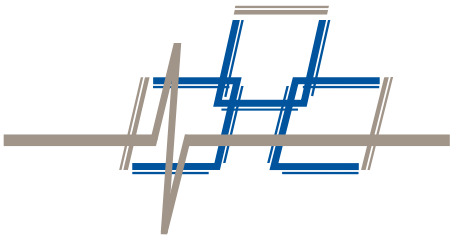
Application Note



Securing a Protected Distribution System (PDS)

SUMMARY

The SecurLAN® product line is designed to protect data cable infrastructure against physical intrusion (cable tapping or sabotage) by detecting vibrations from such attempts and alerting security authorities. A Protected Distribution System (PDS) is a network distribution design used by the US military and government to protect unencrypted data transmissions. This application note covers the PDS layout and discusses ways SecurLAN® can be deployed to help for the PDS.

INTRODUCTION

In instances where it is not reasonable, desirable or feasible to encrypt data transmissions, US government installations are required to protect data against theft or sabotage using electronic, magnetic or physical means or a combination thereof. A network with such a physical architecture is deemed a “Protected (or Protective) Distribution System (PDS)”. Guidelines for creating a PDS are outlined in National Security Telecommunications and Information Systems Security (NSTISSI) publication number 7003.

In its simplest form, a PDS consists of a secure host/client setup where all electronic access to the network is contained in a controlled area. All cables routing through uncontrolled areas or areas with limited controls are either monitored for intrusion on a continual bases or are protected against intrusion through physical means (such as hardened steel conduit).

Fiber SenSys’ SecurLAN® data security system helps form the PDS by “alarming” the data cable - or bundling a vibration sensor with it - in its vulnerable stretches between controlled areas. Any attempt to access the network cables physically causes an alarm. Used in this way, SecurLAN® provides an alternative to continuously monitoring the network cable conduit, ensuring the PDS construction meets the NSTISSI 7003 requirements.

Types of Protected Distribution Systems

There are two type of PDS:

- A "hardened" PDS formed either using a hardened carrier or conduit, or formed from any material and alarmed or viewed continuously by security personnel
- A "simplified" PDS made from any material, inspected regularly

A PDS will often by comprised of a mix of both hardened and simplified carriers.

"Hardened" Carrier PDS

"Hardened" carrier - definition

"Hardened" carriers are used to protect a PDS in areas where network cables must transition through an uncontrolled area or area of limited access control.

A *"hardened"* carrier is a network cable conduit built with "Electrical metallic tubing (EMT), ferrous conduit or pipe, or rigid-sheet steel ducting." Pull boxes used in the carrier must also be sealed, hardened and locked.

Alternatives to hardened material

As an alternative, a "hardened" conduit may be formed using a conduit made from any material, provided the conduit is viewed and monitored at all times by security personnel. A carrier may also be considered "hardened" if it is alarmed and set up to detect intrusion attempts.

"Simplified" Carrier PDS

"Simplified" carrier - definition

"Simplified" carriers are used in a PDS in areas where personnel access is restricted and security controls are in place in the area.

A "*simplified"* carrier may have network cable conduit formed from any material, and need only to undergo periodic visual inspection.

A "simplified" carrier is appropriate for use in any controlled environment. A simplified carrier is not appropriate, however, for protecting network cable runs extending outside a controlled environment. For such stretches, a hardened carrier system must be used.

A "simplified" carrier PDS should not be used for installations outside the continental US exceeding a medium threat level. For installations in a medium threat level environment, a hardened carrier is required for all levels of data classification except for some special category secret data.

Constructing a Protected Distribution System

A PDS must be constructed in accordance with the guidelines outlined in NSTISSI publication number 7003.

As discussed earlier in this application note, a PDS consists of a client/server network where all access points are contained in controlled areas and all data cable infrastructure transiting through uncontrolled areas is protected from intrusion by electronic, magnetic or physical means such as hardened or alarmed carriers.

Definitions

PDS definition

The basic elements of a PDS are defined:

Controlled Access Area (CAA). An area or facility under direct control in which all unauthorized persons are denied access and access by all authorized persons is strictly monitored or controlled through physical or electronic means.

Limited Controlled Access (LCA). An area or facility surrounding a PDS where unauthorized access to the network infrastructure is unlikely or appropriate means to identify and remove a potential security compromise exists.

Line Route. The path of the PDS network cable run.

Lockbox. A metallic box with a lock attached to the end of the PDS run which allows access to the network for authorized personnel and prevents access for unauthorized persons. A lockbox is always located in a CAA. Lockboxes are often used to house Secret Internet Protocol Router Network (SIPRNET) connections.

Pullbox. A metallic box used to pull network cable through conduit from one point to another. Pullboxes must be made of hardened material (such as steel) and locked for use with a “hardened” carrier PDS.

Secret Internet Protocol Router Network (SIPRNET). A proprietary US military/DOD network for transmission of classified data.

Special Category Data (SPECDAT). Definition of this data is classified.

Uncontrolled Access Area (UAA). The internal or external area of a facility through which no access controls can be exercised or are imposed.

Figure 1 shows the typical layout and associated elements of a basic PDS.

Application Note

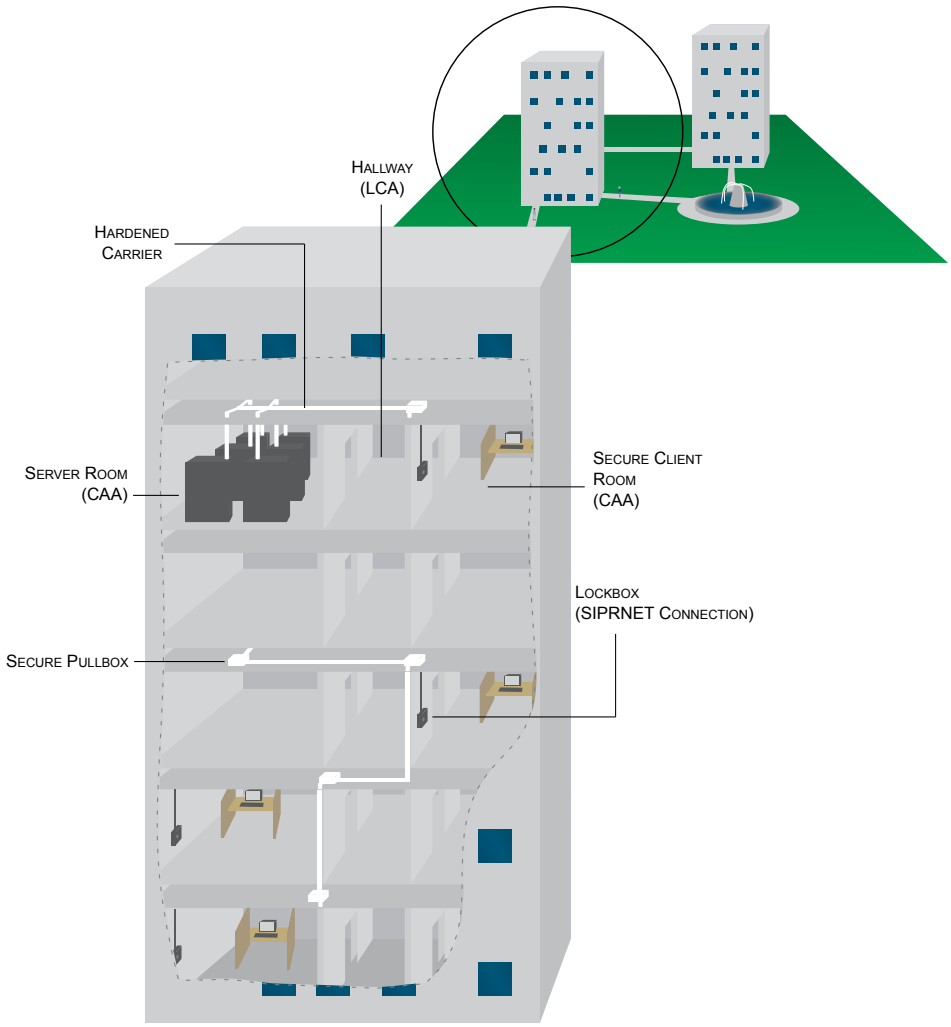


Figure 1 - Basic PDS Components

OVERVIEW

A properly constructed PDS protects cable runs in the confines of a single building or cable runs extending from one building to the next.

SINGLE BUILDING PDS CONSTRUCTION

Generally, a PDS must use a “hardened” carrier for all cable runs extending through LCA or UAA regions. Only within a CAA is use of a simplified carrier permitted.

"Hardened" carrier requirements

Unless a carrier can be visually monitored at all times, it must be constructed of hardened material such as steel. Even if the carrier is only partially obscured (transitioning through walls, for example) hardened conduit must be used to prevent cable tampering.

NOTE:
The use of flexible material in a hardened carrier system is not permitted.

The hardened carrier should extend from one CAA to the next in any area where the network cable must transit through an LCA or UAA. This is true even if the carrier is routed above ceiling tiles, below floorboards, or in walls (figure 2). All pullboxes used in the PDS must also be constructed of welded, hardened material (16 gauge or better) and must be locked to prevent unauthorized access. All lockboxes must be located in a CAA.

If a "hardened" carrier is hidden in any way, however, as it transitions from one CAA to another, it *must* be alarmed in the hidden area with an approved sensor system (such as SecurLAN).

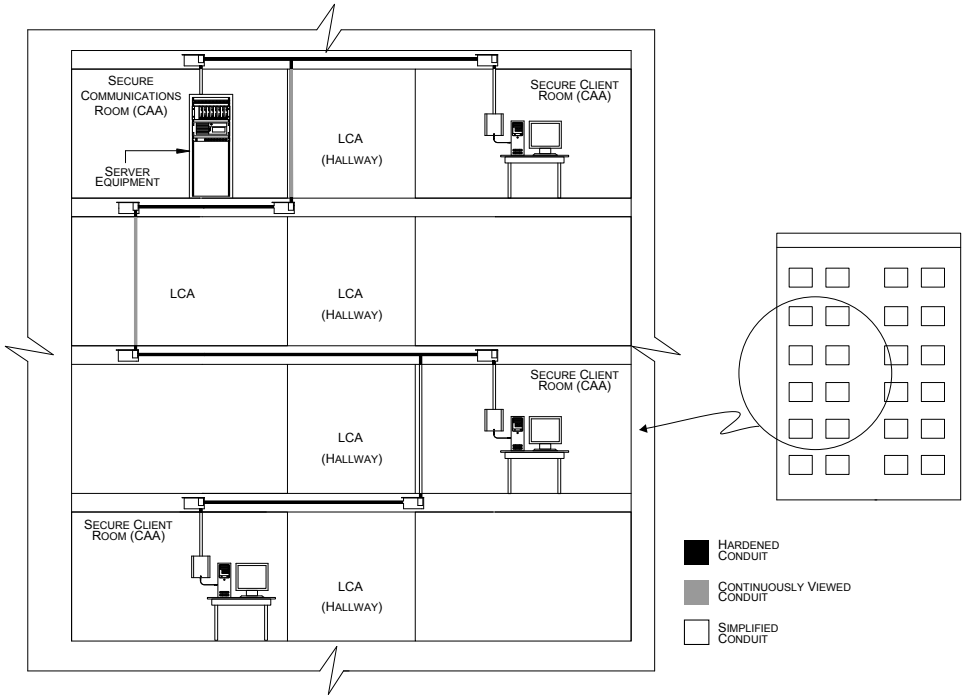


Figure 2- Single building PDS layout

Using an "alarmed" carrier as a "hardened" carrier

As an alternative to constructing a carrier of hardened material, a PDS may be constructed using an alarmed carrier entirely. The performance and effectiveness of the alarmed carrier must be verified on a routine basis and response of security personnel to any alarm within a 15 minute time frame must be assured. In addition, components of the alarmed PDS such as pullboxes must also be alarmed.

Application Note

Using a continuously monitored carrier

A carrier is also considered “hardened” if it is visually monitored at all times by the appropriate security personnel.

Multiple Building PDS Construction

As with a single building PDS, a PDS covering multiple buildings must use a “hardened” carrier for all cable runs extending through LCA or UAA regions. Only within a CAA is use of a simplified carrier permitted.

Using a buried carrier between buildings

A PDS extending across one or more buildings must be constructed to meet the same requirements as those specified for a single building. Network cable runs must be protected by a “hardened” carrier from one building to the next. However, it is permissible to bury the cable run below ground in place of hardened conduit provided that the buried carrier is enclosed in at least 20 cm (approximately 8 inches) of concrete. In addition, the carrier must be buried at least 1 meter (3.3 feet) below the surface on property under ownership or control of the network controlling entity.

Manholes providing access to the buried carrier must be locked to prevent unauthorized access.

“Suspended” carriers

If network data cables are run between buildings in conduit above ground (a setup known as a “suspended” carrier), the carrier must be suspended at least 5 meters (16.4 feet) above ground on property owned or controlled by the network controlling entity. The “suspended” carrier must be hardened and allow for clear, unimpeded inspection at all times.

NOTE:
Areas in which a “suspended” carrier is used must be well lit.

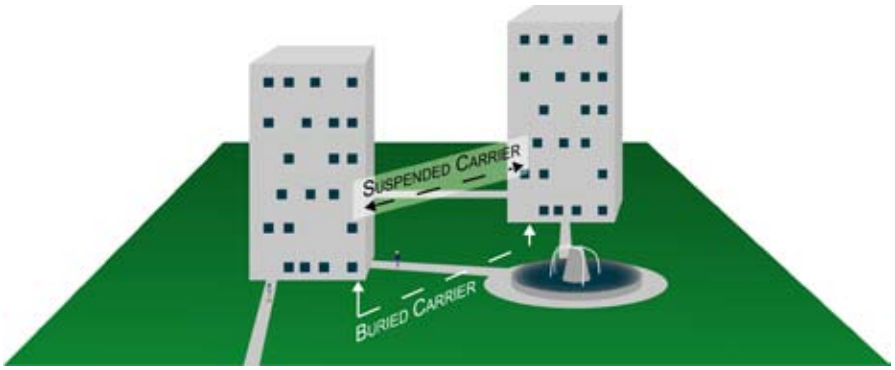


Figure 3 - Building - to - building PDS construction options

Alarming a PDS with SecurLAN®

SecurLAN® definition

SecurLAN® is a vibration sensing system that uses a fiber optic cable as the sensor. When deployed in parallel with a network cable run or embedded in a carrier, the fiber optic sensor cable alarms the PDS, essentially qualifying a non-hardened carrier into a hardened carrier (see "*Hardened" Carrier PDS* earlier in this application note for a description of the hardened carrier qualifications).

Uses

SecurLAN® also enables a "hardened" carrier system to meet the alarm requirements at places where the carrier is obscured or hidden from view (above ceiling tiles, beneath floor boards, etc.).

Introduction

Basic SecurLAN® configuration

In SecurLAN®'s basic configuration, the vibration sensing fiber optic cable is deployed in parallel with the network cable run it is intended to protect (figure 4). The sensor cable is bundled physically with the network cables.

NOTE:
Bundling the sensor cable with the network cables is the preferred method. For protection of the sensor cable, it is recommended that the cable be pulled inside the conduit in all installations.

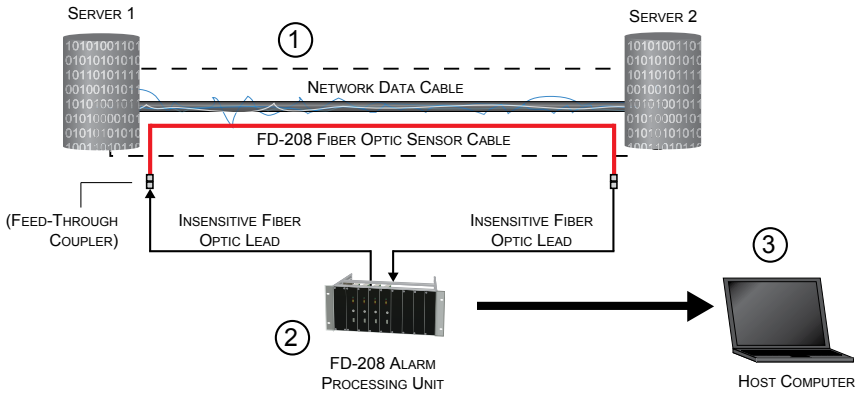


Figure 4 - SecurLAN® Basic Block Diagram

Insensitive lead-in cables

Once the sensor cable is deployed, it is connected at both ends to insensitive lead-in cables. These lead-in cables are also made of fiber optics, but are constructed of single-mode fiber (as opposed to the multimode optical fiber of the sensor cable) and are insensitive to the effects of vibration.

The lead-in cables connect the sensor cable to input and output ports of SecurLAN®'s FD-208 Alarm Processing Unit, or APU, thus forming a closed optical loop.

NOTE:
A closed optical loop must be formed with the sensor cable/insensitive leads for SecurLAN® to operate.

Alarm Processing Unit - APU (purpose)

The APU transmits laser light through the optical loop and analyzes the pattern of returning light. Mechanical vibration from any attempt to access network cables in the alarmed carrier disturbs or temporarily alters the normally coherent pattern of light conducting through the sensor cable. This disruption is detected by the APU, resulting in an alarm state.

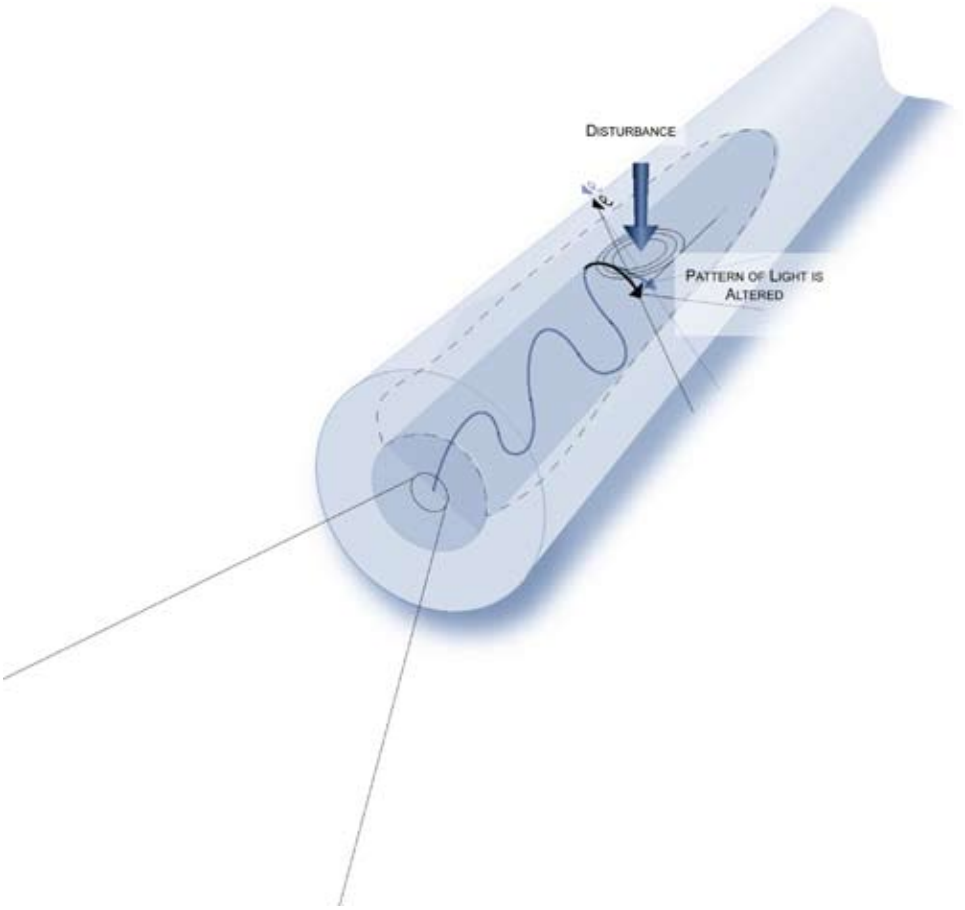


Figure 5 - Effects of vibration on the sensor cable

Alarm signals from the FD-208 APU are transmitted to security personnel via a network of components. Depending on how the user has programmed the system, SecurLAN® may take preventative action to protect the compromised carrier such as divert the data stream to another conduit or cut the data off completely (figure 6).

NOTE:
The FD-208 APU is not a position-resolving sensor. In order to differentiate where an intrusion attempt is occurring, the PDS network must be sectioned into multiple "zones", with one APU module protecting each zone.

Sensor limitations

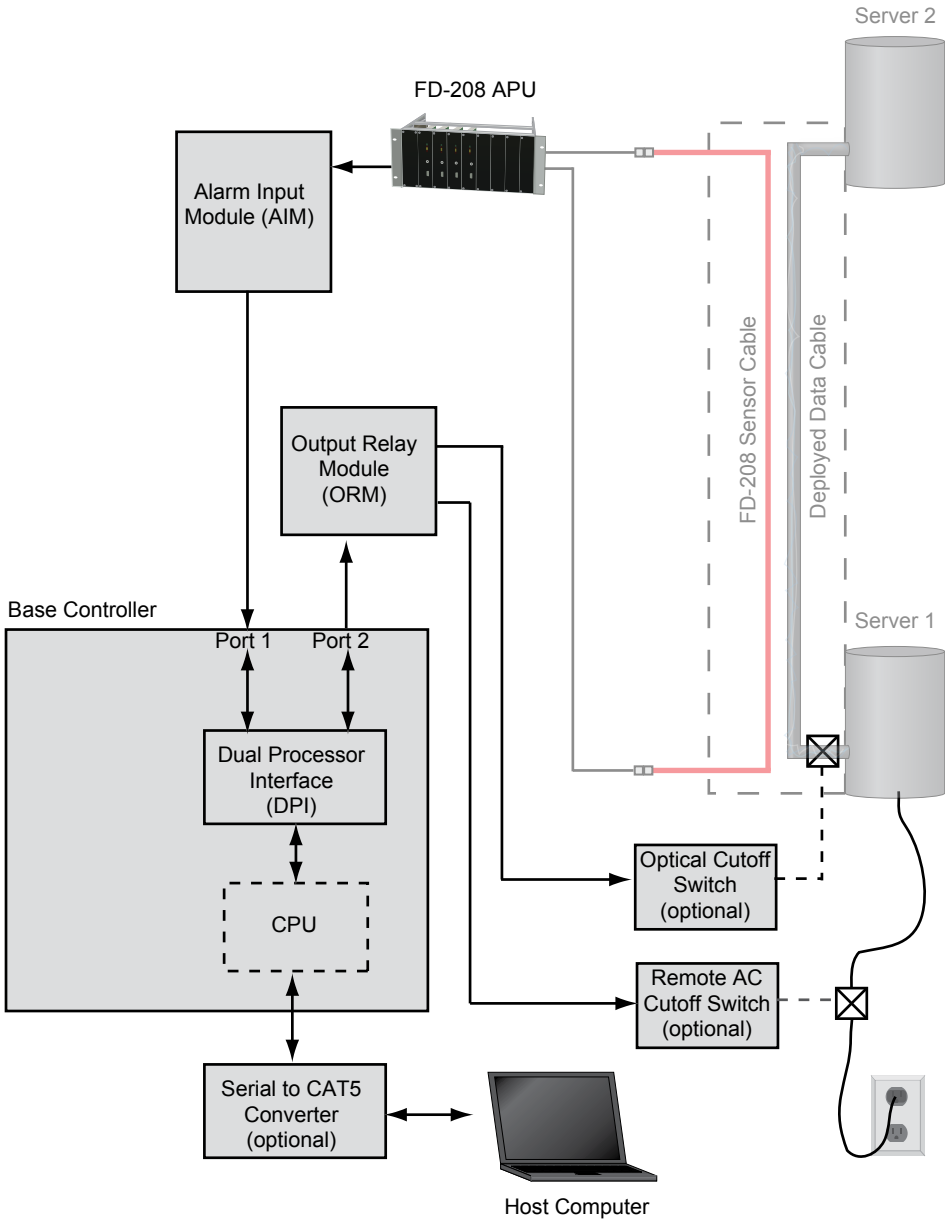


Figure 6 - SecurLAN® component block diagram

Basic SecurLAN® components

Some of the basic components include:

Base Unit Controller. This component is SecurLAN®'s primary signal router. The base unit controller receives alarm signal input from the APU and routes it to the host computer using a direct serial connection, a modem or optional serial-to-CAT5 converter.

Alarm Input Module (AIM). This optional component receives input from multiple FD-208 APU modules and passes them to the base unit controller. Use of the AIM expands the number of possible APU/zones that can be used with each base unit controller.

Output Relay Module (ORM). The ORM receives action signals from the base unit controller and routes them to the appropriate output device. Use of this optional components expands the number of possible output devices that can be connected to each base unit controller.

Optical Cutoff Switch. The optical cutoff switch is an optional component that reroutes a data stream from one fiber optic cable to another or cuts off all optical data flow, depending on how the user programs it.

Remote AC Cutoff Switch. Also an optional component, the remote AC cutoff switch cuts off AC power to any network component if an alarm condition occurs.

Serial-to-CAT5 Converter. The serial to CAT5 converter allows a base unit controller to communicate with the host PC using Ethernet protocol (two other communication options exist: serial communication and modem connection).

System Control Software ("Head End"). The SMS 2000 control software installs on any PC with a Windows 98 operating system or better. Through the control software, users configure SecurLAN®, monitor the alarmed zones and take protective action in the event of intrusion. The head end control software also provides a utility for tracking and printing alarms or alarm events in accordance with NSTISSI 7003 requirements.

Design Basics

In order to protect a PDS in compliance with NSTISSI 7003 standards, SecurLAN® must be set up in such a way that users can accurately determine a point of intrusion and respond within 15 minutes of the intrusion notification. The most effective way to ensure this requirement is met is to separate the PDS into zones small enough to allow quick reaction times for security personnel.

Alarmed carrier minimum requirements

To alarm a carrier to meet the "hardened" carrier requirements satisfactorily, as a minimum, each portion of the carrier transiting through an LCA or UAA *must* be alarmed with sensor cable through the entire length of the area unless it is continuously monitored by security personnel (figure 7).

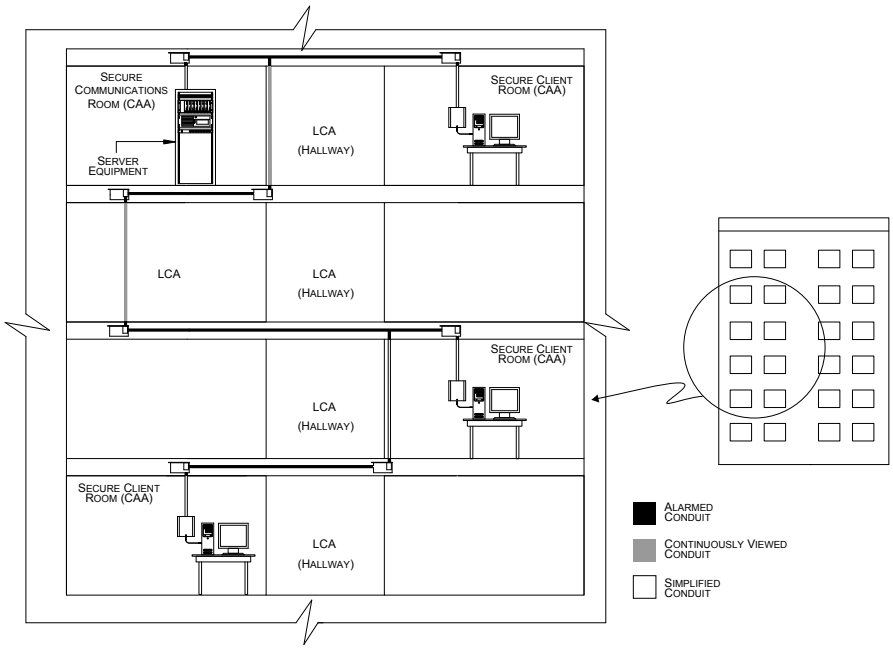


Figure 7 - Example alarmed carrier layout

Note that with the example shown in figure 7, it is still permissible to use a mix of continuously monitored, “simplified” and alarmed carriers throughout the PDS provided each carrier type is appropriate for its environment.

Even if a carrier is constructed from hard material, a hardened carrier *must* be alarmed at any and all points where the carrier is obscured from vision. As shown in figure 8, this includes portions of the PDS where the carrier runs above ceiling tiles or through walls.

Application Note

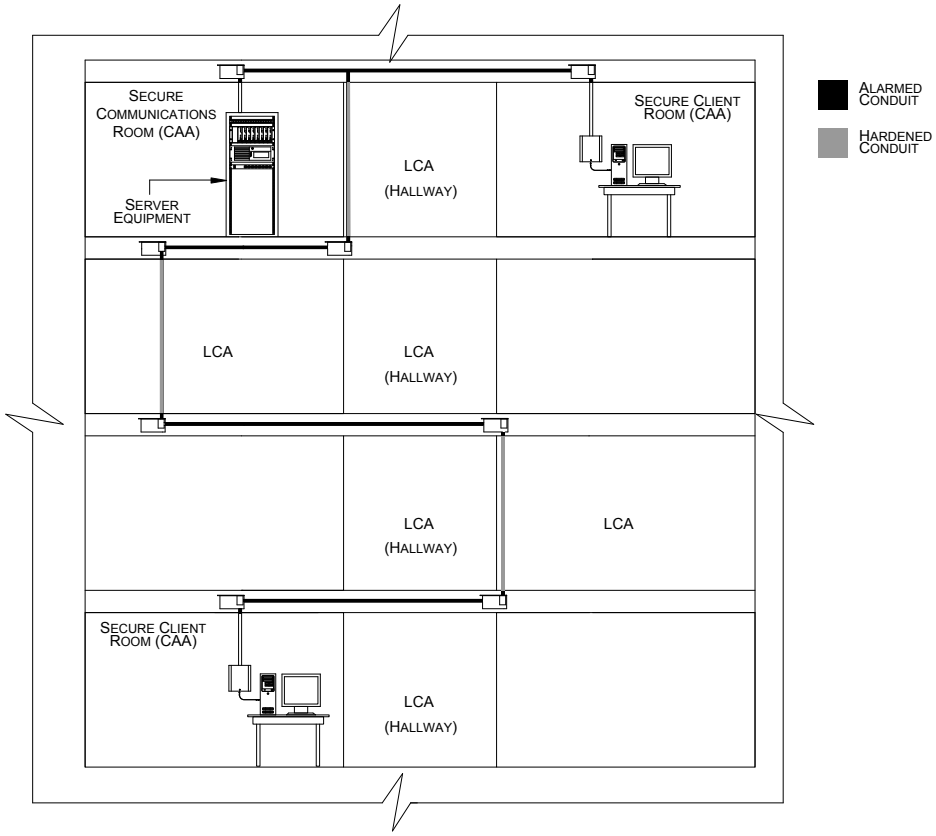


Figure 8 - Alarmed segments of a "hardened" carrier

LOCATING THE HEAD END EQUIPMENT

The SecurLAN® "head end" equipment - the control software, host computer, FD-208 APU (s) and base unit controller (s) - must be placed physically in a CAA to prevent unauthorized access to critical system components. In order to meet alarmed PDS requirements, the control software must be located in a designated security CAA, with personnel on hand to monitor the system on a continual basis.

NOTE:
For space considerations, locating the FD-208 APU and the base unit controller in the same CAA is strongly recommended.

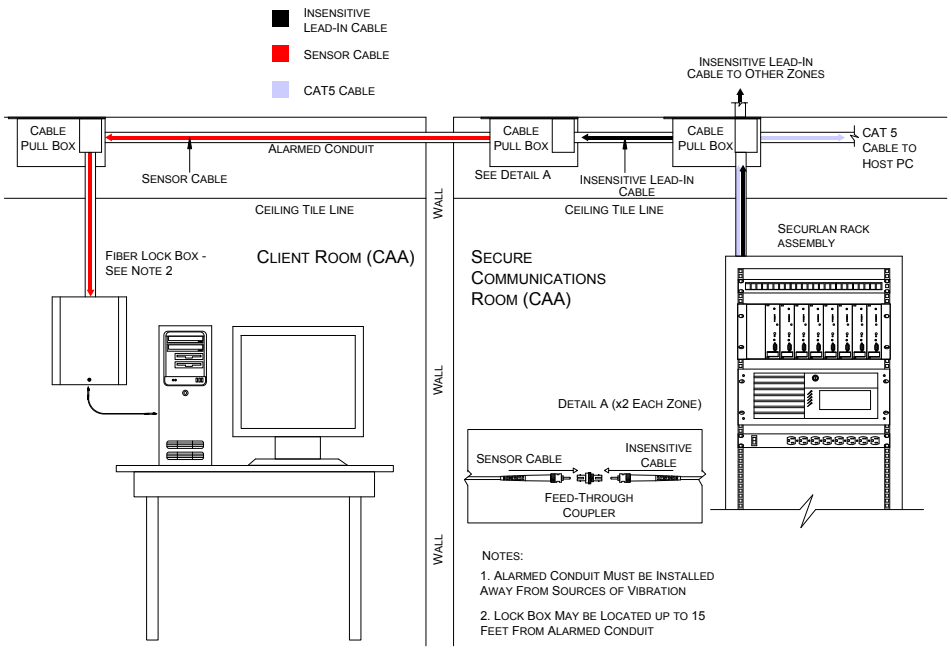


Figure 9 - SecurLAN® cable deployment scheme

SecurLAN® rack-mounted hardware

Both the FD-208 and the base unit controller come with “rack-mount” hardware versions allowing the components to be mounted in the same 19-inch equipment rack assembly. This deployment configuration is advantageous because it facilitates pulling the insensitive leads of the FD-208 and any CAT5 cables connecting the base unit controller and host computer through a common conduit section (figure 9).

The rack-mounted version of the FD-208 is known as the “FD-208R”. It is made to insert into a unique rack known as the RK-208. Up to eight (8) FD-208R units can be mounted into one 19-inch RK-208.

RK-208/FD-208R power requirements

Power to each APU is provided by the RK-208 (which itself requires 120/240 VAC input).

Insensitive Leads

Insensitive cable maximum length

Each APU supports a maximum of 5 km (3 miles) of sensor cable. Each insensitive lead, however, can measure up to 20 km (12.4 miles) long. In this way, the insensitive leads allow the centrally-located APU to connect to zones located physically in remote regions of the PDS.

Every FD-208 requires two (2) insensitive leads: one (1) cable on the APU input and one (1) cable on the APU output (refer to figure 4). Therefore, 1 APU module and two (2) insensitive leads are required for every zone into which the PDS is divided. This scheme can require large numbers of single-mode insensitive leads. Systems using the FD-208R/RK-208 feature generally offer a better way of managing these cables than a system using individual APUs (figure 10).

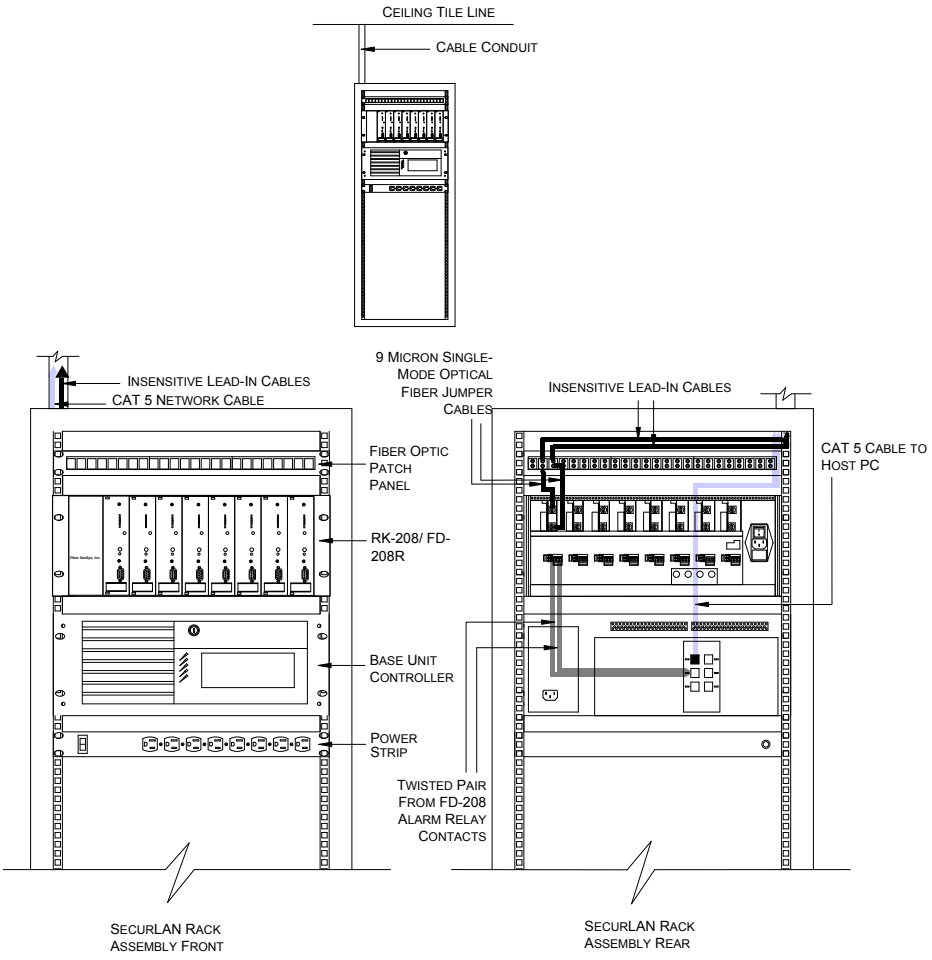


Figure 10 - Cable connection details of the rack-mounted equipment

Using a fiber optic patch panel organizes the insensitive leads, allows them to thread easily through the carrier conduit and helps to prevent the individual APUs from being connected to the wrong zones. Since the insensitive leads are made of standard 9um/125um single-mode optical fiber, standard single-mode fiber optic patch cords or jumpers can be used to complete the connection from the patch panel to the ST-connectors on the back of the APUs.

Transition zones

Insensitive leads also form *transition zones*, or areas between an APU and its remote corresponding zone. Transition zones in certain areas of a PDS may or may not require alarming. Examples of areas not requiring alarming include CAAs, LCAs where hardened conduit is used as the carrier and is clearly visible, and LCAs or UAAs where the carrier is continuously monitored by security personnel.

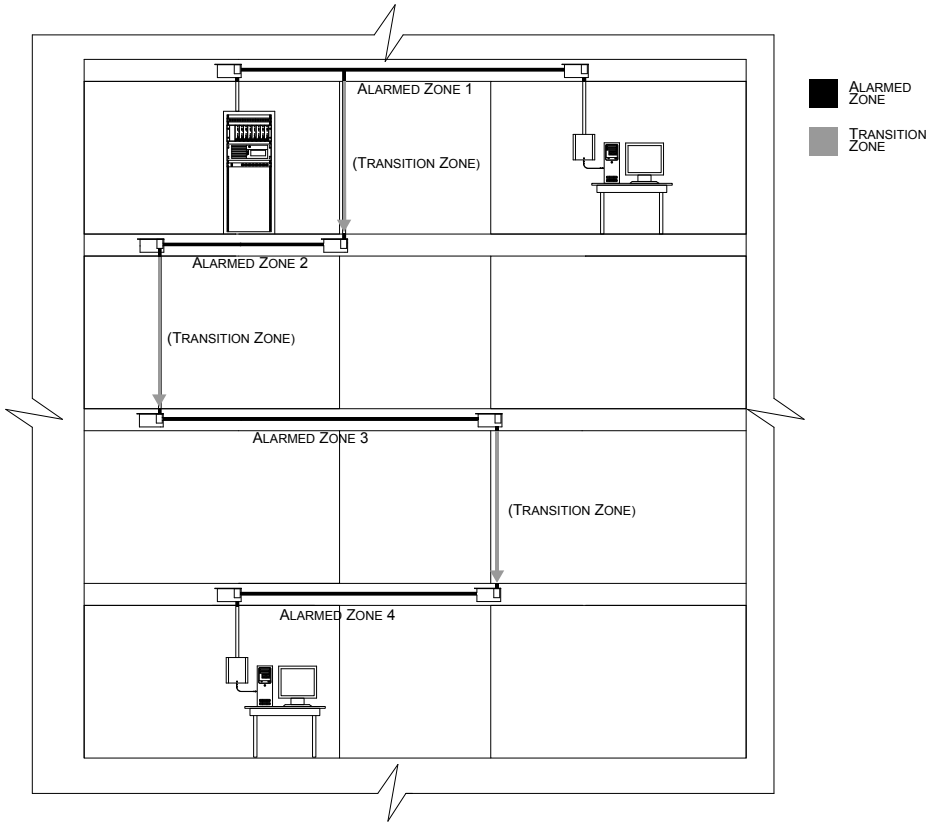


Figure 11 - Transition zones in an alarmed PDS

Figure 12 provides a more detailed cable layout diagram of these transition zones.

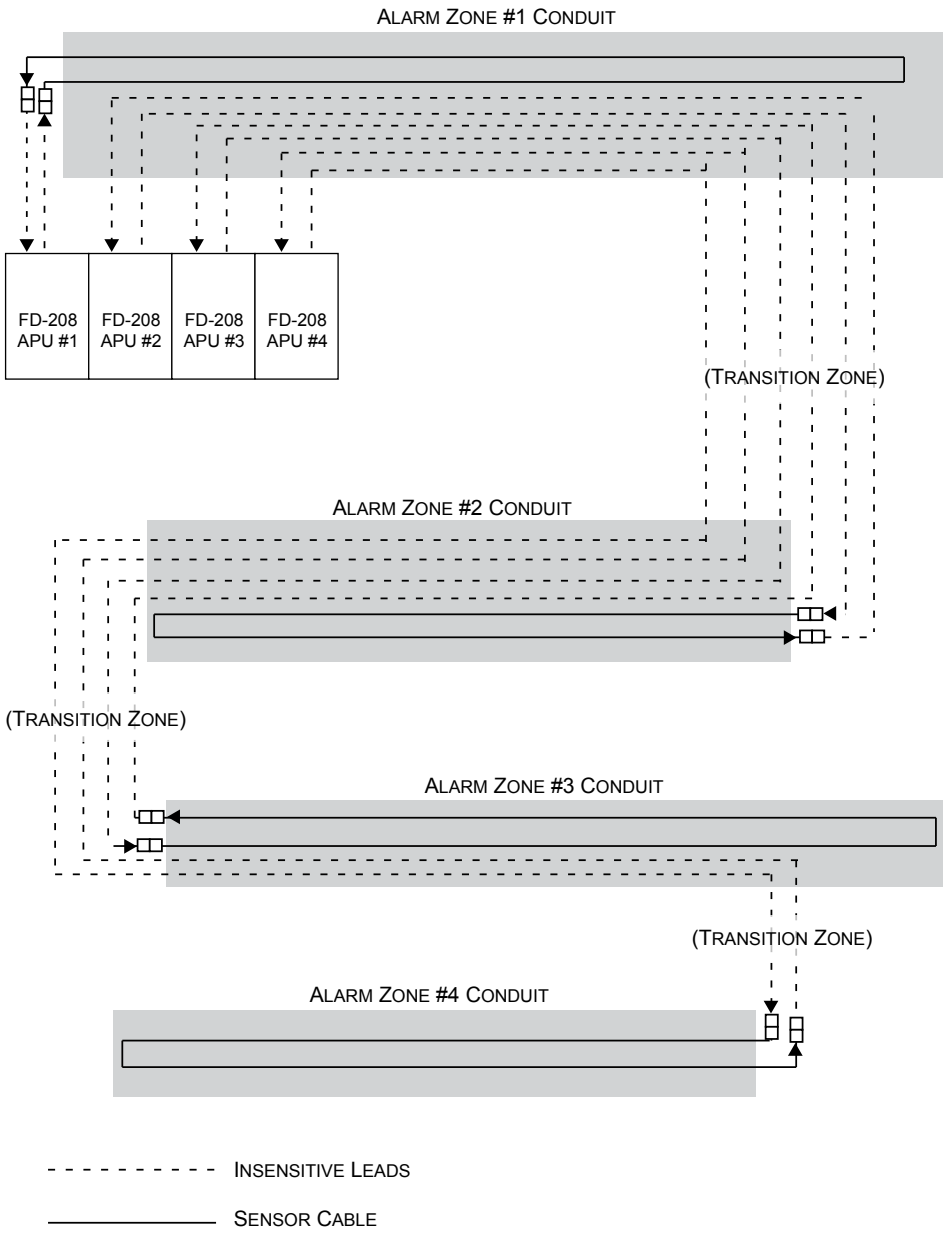


Figure 12 - Cable layout diagram

Note that the insensitive leads in this example are routed through both the transition zones and the conduit of other alarm zones.

Coupling insensitive leads to sensor cable

Optical couplings (called *feed-through couplers*) connecting the insensitive leads to the sensor cable are typically housed in pullboxes.

Transition zones connect APUs to remote zones within the same building or they may connect APUs to corresponding zones in different buildings (figure 13).

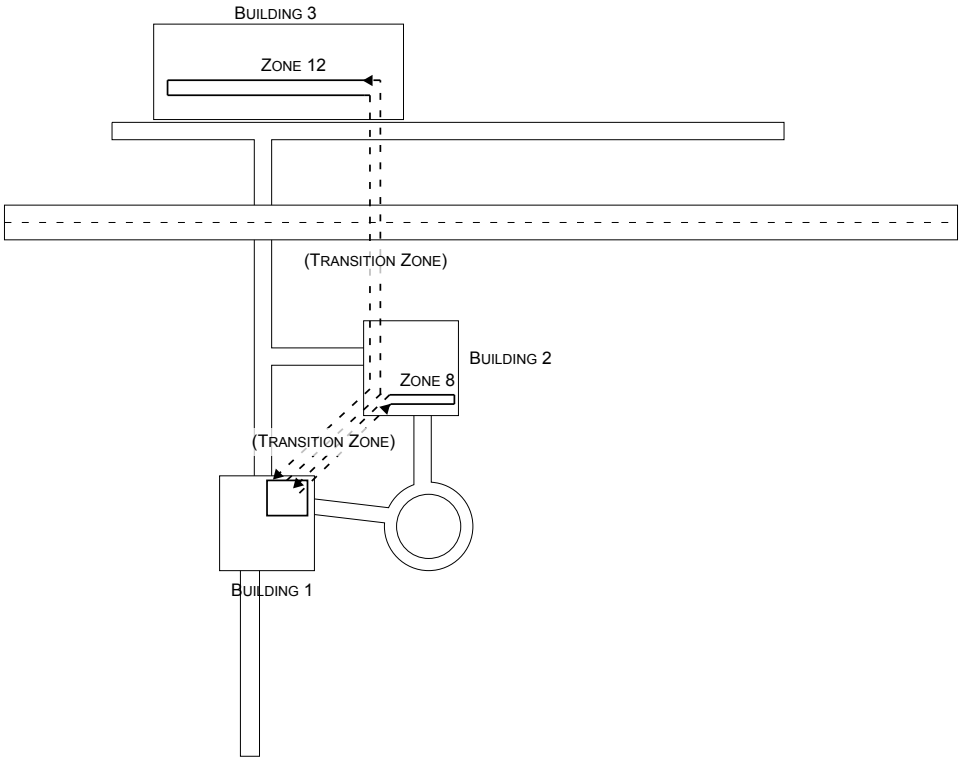


Figure 13 - Transition zones in a multi-building layout

Because a PDS network can be divided into many different zones, the use of bundled or multi strand single-mode fiber optic cable may be a better option then pulling individual single-mode strands for each zone. For more information, see *Layout Options* later in this application note.

SENSOR CABLE DEPLOYMENT

Sensor cable maximum length

The fiber optic sensor cable is a vibration-detecting sensor. Its maximum range is 5 km (3 miles). In order to be most effective, the sensor cable must be deployed in parallel with the network cables it is meant to protect.

Protecting network conduit with the sensor cable

The primary means of alarming a carrier with the SecurLAN® sensor cable is to bundle or embed the sensor cable with the network cable inside the carrier conduit. This is accomplished by pulling the sensor cable into existing conduit or pulling it in parallel with network cables when installing a new network.

Because the sensor cable is a vibration-sensing device, attaching the sensor cable to the outside of the carrier is not recommended. This is because securing the sensor cable to the conduit creates “dead spots” at points wherever the cable is tied.

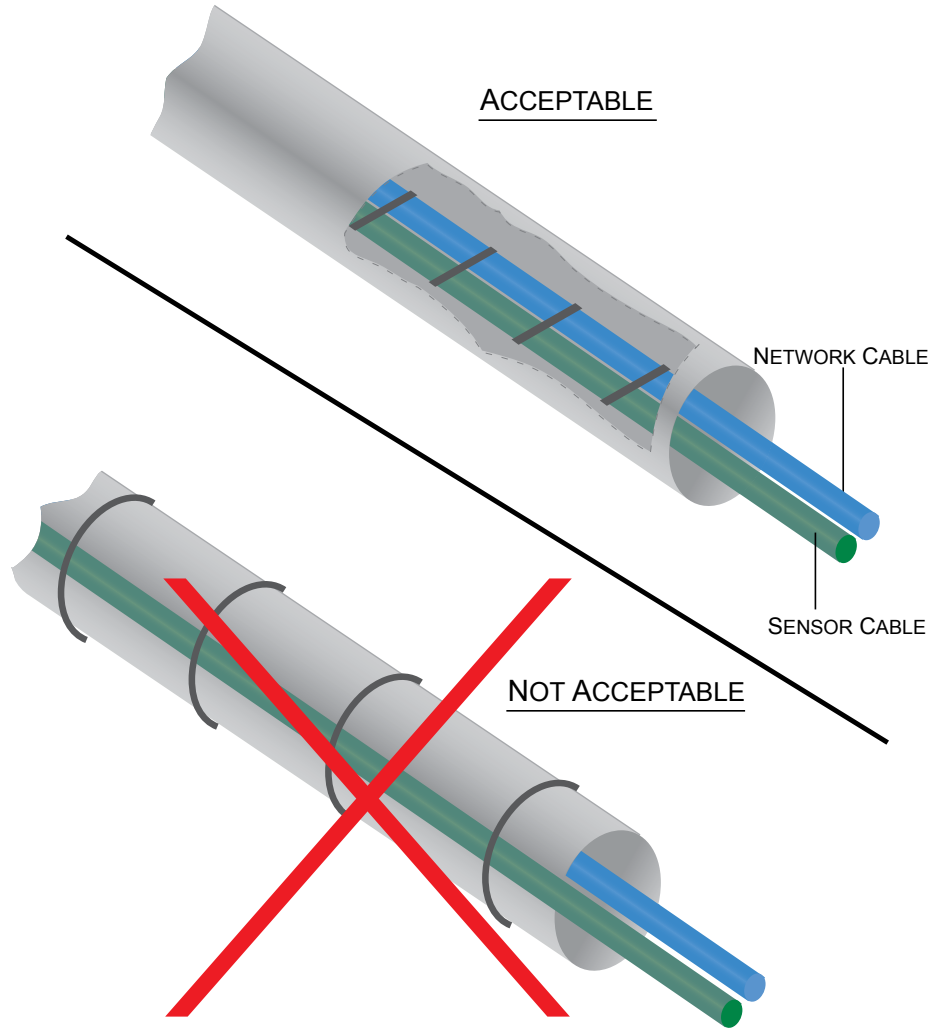


Figure 14 - Alarming a carrier with the sensor cable

Sensor cable minimum bend radius

SecurLAN®'s sensor cable is surrounded by a thick, UV-resistant jacket making it difficult to pull through tight bends. The cable should not be bent in a radius tighter that 5 cm (2 inches) or damage to the fiber optic cable may result.

Wherever the sensor cable is installed, it should be protected against non-threatening sources of vibration Slamming doors, vibrating windows and rattling air conditioning ducts are three main sources of non-threatening vibrations common to building applications.

Fiber SenSys offers multiple plenum-rated cable assemblies with and without the sensor cable already bundled within. Fiber SenSys also offers cable assemblies bundled in an armored jacket, allowing segments of the PDS to be established in some instances without hardened conduit. For more information on these bundled cable options, see *Layout Options* later in this application note.

Pullboxes and Lockboxes

Pullboxes and lockboxes are both important elements in a PDS. If a PDS relies upon an alarmed carrier as its "hardened" carrier, all lockboxes and pullboxes must be alarmed.

Alarming a pullbox

A pullbox is best alarmed by attaching a loop of sensor cable to the access lid. This is accomplished by pulling an extra length of sensor cable through the conduit (about 0.3 meters or 1 foot), coiling it and attaching the coil to the lid with Velcro® or tape. Once the lid is secured in place, any movement of the lid disturbs the loop of sensor cable, resulting in an alarm.

For "hardened" conduit, any pullboxes which are alarmed should also be secured with a padlock.

Pullboxes also form excellent "break-out" boxes or enclosures for housing couplings that connect single-mode insensitive leads to the sensor cable of the various zones.

Alarming a lockbox

Lockboxes can be alarmed in a similar manner. As an alternative, however, it is possible to rely on the nearby alarmed conduit detecting vibrations from anyone accessing the lockbox. For the connecting alarmed conduit to adequately detect disturbances, however, the lockbox can be located no further than 5 meters (15 feet) away from where the alarmed conduit terminates (see figure 9).

Layout Options

Fiber SenSys offers several cable assembly options to reduce the volume of cable that must be pulled to alarm a PDS.

There are three cable assemblies customized for SecurLAN® applications:

SecurLAN® bundled cable options

SecurLAN® Retrofit Cable. This cable assembly consists of one (1) single-mode fiber optic cable and one (1) sensor cable housed in a common, plenum-rated jacket. The advantage of this cable assembly is it requires users to pull one cable as opposed to two. Using a single-mode jumper at the far end, installers can complete the optical loop without having to pull a separate strand of single-mode optical fiber.

IC-3D Insensitive Duplex Cable. Duplex cable bundles two (2) single-mode optical fibers in a common jacket. With duplex cable, installers need to pull only one cable to deploy both insensitive leads that form the closed optical loop.

SecurLAN® Backbone Cable. The most versatile bundled cable assembly, the SecurLAN® backbone cable contains two (2) sensor cable strands, two (2) single-mode insensitive leads and four (4) cable subassemblies with between 12 and 96 single-mode and multimode optical fibers for data transmission. The SecurLAN backbone cable is protected by a helical, aluminum armor sheath. By using this bundled cable assembly, users establish an alarmed, armored PDS with just one cable type.

For more information on using these unique SecurLAN® cables, refer to the *SecurLAN® Cable Applications* application note.

Maintenance Requirements

Routine maintenance requirements

In order to ensure an alarmed carrier continues to meet PDS requirements, some basic routine checks must be performed.

- A record of all alarm events must be kept and maintained. SecurLAN®'s SMS 2000 control software has a built-in event and alarm log. Events and alarms received by the base unit controller are stored in a buffer and transmitted to the host PC at user-programmed intervals. It is recommended users print out a copy of the event and alarm logs at least once daily.
- Functional testing of the SecurLAN® system and satisfactory alarm verification must be performed at least daily for carriers transmitting top secret information, weekly for carriers transmitting secret and monthly for alarmed carriers transmitting confidential information.

For more information on buried installations, please contact Fiber SenSys' sales or technical support team at +1.503.692.4430 or by e-mail at info@fibersensys.com.

Fiber SenSys

2925 NW Aloclek Drive, Suite 130

Hillsboro, OR USA 97124

Phone: +1-503-692-4430

Fax: +1-503-692-4410

www.fibersensys.com