can now use the calibration and maintenance utility to adjust or monitor the individual APU from a central location. This feature saves the security personnel from constantly having to ignore warning messages until they can physically go out into the field and adjust the APU. The TCPPIPE feature creates a seamless data pipe for the serial PC application connected to a given APU. Additionally, the robust scripting capability allows for even more advanced functions based on what the security personnel wants to do.

Required components used in this solution:

The Fiber SenSys application utilizes a generic LAN/WAN architecture for the alarm management transport. As stated previously, the network topology is agnostic to the overall solution, as long as the network is bridged (switched) or routed using TCP/IP. The critical elements involved in the solution are:

Field level components used in this solution:

- Fiber Sensys Fiber Defender APUs in the field connected to an LX-1004 via a single RS-232 serial connection and two to four dry contact closures.

- IP Cameras-Used for real-time monitoring of protected zones.

Security Control Room level components used in this solution:

- One or more LX-4000 series that are:
  - Connected to the SecurLAN® APUs with an RS-232 connection and 2-4 dry contact closures
  - Connected to the alarm control panel with control output connections. This will vary depending on how many external devices need to be controlled via the Alarm and Control Panel.
  - Connected to 10/100 ethernet along with the MRV Megavision Pro Server and the Fiber Sensys Spectraview Manager

- Optionally utilizing the MRV LX-5250 for power control of SecurLAN® APUs and other devices for power control.

In Conclusion, a business case for the solution:

Physical security is the base layer of an overall sound security policy. Utilizing a physical intrusion detection sensor for physical network security can help determine if a threat is cyber (logical) or physical - and thereby accelerate the investigation and identification of the network problem. In the context of "Total Network Protection", Layer One security considerations, and the awareness of the vulnerability at the physical layer is projected to increase in importance as security and risk managers seek a complete threat mitigation posture.

Utilizing sophisticated physical security sensors can mitigate the overall threat to a given facility that can cause untold damage to personnel or sensitive products or sensitive information. The combination of the Fiber Sensys APUs, the MRV Communication LX servers, and Megavision PRO, offers a very sophisticated level of layer 1 physical intrusion detection with the necessary alarming and reporting tools to satisfy even the most demanding security installations.

The overall solution makes sound business sense when considering it against utilizing older, more propriety alarming and reporting mechanisms. The MRV LX acts as an intelligent gateway or proxy for the APUs installed in the field. Readily available network technologies from companies like MRV Communications offer a flexible, cost effective transport of alarm notification messages and automated processing of alarms to a centralized security control center thus increasing the overall effectiveness of a layer 1 physical intrusion detection system.