Tuning and Calibration for Alarmed Carrier PDS

Introduction

Physical protection of networks and the security of Protective Distribution Systems (PDS) has been a primary application of the Fiber SenSys, Inc. (FSI) Alarm Processor Units (APUs) since 1996. Over the years, our products have been continuously evaluated and approved by Certified Tempest Technical Authorities (CTTAs) within the Department of Defense (DOD).

Most recently, the **SecurLAN®** Model SL508 alarm processor unit was developed specifically for use in alarmed carrier PDS systems. This APU has been evaluated and tested by Space and Naval Warfare Systems Command (SPAWAR), the U.S. Air Force, and the U.S. ARMY. Although **SecurLAN** products have been implemented primarily by the U.S. Federal Government, Fiber SenSys also has numerous private sector customers including financial institutions, healthcare facilities, casinos, and many others.

Each facility or campus is unique, with its own set of characteristics and environmental conditions. FSI provides tuning and calibration software tools for adjusting the APUs. For optimal performance, each FSI Alarm Processor Unit is tuned and calibrated to match the specific environment that it is protecting.

Possible nuisance alarms caused by indoor activities such as the closing of doors, the unlocking and opening network drop-enclosures, and facility HVAC systems need to be considered. This tech tip outlines the process of configuring APUs to protect data systems in their environment.

Basic Configuration

The methodologies employed by would-be intruders who wish to gain physical access to the network (fiber or copper infrastructure) are in two categories:

1.) Lower frequency intrusions using hand-tools, or
2.) Higher frequency intrusions using power tools

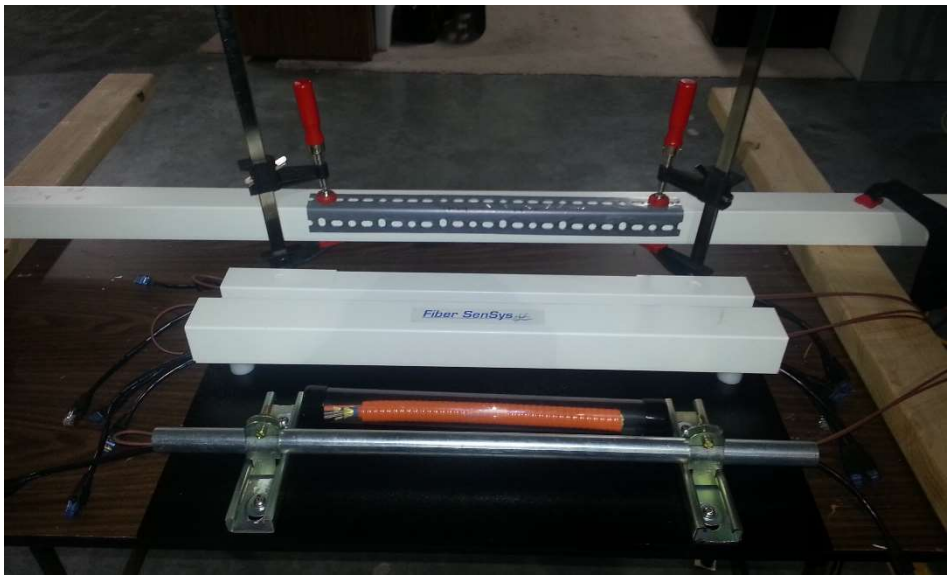
To configure the system, you need to simulate the possible intrusion methods as closely as possible without damaging the cable or conduit. FSI recommends prior to simulating intrusions, apply a shielding layer over the data or sensing cable or conduit. The shielding layer should be composed of a material that closely resembles the inner layer. Once shielded, simulate an intrusion by attempting to break into the shielded layer.

Each channel of the APU utilizes two virtual processors that are specifically tuned for low-frequency and high-frequency intrusions. By default, virtual processor one is tuned for low-frequency intrusion attempts and processor two is tuned for high-frequency intrusion attempts. As an example, if the protected network is contained within a

hardened carrier PDS, an effective simulation would be removing the top cap of the hardened raceway, which would fall into the low-frequency intrusion category.

Configuring for the Low-Frequency Intrusion

For the low-frequency intrusion configuration, simulate the type of low-frequency intrusions that you would anticipate an intruder to execute and make changes to processor one such that each simulation causes processor one to alarm once. If multiple alarms occur from a single intrusion simulation, the system may be set too sensitively, and nuisance alarms could potentially become a problem. Standard low-frequency intrusion simulations would encompass striking the protected conduit with a mallet (a metal hammer can damage the conduit). When testing metal conduit, clamp a short section of sheet metal to the outside of the hardened raceway and conduct intrusion testing on the metal section. Simulate hacksaw intrusion attempts on the clamped metal layer and make changes to processor one. This process requires two people; one for simulating the intrusion and a second for making changes to the APU.

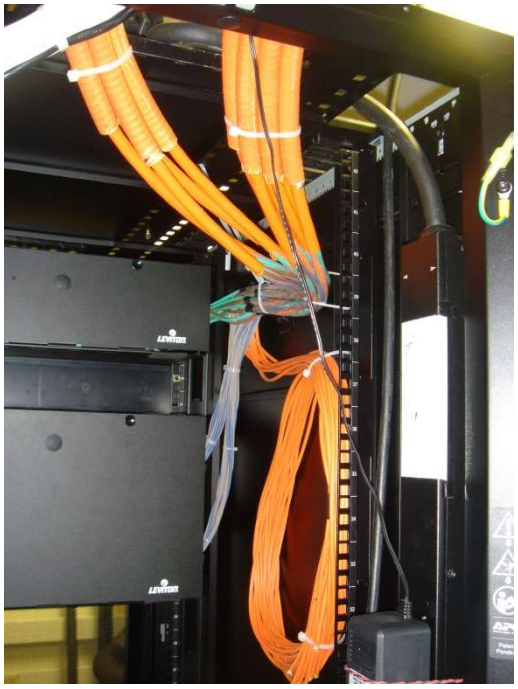


Sample testing setup using hardened raceway. The metal grating protects the raceway from being damaged during the testing process.

Configuring for High-Frequency Intrusions

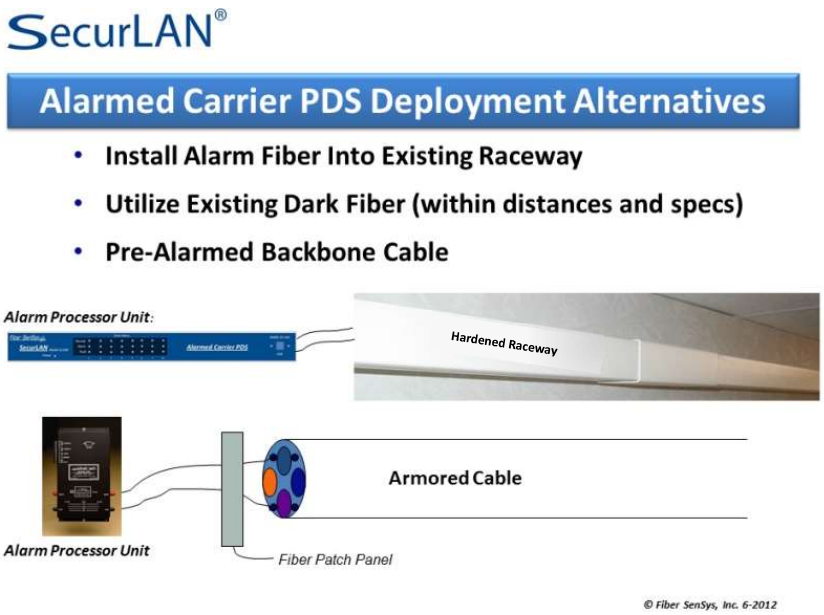
High-frequency intrusions are more challenging as high-frequency noise typically does not require the same magnitude of force as lower frequency intrusions. Simulate high-frequency intrusion attempts by again attaching a comparable material layer to the data bundle and cutting into the test layer. Look for spikes along the frequency axis using the *RealTime* mode function of the configuration software and make changes to the low-frequency and high-

frequency settings accordingly. High-frequency vibrations tend to exist anywhere between 100 Hz and 600 Hz and should be easily discoverable by viewing the spectral data while applying the power tool to the test layer. Using a variety of equipment types for testing, such as drills and rotary cutting tools, is recommended to ensure that differing revolutions per minute (RPMs) cause alarms. The Fiber SenSys Support Department is available at (503) 726-4455 and support@fibersensys.com for additional suggestions. If nuisance alarms become an issue, consider saving spectral data recordings of the nuisance alarms along with recordings of intrusion simulations and emailing them to us; we can analyze the recordings and return our parameter recommendations.



Configuring for Environmental Noise

Nuisance alarm sources for **SecurLAN** applications general come from doors slamming, vehicles passing, and indoor machinery such as air conditioners and elevators. After tuning for low-frequency and high-frequency intrusions, it is recommended the system be monitored during a time when potential nuisance alarm conditions occur and ensure that nuisance events and alarms do not occur. Typically, the system should be tested for nuisance alarm rate and false alarm rate (NAR/FAR) over a period of at least one week. All probability of detection (PD) and NAR/FAR tests should be completed before a system can "go live."



Conclusion

After installing our fiber optic sensing cable or activating an already existing dark fiber for use with our APUs, the next step is configuring the APUs for low-frequency and high-frequency intrusions. The configuration of the system involves simulating intrusions and ensuring that alarms are activated. Additionally, ensuring that nuisance alarms and false alarms do not occur is also a large part of the tuning process. Low-frequency alarms are generally simulated using a hammer and/or a hacksaw; high-frequency alarms are simulated using power tools. In both cases, a protective layer should be added to the secured network bundle before testing so that the optical fiber or protective conduit of the network is not damaged.

Fiber SenSys has supported network security for over 20 years. With alarm processors specifically designed for network security applications, we've earned high-security certifications from the military. Furthermore, we've established a positive reputation in the public sector and private sector as well. We recognize the importance of securing networks in today's digitalized world, and we intend to continue to strengthen our reputation through our quality products, service, and support.

For more information, contact us at
info@fibersensys.com
Tel: +1(503)692-4430
Toll free (US) +1(888)736-7971

Fiber SenSys®

High Performance – High Reliability – High Security