Fiber SenSys®

FD-348R

FIBER OPTIC INTRUSION DETECTION SYSTEM

USER'S REFERENCE MANUAL

Fiber SenSys Inc
2925 NW Aloclek Drive, Suite 120
Hillsboro, Oregon 97124 USA
Tel: +1.503.692.4430
Fax: +1.503.692.4410
E-mail: info@fibersensys.com
www.fibersensys.com

PM-ENG-011
Rev. G
October 24th, 2013

IMPORTANT SAFETY INFORMATION

The FD-348R has been supplied in a safe condition. It has been designed to meet or exceed the following minimum operating conditions:

- Indoor Use Only
- Altitude up to 2000m
- Temperature 0°C to 55°C
- Up to 95% humidity non-condensing
- Installation category II
- Pollution Degree 2

Refer to the appendix of this manual for exact product specifications.

Follow the information and warnings in this chapter to ensure safe operation and to retain the unit in a safe condition.

Safety Terms

Where necessary, the following terms may appear throughout the manual and are defined as follows:

CAUTION - Identifies conditions or practices that could result in damage to equipment or other property. Cautions may also indicate a loss of data or contamination of your files

WARNING - Identifies conditions or practices that could result in non-fatal personal injury

DANGER - Identifies conditions or practices that could result in loss of life or limb

Electrical Safety

The FD-348R operates on 50 to 60 Hz single-phase power with a protective ground and is intended to operate from a 120/240 VAC power source between the supply conductors or between the active supply conductor and ground.

Use only a power cord that is shipped with the FD-348R. Order a replacement cord through Fiber SenSys if the original becomes worn or unserviceable.

A protective ground connection by way of the grounding conductor in the power cord is essential for safe operation of the FD-348R. To avoid electrical shock, plug the power cord into a properly wired receptacle. If this is not done, or if the ground connection is lost, all conductive parts of the instrument (including some controls that may appear to be insulating) can render an electric shock.

Whenever it is likely that the integrity of the product has been impaired, the apparatus should be made inoperative and secured against unintended operation. The operation is likely to be impaired if, for example, the apparatus:

- Shows visible damage
- Fails to perform the intended functions
- Has been subjected to prolonged storage under unfavorable conditions
- Has been subjected to severe transport stresses

Such apparatus should not be used until qualified servicing personnel have verified its safety.

Power cord connections and the ON/OFF switch for the RK-348 are located on the rear, right-hand side of the rack (when viewed from the rear).

There are two fuses located in the main power supply entry module for the RK-348. These fuses must be replaced with the same type and rating of fuse in order to avoid possible electrical fire and/or shock. The fuses are rated as follows:

100-240V - 1.0 amp, 250V (T)

Refer to the installation section of this manual for instructions on replacing the fuses.

Covers and Panels

To avoid personal injury, do not remove any of the product's covers or panels unless specifically directed to do so by the procedures of this manual. Follow the procedures exactly. Ensure all power is removed to the unit prior to removing any protective covers. Do not operate the product unless the covers and panels are properly installed first.

Inspection

The FD-348R components should be inspected for shipping damage. If any damage is found, notify Fiber SenSys and file a claim with the carrier. The shipping container should be saved for possible inspection by the carrier.

Optical Connectors

The FD-348R Alarm Processing Unit (APU) uses ST-type connectors. Use of other types of connectors will reduce optical performance and may damage the APU connectors.

Class I Laser Product

The FD-348R is a Class I laser product as defined by IEC 60825-1 Safety of Laser Products and 21 CFR subchapter J.

A Class I laser product emits insufficient levels of laser radiation to constitute a hazard according to established limits. Despite this, it is good operating practice to avoid direct eye exposure to the output of this product or to the open end of any optical fiber cable connected to this product.

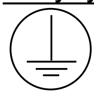
Despite this, it is good operating practice to avoid direct eye exposure to the output of this product or to the open end of any optical fiber cable connected to this product. See the figure to the right to help identify the laser output.

Fiber Handling Precautions

The optical fiber is made of glass. The ends of a broken fiber can be sharp and may become lodged in the skin. Therefore, appropriate glass-handling precautions should be taken.

At no time should the optical fiber be bent in a radius less than **5 cm** (**2 inches**) in diameter.

Safety Symbols



This symbol identifies a protective earth ground.

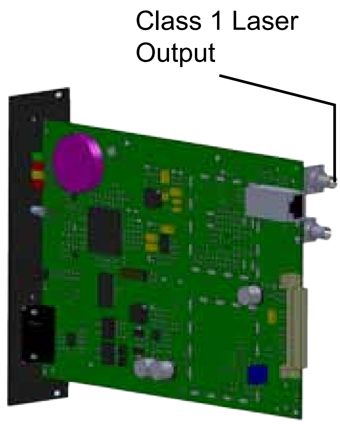


Figure Safety-1: Class 1 Laser output

FCC Rules

NOTE- This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Important Safety Information

Table of Contents

1. Introduction

2. Product Description

3. Site Planning and Assessment

4. INSTALLATION

5. System Calibration

6. Maintenance & Troubleshooting

7. Network Integration

Appendix A: Connecting Conduit Sections

Appendix B: Terminating Optical Fiber

Appendix C: Product Specifications

Appendix D: Warranty

Index

1

INTRODUCTION

Introduction to the FD-348R Series

The Fiber SenSys FD-348R Series Fiber Optic Intrusion Detection System builds upon a proven design. The optical fiber-based system has been designed to be immune to the effects of Electromagnetic Interference (EMI), lightning and radio frequency emissions. The system has also been designed to resist most environmental factors that cause nuisance alarms such as animals, wind, trees and other such non-threatening events. The FD-348R provides maximum effective intrusion detection through it's inherent system flexibility and advanced programmability.

Improved network flexibility is included with the FD-348R APU allowing the end user the choice of either embedded Fiber Security Network (FSN) compatibility or IP/XML communication for direct network interface.

As with previous generation models, the key component of the FD-348R APU is its fiber optic sensor cable. This uniquely-designed cable, which is sensitive to movement, pressure and vibration, can be routed along the fabric of a fence to detect climbing and cutting or it may be routed along the ground and covered over with gravel or sod to detect an intruder's footsteps. In both of these applications, referred to as *fence line* or *buried applications* respectively, detection of an intruder triggers an alarm in the Alarm Processing Unit (APU). The FD-348R series can also be used in rooftop or wall applications.

Some of the intrusions the FD-348R can detect include:

- Fence climbing (along both the fabric and post)
- Fabric cutting
- Digging underneath a fence
- Ladder assisted climbing of a fence
- Slow walking, running or crawling across a secure zone
- Tunneling underneath a secure zone

Advantages of the FD-348R APU

The FD-348R can be rack mounted up to 20 kilometers (12.4 miles) from the secure or protected zone. This feature lets the user install the APU in a location that is close to power and communications as well as secure from weather. As a rack-mounted member of the 300 series product line the FD-348R allows up to 8 separate zones to be monitored from a single 19 inch rack.

The system is able to monitor the site from such a distance because it uses *insensitive leads* to tie the APU to the sensor cable. These fiber optic leads are not sensitive to movement.

Since the APU is connected to the protected zone via the glass optical fiber, there is no conductive path for lightning or power surges. The optical fiber is intrinsically safe from EMI and radio frequency emissions. When correctly deployed, the sensor cable also meets the "intrinsically safe" requirements for Class I, Division II flammable hazardous areas as defined by *29 CFR Part 1910, Subpart S, Electrical Safety in the Workplace*. For more information on deploying the FD-348R for use in Class I, Division II environments, refer to *Protection of Flammable Hazardous Areas*, an application note available from Fiber SenSys.

With buried applications, the detection zone is covered and the sensor cable position cannot be detected without digging.

Using This Manual

This user's manual covers setup, calibration, operation and maintenance of the FD-348R Fiber Optic Intrusion Detection Systems. Theory of operation is covered in Chapter 1. Chapter 2 provides connection details and system component description. Chapters 3 and 4 provide instructions for planning and deploying the system. These chapters should be read as a minimum prior to installing the system.

Principles of Operation

The FD-348R's effectiveness is based upon the abilities of its fiber optic sensor cable. The system works because while the sensor cable is immune to the effects of lightning, Electromagnetic Interference (EMI) and radio frequency transmissions, it is still extremely sensitive to movement, vibration and even pressure. The FD-348R uses this principle by transmitting light from a laser in the APU through the sensor cable and back to a detector. When the sensor cable is physically disturbed by vibration or pressure, it induces a phase shift in the transmitted light which the APU receiver then detects and translates into an event.

How Optical Fiber Conducts Light

Optical fiber conducts light using principles of *refraction*.

Light traveling in a vacuum travels at 3.0 x 108 meters/second; however, light travels at a slower speed when traveling through a different medium such as glass. When we compare the speed of light in a vacuum to the speed of light as it travels through a medium, we end up with a ratio called the *index of refraction*. This ratio can be expressed:

$$n = \frac{\text{speed of light in a vacuum}}{\text{speed of light in a medium}}$$

Where n is the index of refraction.

An optical fiber is constructed so that the light-conducting core (see Figure 1-1) is made of a silicon material with one index of refraction while the cladding that surrounds it is made of silicon with a lower index of refraction, meaning the material is less dense and light travels faster through it.

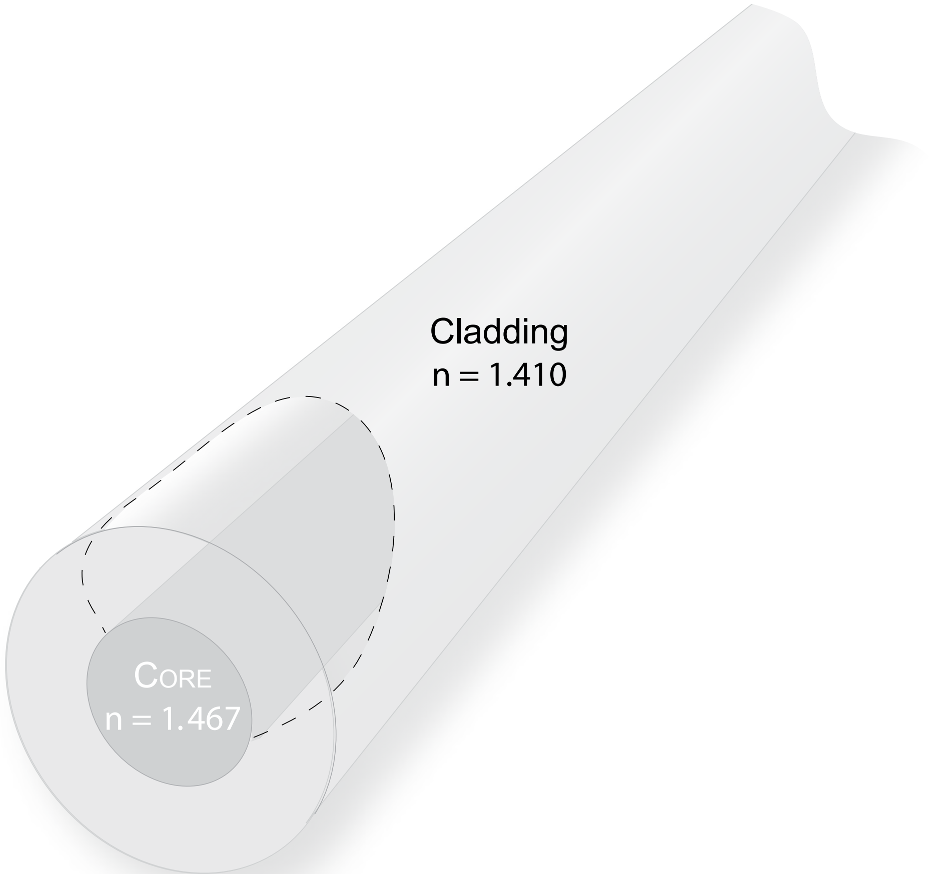


Figure 1-1: Cross sectional view of a glass fiber

Modes of light entering the core at an angle reach the cladding and bend back into the core because of a difference in propagation speed (light travels faster in the cladding – see Figure 1-2). This bending of light is known as refraction.

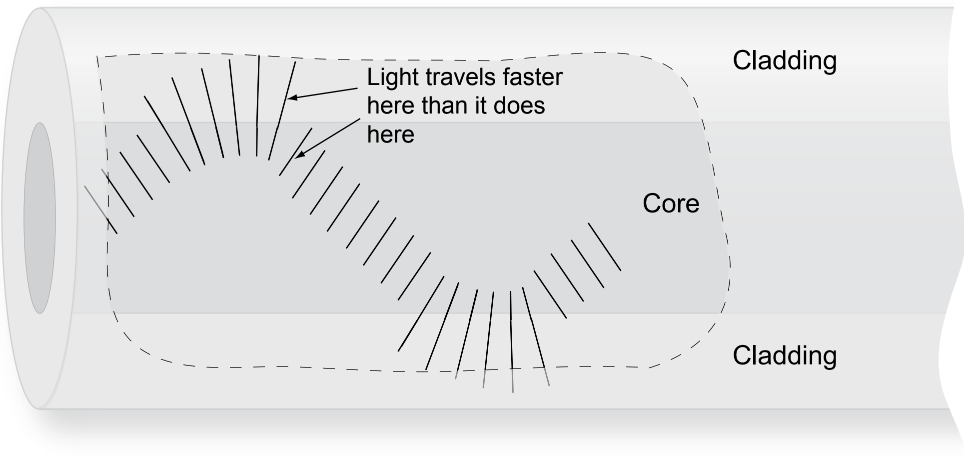


Figure 1-2: Light refraction and propagation in a fiber

Because modes of light traveling at an angle are bent back into the core (a principle called *Total Internal Reflection*), they continue to propagate down the length of fiber, enabling the fiber to conduct light from one end to the other.

How the Sensor Cable Works

The sensor cable is an optical fiber with a specific core size and unique jacket design that ensures it picks up tiny vibrations while remaining relatively impervious to the effects of weather and other harsh environmental variables.

While light is launched from the laser into the fiber optic cable, the APU monitors its phase as it returns. Assuming nothing has disturbed the sensor cable or propagation of the light, the phase remains the same. When the sensor cable is disturbed by movement or vibration, however, the conditions of the traveling mode of light change.

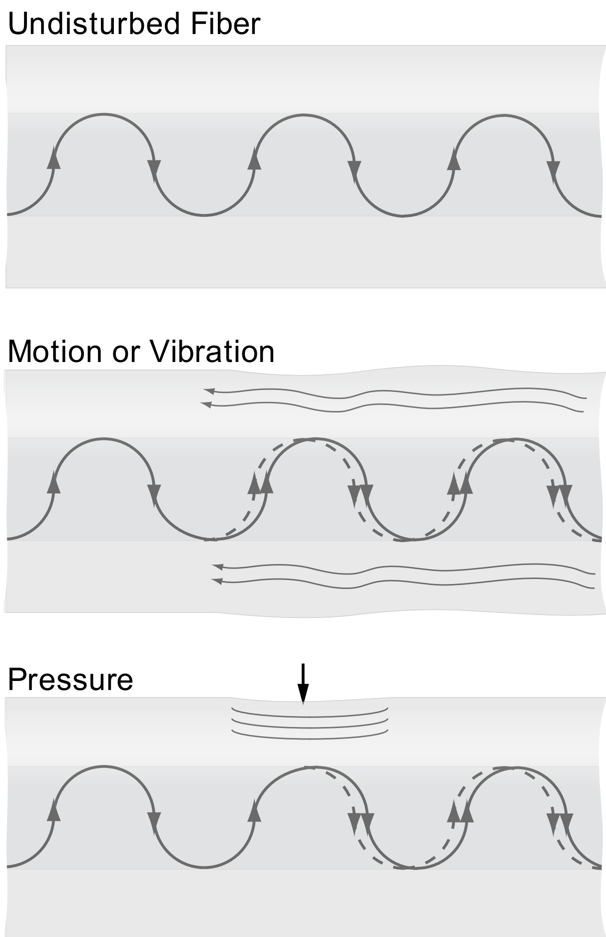


Figure 1-3: Effects of motion and vibration

Motion, vibration or pressure induces modal interference resulting in a net *phase shift* in the light. The APU receiver detects the phase shift, which is directly proportional to the amount and type of disturbance detected by the sensor cable. The detected signal is then processed to determine if it represents a valid event or if it is something to be ignored. Whether or not a detected signal qualifies as an event is determined by user-adjusted APU calibration parameters.

Effects of APU Calibration

The electronics convert the optical signal it into an electrical one and then digitize it. A Fourier transform is performed to convert the signal from the time domain to the frequency domain to look for vibrational signatures characteristic of an intruder.

Two separate processors reside in the FD-348R APU to process and evaluate the incoming digitized signal. These processors, labeled Processor 1 and Processor 2, are programmed individually to alarm for different conditions (Figure 1-5). This allows the user to calibrate the FD-348R to take into account how a fence-climbing intruder affects the sensor cable versus one who is cutting the fence fabric. With the FD-348R, Processor 1 default settings are optimized to detect fence climbing and Processor 2 settings are optimized to detect fabric cutting. With buried applications, only 1 processor is needed. Thus, Processor 2 is typically disabled. For more information on these settings, see Chapter 5.

When an intrusion is detected in the returning optical signal and the magnitude of the initial disturbance, its corresponding frequency and other conditions meet the programmed criteria in either Processor 1 or Processor 2, an alarm condition will result.

Figure 1-4 depicts the signal processing diagram for the FD-348R APU.

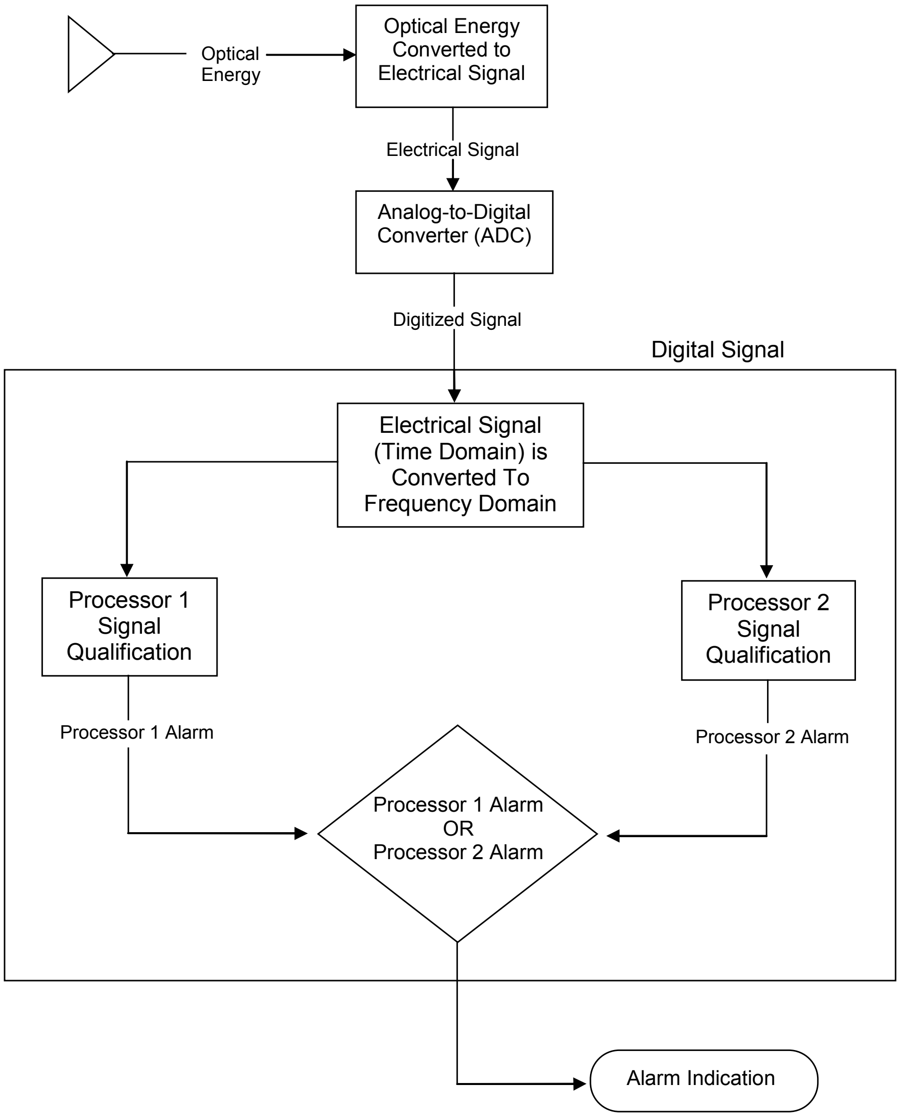


Figure 1-4: FD-348R signal processing block diagram

When an alarm condition is met, the APU activates an alarm relay, causing a corresponding set of normally-open and normally-closed contacts to change state on the back of the RK-348. The FD-348R does not provide users with any active alarm signals.

Users can calibrate or adjust the FD-348R parameters to account for the affects of wind, tree branches, animals and other sources which might generate nuisance alarms. Proper calibration ensures that nuisances are largely ignored while valid conditions created by an intruder generate an alarm, regardless of how stealthy.

For more detailed information on system calibration, see Chapter 5.

2

PRODUCT DESCRIPTION

Product Components

The FD-348R Alarm Processing Unit (APU) is intended for use in situations where multiple "zones" must be protected and monitored independently of one another. It is mounted into the RK-348, a standard 19 inch rack that accommodates up to 8 APU modules. In addition to relay contacts two user-selectable communication methods are available on the FD-348R: Fiber Security Network (FSN) or XML via TCP/IP connectivity. For more information on configuring and using both communication methods see *Network Integration,* chapter 7. A complete FD-348R series system includes the following components:

- The FD348R APU (up to 8 per RK-348 rack)
- The RK-348 rack
- Sensing cable
- Insensitive lead in cable
- Cable conduit (fence-mounted applications only)

Figure 2-1: FD-348R series system components

The FD348R APU

The (APU) is a module containing a laser, optical detector and the electronics for processing return optical signals. The APU is a user-calibrated instrument allowing users to define the alarm thresholds on a custom basis per APU.

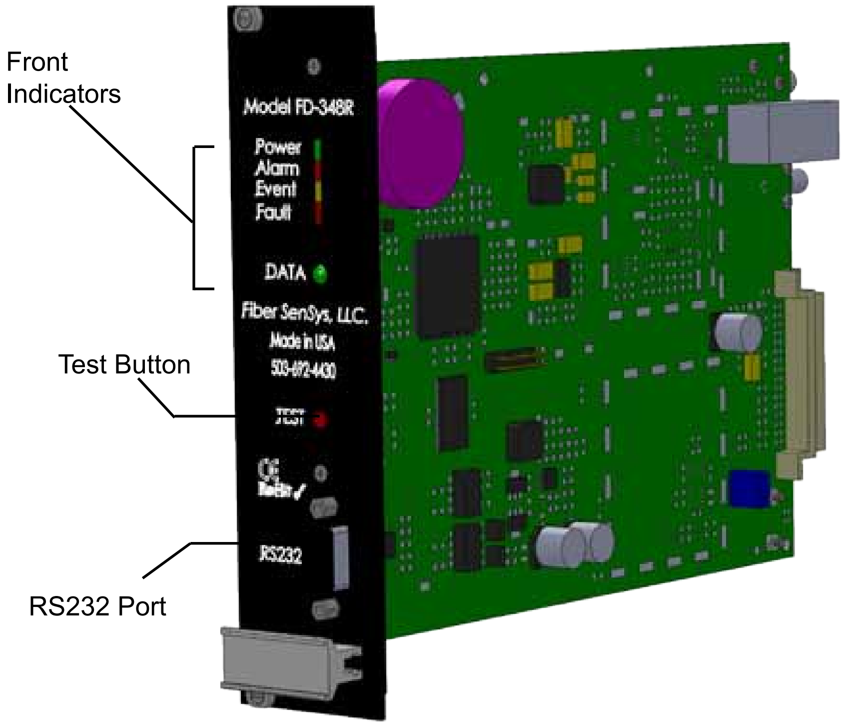


Figure 2-2: The FD-348R APU front panel

RS-232 Port

The RS232 connector is used for connecting to a calibration interface such as a PC with SpectraView® or terminal emulation software.

RS-232 Connector Pinout

The pinout for the RS-232 connector on the FD-348R APU is as follows:

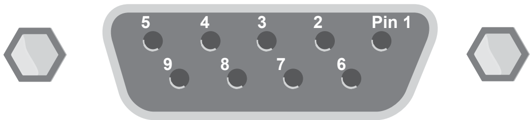
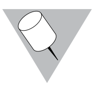


Figure 2-3: The APU's RS-232 connector pinout

Table 2-1

Pin Number	Description
1	No connection
2	T x D transmit
3	R x D receive
4	No connection
5	Ground
6	No connection
7	RTS
8	CTS
9	No connection



NOTE:
Cables connected to the APU’s RS-232 connector must be straight-through type DB-9 serial cable.

Indicator Lights

- "Power" LED Illuminates when power is applied to the unit.
- "Alarm" LED indicates an alarm condition has occurred
- "Event" LED indicates a disturbance or event has been detected in the sensor cable
- "Fault" LED indicates a loss or significant degradation of returning optical power
- "Data" LED shows network activity (FSN and XML) and is green when the network is active. When data is transmitted the light will flash red.

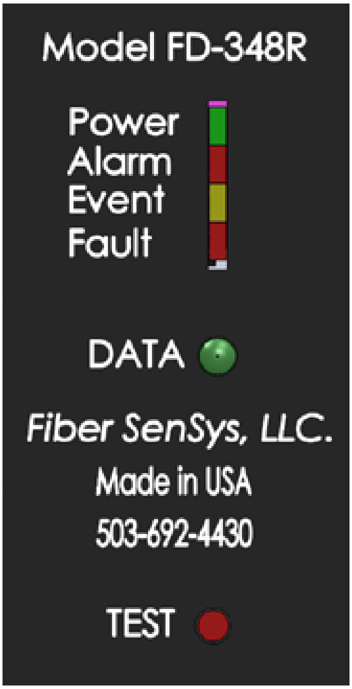


Figure 2-4: Close-up of front panel indicators.

Test Button

The "**Test**" button found below the LED indicators activates the alarm and fault relays. Pressing the Test button causes the Alarm and Fault LEDs to illuminate and the corresponding relay contacts to change state.

Rear connections

The back of the FD-348R has two optical connections and one RJ45(ethernet) receptacle.

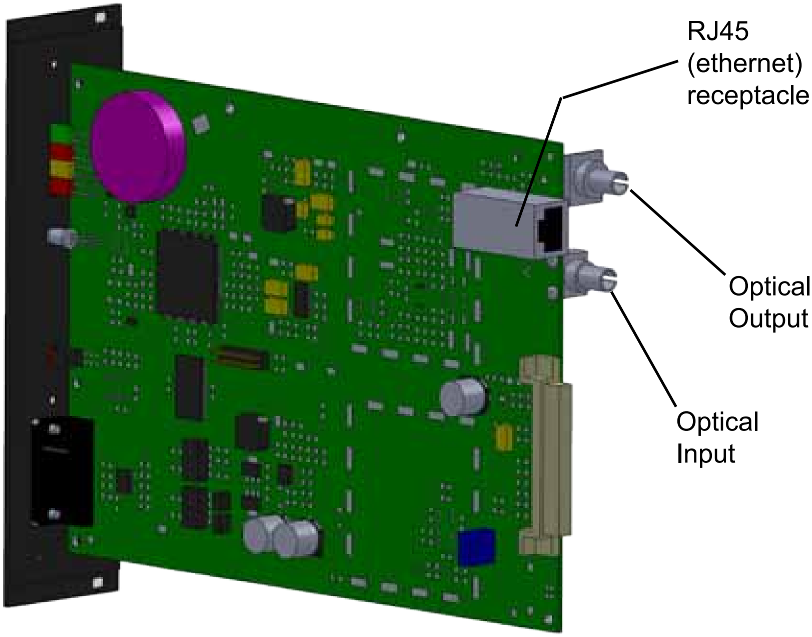


Figure 2-5: The FD-348R rear connectors

Optical connectors. Optical connectors (input and output) are located on the upper rear of the APU modules and are accessible on the back of the RK-348 when the modules are mounted in the rack. The insensitive leads of the FD-348R are connected to these connectors.

RJ45(ethernet) receptacle: The RJ45 receptacle used for XML integration via TCP/IP communication is also located on the rear of the APU modules and is accessible on the back of the RK-348 when the modules are mounted in the rack. Standard RJ45 ethernet connectors are compatible with these receptacles.

Rack-Mount Chassis (RK-348)

The rack-mount chassis shown in Figure 2-6 holds up to eight FD-348R APU modules and provides power to each.

Figure 2-6: The RK-348 with 8 FD-348R APU modules

The power switch and AC power connector is located on the rear panel of the rack. The power switch provides power simultaneously to all installed APU modules. The input power to the RK-348 power supply is user selectable from 120 to 240 VAC, 50 to 60 Hz. For more information on setting the input voltage range, see *Setting the Input Voltage Range* in Chapter 4.

WARNING!
A PROTECTIVE GROUND CONNECTION BY WAY OF THE POWER CORD IS ESSENTIAL FOR SAFE OPERATION. IF THE GROUND CONNECTION IS LOST OR IF THE PLUG IS NOT PLUGGED INTO A PROPER RECEPTACLE, ALL CONDUCTIVE PARTS OF THE INSTRUMENT CAN RENDER AN ELECTRIC SHOCK.

RK-348 Rear Panel Connections

The back of the RK-348 exhibits several mounted FD-348R connections and an on/off switch. These connections are shown in Figure 2-7 seen below.

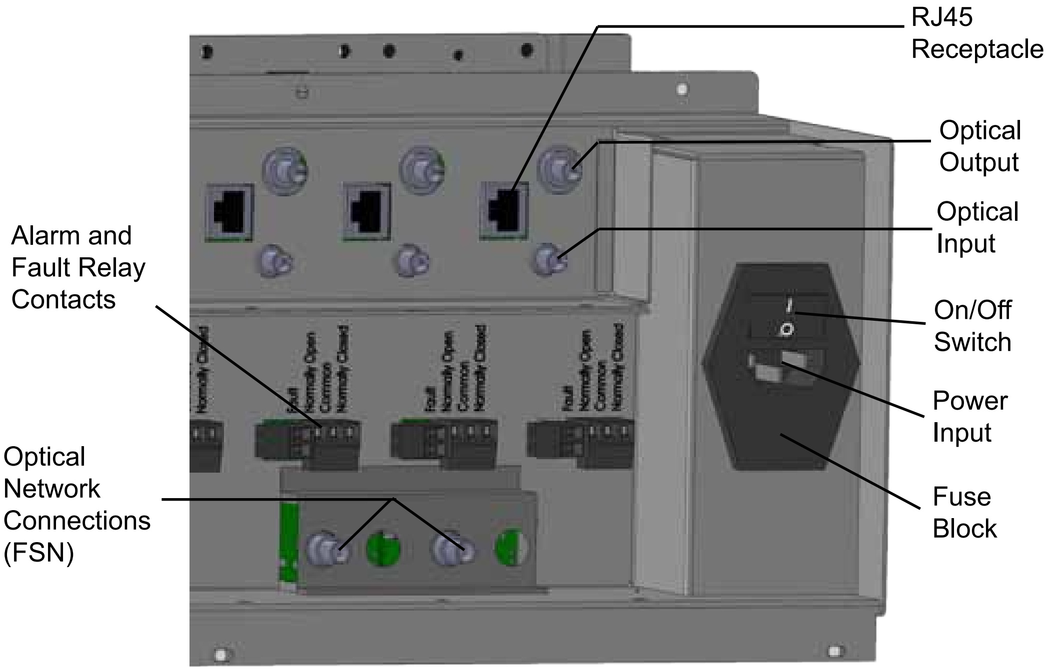


Figure 2-7: RK-348 Rear Panel Connections

Connections are as follows:

- The terminal block connections that convey alarm and fault status via normally open and normally closed relays
- Optical connections for the insensitive lead in for the APU
- RJ45 (ethernet) connections to each Alarm Processor
- Optical Connections for the Fiber Security Network (FSN)
- Power Cable Connection
- On/Off switch

Relay Terminal Block Connections

The alarm terminal block connections are detailed below in Figure 2-8.

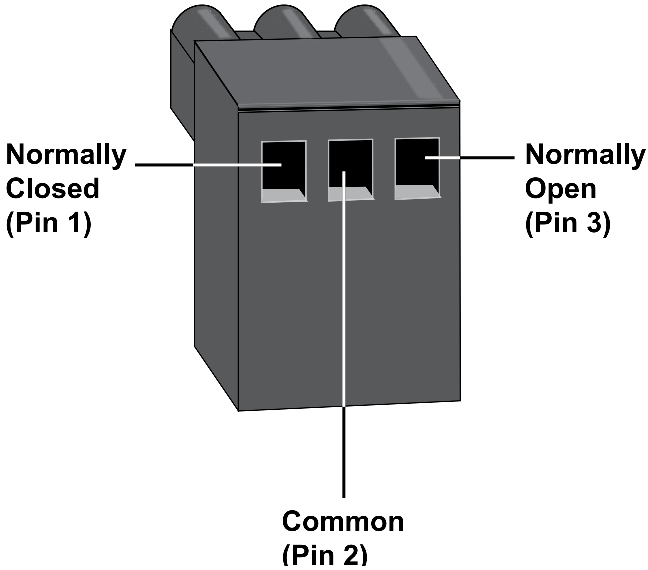


Figure 2-8: FD-348R alarm relay contacts

Alarm and fault relay connectors. Below the optical connectors of each module are terminals for connecting to the fault and alarm indicating relays. The normally-closed fault relay contacts open whenever optical power drops more than 25dB below the nominal output level.

There are three pins for connecting to the alarm indicating relay. Pins are numbered 1 to 3 from left to right (as viewed from the rear of the rack assembly - see Figure 2-7). Connect the common lead to **Pin 2**. To wire a system for a normally closed alarm indicating relay, connect the positive lead to **Pin 1**. To wire a system for a normally open alarm indicating relay, connect the positive lead to **Pin 3**.

WARNING!
DO NOT APPLY AC VOLTAGE TO THESE PINS. THE ALARM RELAY CONTACTS ARE RATED FOR DC VOLTAGE ONLY (100 mA at 24 VDC).

Sensor Cable

The sensor cable for the FD-348R series is distinguished by its brown or dark green protective jacket. This jacket ensures the cable is resistant to weather, dirt, etc. The sensor cable forms the backbone of the FD-348R.

Sensor cable comes in 2 configurations, depending upon the application:

SC-3 (brown jacket) – 3 mm sensor cable used for fence line or wall applications

SC-4 (green jacket) – 4 mm sensor cable used for buried applications

Sensor cable comes in varying lengths, with up to 2000 meters (6500 feet) per spool.

Insensitive Leads

The insensitive leads, so named because they are unaffected by vibrations, are distinguished by their gray or blue protective jackets. Like the sensor cable, the insensitive leads are made of optical fiber that is immune to RF and EMI energy. The insensitive leads are also weather resistant. These leads are used to transmit light from the APU to the sensor cable mounted in the protection zone and back again.

Insensitive leads come in 3 configurations, depending upon the FD-348R's application:

IC-3 (gray jacket) – 3 mm exterior-grade cable for above ground applications

IC-3D (gray jacket) – 6.5mm exterior-grade duplex cable containing two fibers for sending and receiving within a single cable (above ground applications)

IC-4 (blue jacket) – 4 mm exterior-grade cable for buried applications

Cable Conduit

The sensor cable is enclosed in a protective cable conduit before it is deployed. The conduit most commonly used with the FD-348R is the EZ-400NSS, offered by Fiber SenSys in a kit containing 100 meters of 1/2 inch diameter non-split conduit, 500 stainless steel wire ties, a barrel coupler and a box coupler for connecting two sections together.

The EZ-300NSS is a more rigid and thicker non-split conduit with a diameter of 5/8 inch.

Fiber SenSys also offers a split conduit kit, the EZ-300SS. This kit contains 100 meters of split conduit, 4 expansion joints (for coupling sections of conduit together) and 500 stainless steel wire ties.

System Block Diagram

A block diagram of the FD-348R and its system components can be found below in Figure 2-9:

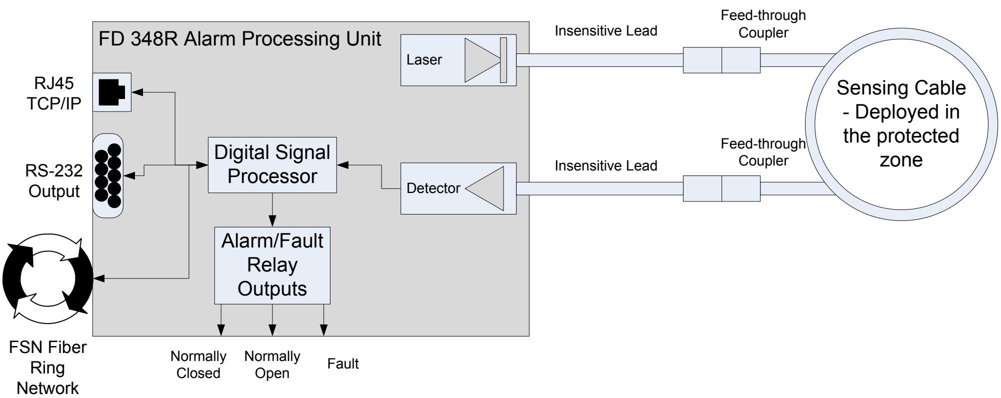


Figure 2-9: FD-348R system block diagram

For more information on the principles of operation behind the FD-348R and its components, refer to *Principles of Operation* on page 1-1 in Chapter 1.

3

SITE PLANNING AND ASSESSMENT

The successful installation and operation of the FD-348R is determined by a thorough understanding of the security needs of the site to be protected as well as proper deployment of the sensor cable. This chapter will lead the reader through the site planning and threat assessment procedure.

Prior to installing the FD-348R and deploying the sensor cable, the site to be protected must be assessed carefully for all security needs and threats against it. For example, if there is a possibility that a potential intruder could cut the fabric of a perimeter fence, sensor cable needs to be deployed along the fabric to detect the intrusion.

In addition to the security needs and threat assessment, the system maintenance requirements and compatibility of the equipment must also be taken into account. If, for example, the FD-348R alarm relays are wired to activate remote video equipment, the maintenance requirements and compatibility of the FD-348R and video equipment should be considered.

Careful assessment of these principles is necessary for a successful installation.

Fenced Perimeters

Possible Threats

There are 6 specific threats against any fence line:

- Climbing the fabric of the fence
- Climbing the fence posts
- Cutting the fabric
- Digging under the fence
- Lifting the fence fabric
- Ladder-assisted climbing of the fence

Successful protection against these threats depends on the proper deployment of the sensor cable and calibration of the APU.

Fence Line Sensor Cable Deployment Guidelines

Deploying the sensor cable properly will ensure the FD-348R detects threats against a fence line.

When determining a strategy for protecting the site, there are 3 important points to keep in mind regarding the sensor cable:

- The sensor cable detects vibration. Therefore, the sensor cable should be deployed in such a way that it will ideally be free of vibration until and unless it is caused by an intruder.
- The sensor cable has the same level of sensitivity throughout the cable. Areas which are affected better by vibrations may need sensor cable run through only once but areas in which vibration is conducted less readily (such as fence posts or reinforced fence sections) should have more sensor cable deployed to compensate.
- The detection system is *linear*, meaning the APU cannot distinguish where along the sensor cable an event occurs. In order to localize the point where an intrusion occurs, the FD-348R deployment must be separated into multiple zones at intervals reasonable enough to help locate an intruder when an alarm is received.

To ensure the sensor successfully detects against intrusions, take these other considerations into account:

Fence noise. The fence should not generate excessive noise. For chain link fences, re-tensioning the fence fabric and adding additional fence fabric wire ties to eliminate metal-to-metal banging of the fabric can quiet the fence. The fabric should also be secured firmly to all fence posts.

Fence material. The entire fence line should be composed of the same material inside the protected zone (similar gauge and construction). For a chain link fence, all of the fabric in the zone should be tensioned to the same level.

Fence clearance. There should be a clear area around the fence on both sides, free from tree limbs, large rocks or structures – man-made or natural – which could aid an intruder in climbing over. There should also not be any point along the fence line under which an intruder could easily crawl or dig under the fence.

Man-made and natural barriers. Buildings, structures, waterfronts and other barriers used in place or as part of the fence line should provide adequate protection against intrusion. Ensure there are no windows, doors, openings or unguarded means of access.

Figure 3-1 shows two common fence line sensor cable deployments based upon the level of the security threat. One deployment is for medium level threats and the other is for high level security threats.

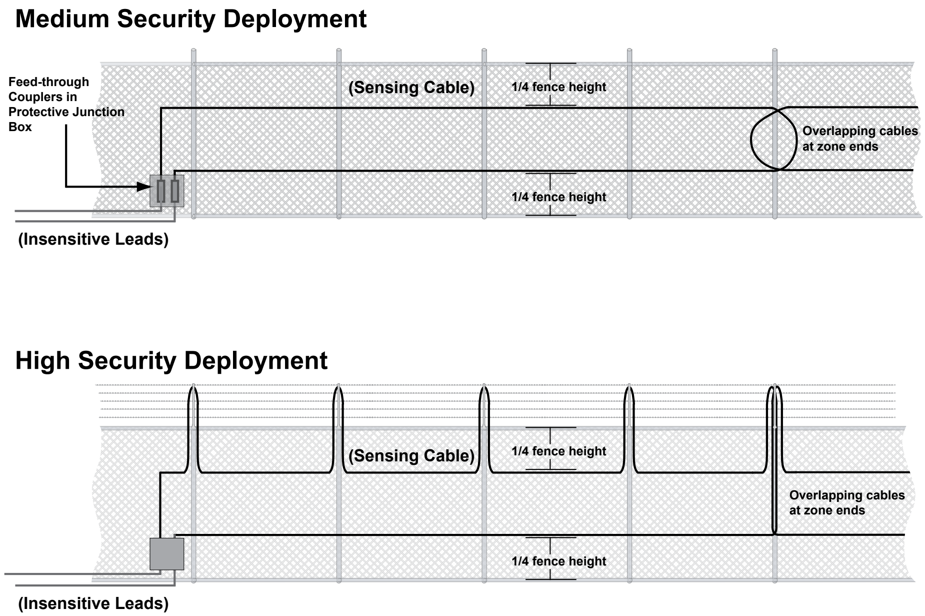


Figure 3-1: Sensor cable deployment types

Within each zone, the sensor cable loop is attached 1/4 of the fence height from the top and bottom of the fence.

Medium Threat Level: Medium threat level deployment is where moderately sophisticated intrusion attempts are expected from the intruders. The sensor cable is deployed along the lower and upper levels of the fence places the sensor cable in close proximity to the source of the stealthy intrusion (e.g. intruders attempting to tunnel under the fence, clime fence posts, etc.).

High Threat Level: Provides maximum detection capability of stealthy intrusion attempts for high security facilities. Sensor cable added to the fence outriggers raises the system sensitivity to intruders trained in security system penetration.

In both deployments, note that the sensor cable is routed along the fence in a loop encompassing the length of the zone (for a maximum total sensor cable length of 5 kilometers or 16,400 feet) and the sensor cable loop is attached 1/4 of the fence height from the top and bottom rails of the fence.

To further increase the system sensitivity to stealthy intrusion attempts, the sensor cable should be routed between the fence fabric and the fence posts where possible. The sensor cable should also overlap from one zone to the next. With high threat level installations, running an additional sensor cable loop up each post to the top of the outrigger protects against intruders climbing the fence posts. For more information on protecting fence posts, see *Corners and Posts* on page 3-12. Details for protecting top guards are discussed further in *Outriggers (Barbed or Razor Wire)* on page 3-10.

There are many ways to deploy the sensor cable to protect a fence line, two of which are the medium and high security deployments in Figure 3-1. Choose a cable deployment that best protects the fence line against all possible types of intrusion determined during threat assessment.

While developing a strategy take note of and record:

- The length of the fenced perimeter (not including the gates)
- The number of gates and the length of each
- The number of reinforced sections and their lengths
- Distance from the fence to the APU
- The width of roadways or walkways through all site gates
- The height of the fence
- The fence structure and type of material

NOTE:
Keep a detailed list of these factors and their associated numbers. They will be used during the installation procedure.

The following sections outline recommended sensor cable deployment strategies for different barrier types.

Chain Link Fence

Generally, sensor cable deployed across the middle of a chain link fence is enough to detect any intruder attempting to climb over, or cut the fence fabric, but deploying sensor cable in a loop raises the probability of detecting these threats. The loopback configurations illustrated in Figure 3-1 also protect against intruders attempting to lift the fence fabric.

In order for the sensor cable to be most effective, the fence should meet the recommended height specifications outlined in this chapter. Fences taller than 2.4 meters (8 feet) may require repositioning of the sensor cable or adding an additional loop of deployment. For more information, see *Chain Link Fence Specifications* later in this chapter.

Reinforced Fence Sections

Because they’re less likely to transmit vibration as readily as non-reinforced fence sections, reinforced fence sections require additional cable in order to increase the effectiveness of the cable through the region. The best and simplest way to accomplish this is to add an additional local “loop” of sensor cable in the reinforced section as shown in Figure 3-2. Adding the loop increases the amount of sensor cable per unit of area, resulting in a net increase in vibration sensitivity in the affected section.

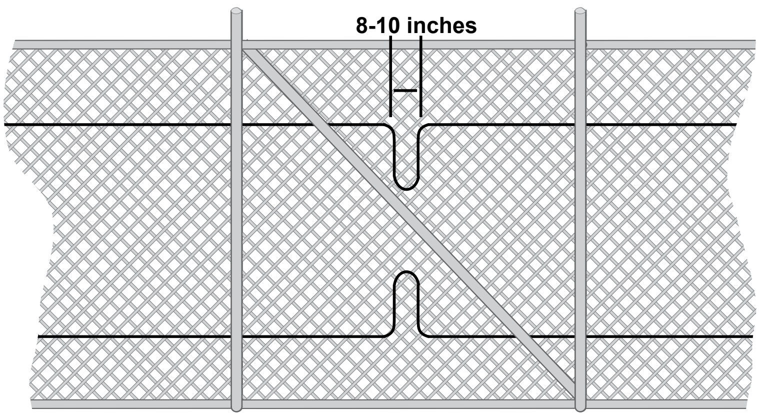


Figure 3-2: Deployment in a reinforced fence section

The extra loop is added to both the top and bottom strands of sensor cable (for a loopback deployment). Make the width of the loop(s) between 20 to 25 cm (8 to 10 inches).

Cable deployment in reinforced sections differs when a top guard is used in tandem with the fence. In such a case, the sensor cable is attached just 5 cm (2 inches) from the bottom rail of the fence, as shown in Figure 3-3. In all non-reinforced sections, the sensor cable is attached 1/4 of the fence height above the bottom rail.

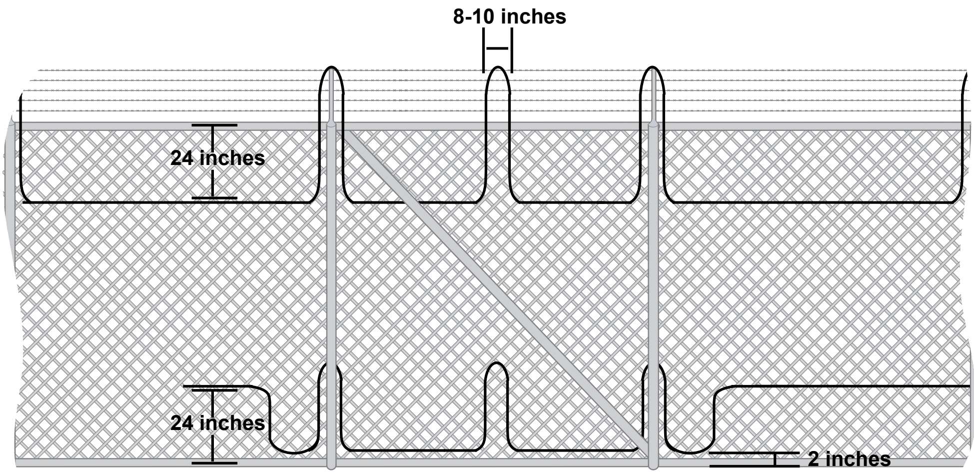


Figure 3-3: Detailed view of a reinforced section with an outrigger

The loop in the top strand of the sensor cable should extend to the top of the outriggers and top guard. As is done with fence posts, the sensor cable is run between the fence fabric and the reinforcement bar where possible.

The added loops on the fence posts increases the system sensitivity in the region. For more information, see *Corners and Posts* beginning on page 3-13.

Outriggers (Barbed or Razor Wire)

The typical way of protecting an outrigger, such as barbed or razor wire, is to deploy sensor cable across it. In the case of barbed wire, this means looping the sensor cable across all strands as shown in Figure 3-4.

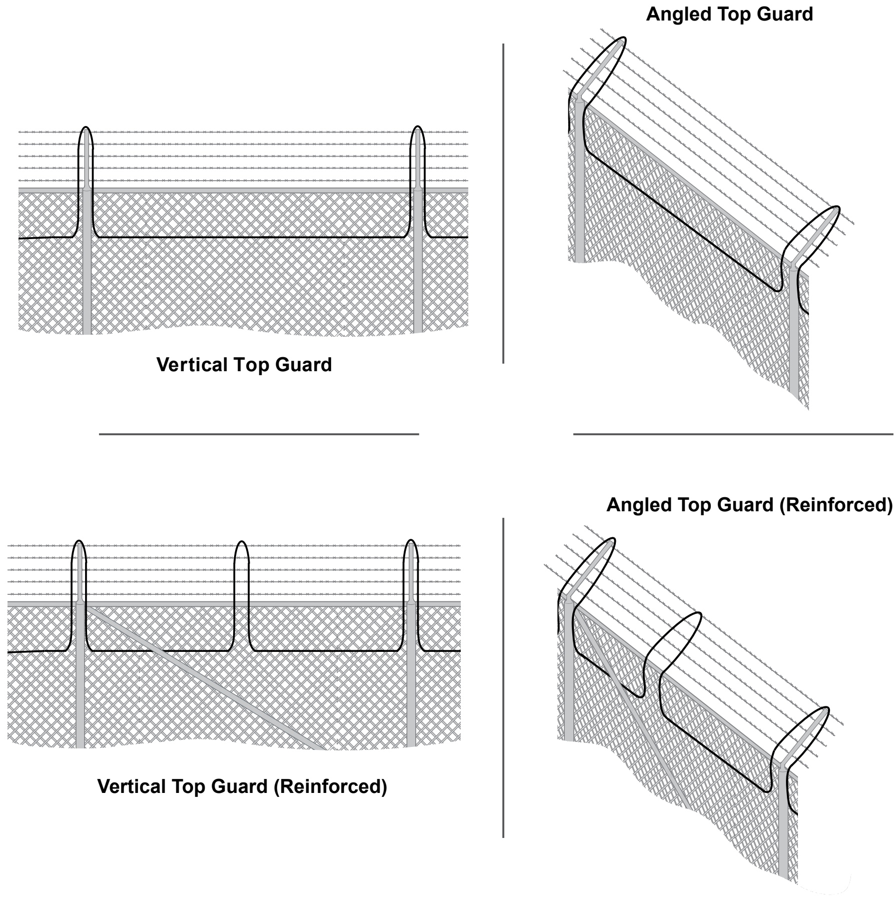


Figure 3-4: Examples of barbed wire sensor deployment

In all cases where barbed wire is used with a chain link fence, the sensor cable should be deployed in the high security configuration shown previously in Figure 3-1. Ensure the sensor cable loops protecting the outrigger extend to the top. An extra cable loop must be added to the middle of any reinforced sections.

If razor wire (also known as concertina or “c-wire”) is used as a top guard, the recommended method of deploying sensor cable is to attach it to the inside of the razor wire coils.

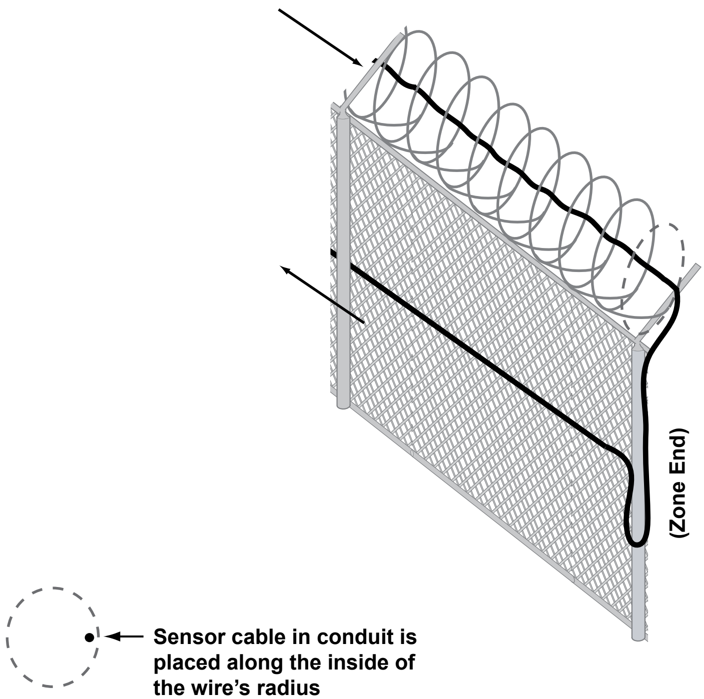


Figure 3-5: Razor wire sensor cable deployment

Corners and Posts

Because corners and posts are rigid and less likely to transmit vibration than the fence fabric, they should be protected by adding extra sensor cable in a loop as shown in Figure 3-6.

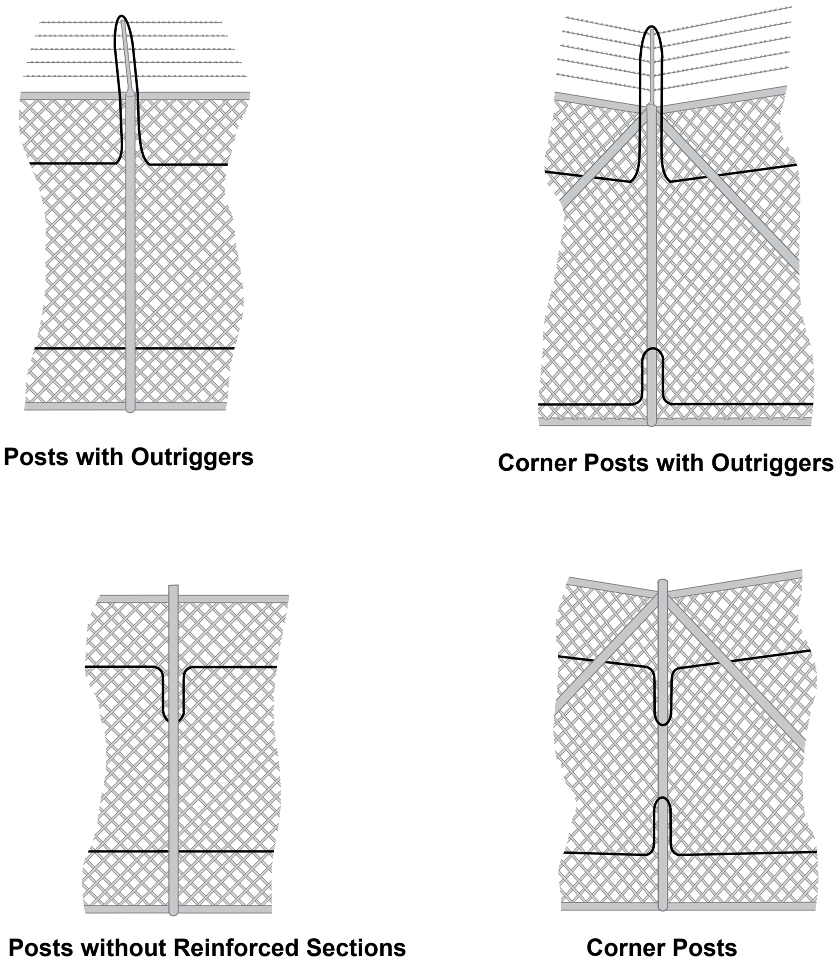


Figure 3-6: Fence post protection methods

For fences with outriggers, the cable loop should extend up to the top of the outrigger, protecting both the post and outrigger. Because fence sections at corners are normally reinforced, the prescribed method for deploying sensor cable in reinforced sections should be followed. For more information, see *Reinforced Fence Sections* on page 3-6.

Service Loops

Loops should be added at periodic intervals to allow the sensor cable to be re-spliced as necessary without having to remove then redeploy the entire cable. A good rule of thumb to use when considering service loops is to plan on adding one every 91 meters (300 feet) or so. Generally, plan on using an additional 1 and a half meters (about 5 feet) of cable with each sensor loop.

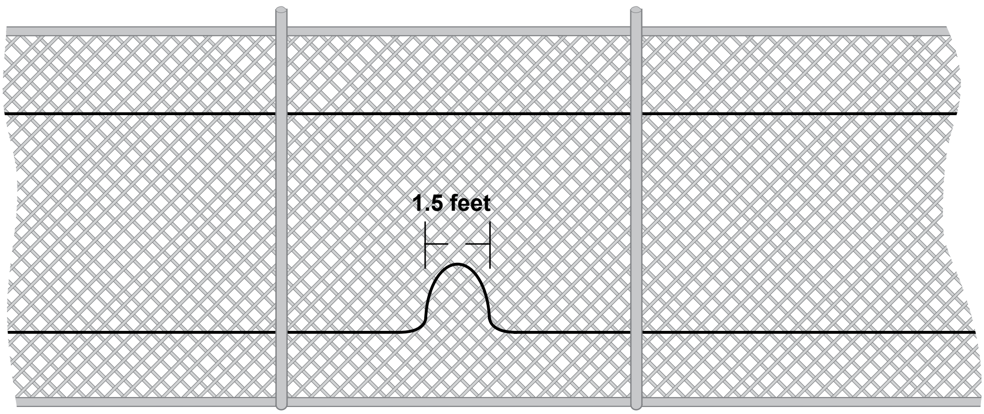


Figure 3-7: Service loop in sensor cable

Wrought Iron Fence

With proper deployment, the FD-348R sensor cable can also protect a wrought iron fence. For such an instance, the sensor cable is best deployed along the top and bottom fence rail. Because a wrought iron fence is designed to be rigid, the FD-348R must be calibrated carefully to ensure that nuisances have a minimal effect while maximum intrusion protection is afforded to the fence.

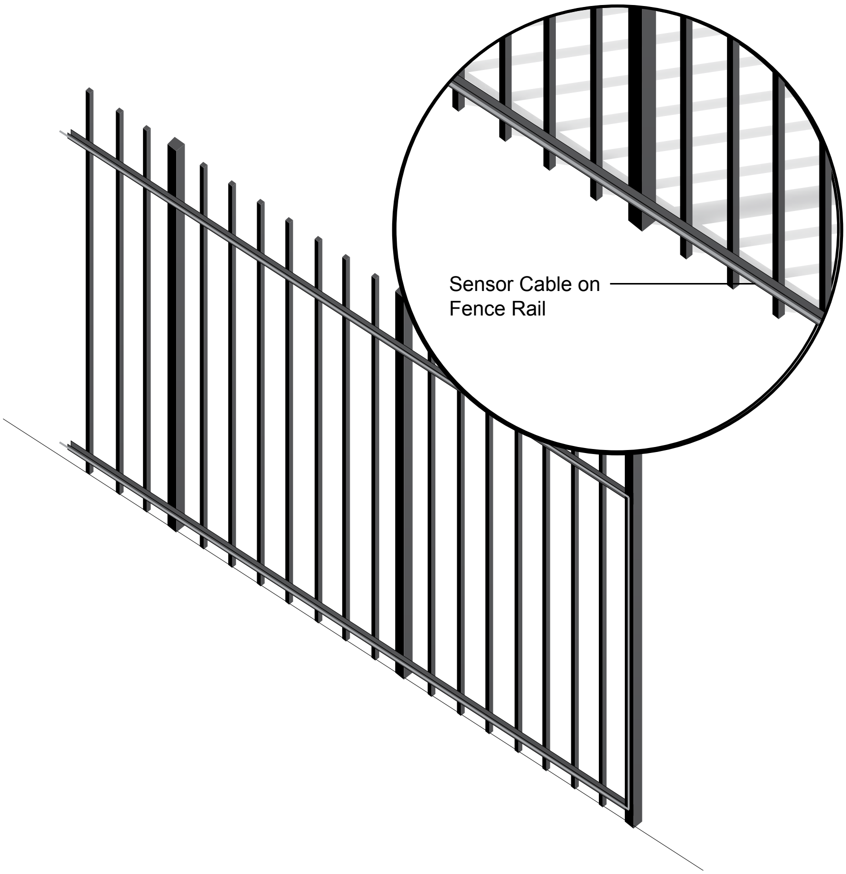


Figure 3-8: Deployment on a wrought iron fence

“Anti-Ram” Barrier Fences

Modern fence manufacturers have created various versions of “anti-ram” barrier fences. These barriers, which resemble wrought-iron fences in appearance, are made to withstand direct, high-pressure impacts from heavy vehicles. Such barriers are successful because they have built-in channels, allowing for the insertion of heavy, rolled-steel reinforcement cable. These channels are also ideal for inserting sensor cable.

With anti-ram barrier fence, deployment of the FD-348R fiber optic sensor cable is like that on a standard wrought iron fence. The cable is inserted into conduit (usually black in color) and attached to the top and bottom rails or channels. Secure the conduit/sensor cable assembly in place using UV-resistant cable ties. On most anti-ram barrier fences, the channels have been perforated with cutouts every 15 cm (6 inches) to allow cable ties to be threaded through.

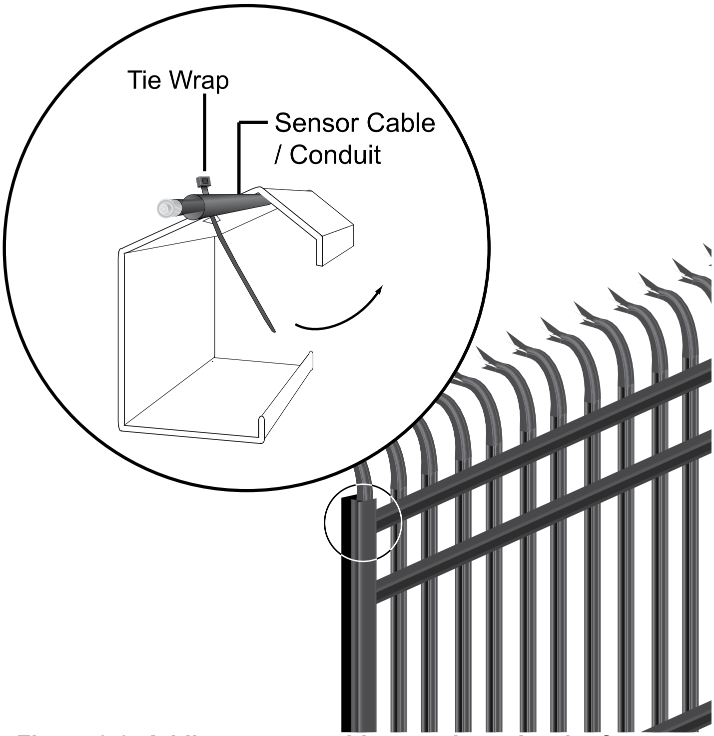


Figure 3-9: Adding sensor cable to anti-ram barrier fence

Glass Walls

The sensor cable can be mounted flush against the surface of the glass wall and detect virtually any threat against the glass. When deploying the cable, consider the need to place the cable so it is inconspicuous and develop a strategy accordingly. Also, take the effect of possible nuisances into account, i.e. the wind, low frequency vibrations from aircraft, animals tapping against the glass, etc.

Perimeter Walls

Concrete resting caps are used for decorative purposes with many brick wall perimeters. These resting caps make ideal platforms for concealed sensor cable. Sensor cable placed under a loose resting cap will detect an intruder attempting to climb over top of the wall (Figure 3-10).

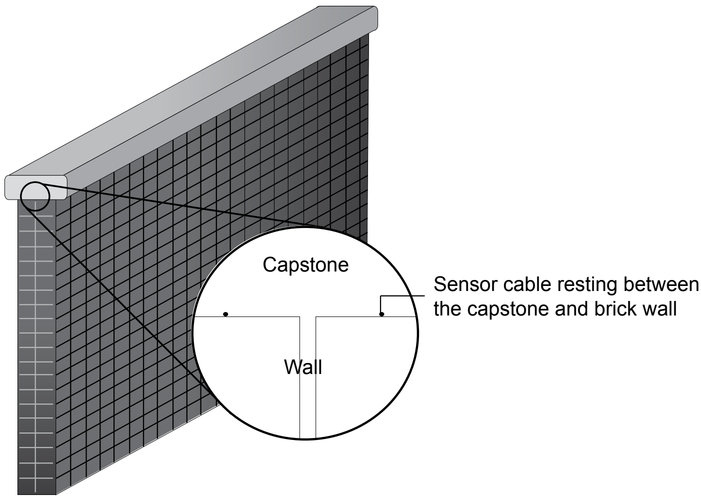


Figure 3-10: Deployment under a loose resting cap

When deploying a sensor cable in this application, a loopback configuration should be used to ensure there is equal weight distribution of the resting cap across the sensor cable (two cable strands can carry the weight evenly, as opposed to a single strand of cable which forms a fulcrum). Keep in mind that the resting cap should be secure enough to prevent movement during strong winds. Likewise, it should be unaffected by the presence of small birds, squirrels, etc.

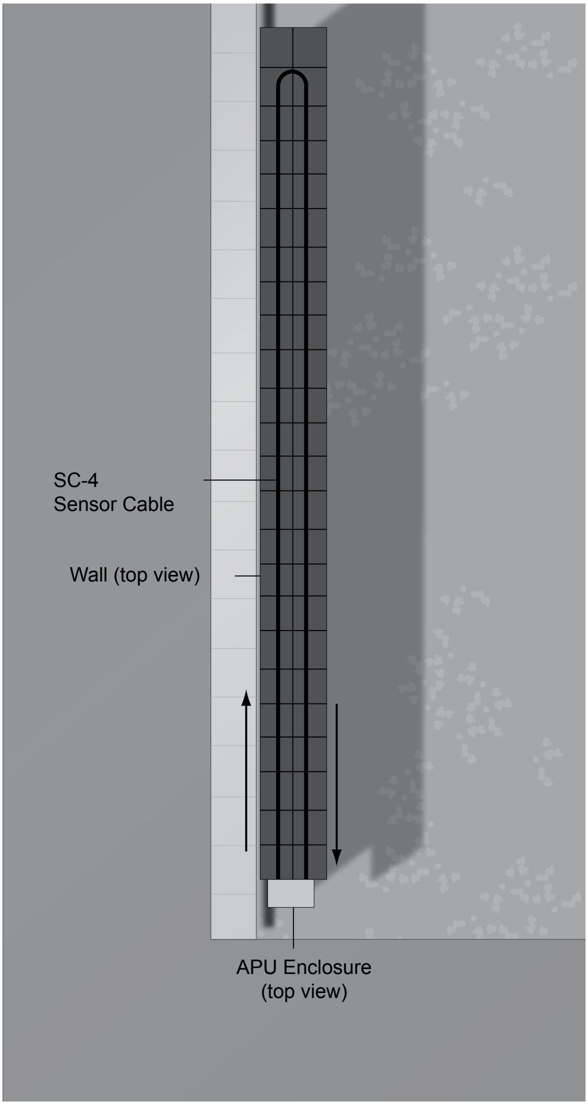


Figure 3-11: Loopback deployment below the capstone (top view)

SC-4 sensor cable must be used when doing a covert deployment beneath any resting cap.

Sensor cable is deployed on outriggers to protect concrete perimeter walls lacking capstones. This configuration also detects intruders attempting to climb over the top (Figure 3-12).

Outriggers used to support the sensor cable should be imbedded in the wall at least 2.5 cm (1 inch) or more and should have approximately a 10 cm (4 inch) clearance. Outriggers should also be imbedded near the outside edge of the wall at approximately a 45° angle. This practice ensures any attempt to scale the wall using a ladder will be protected. As with brick wall/capstone deployments, the sensor cable should be laid out in a loopback configuration.

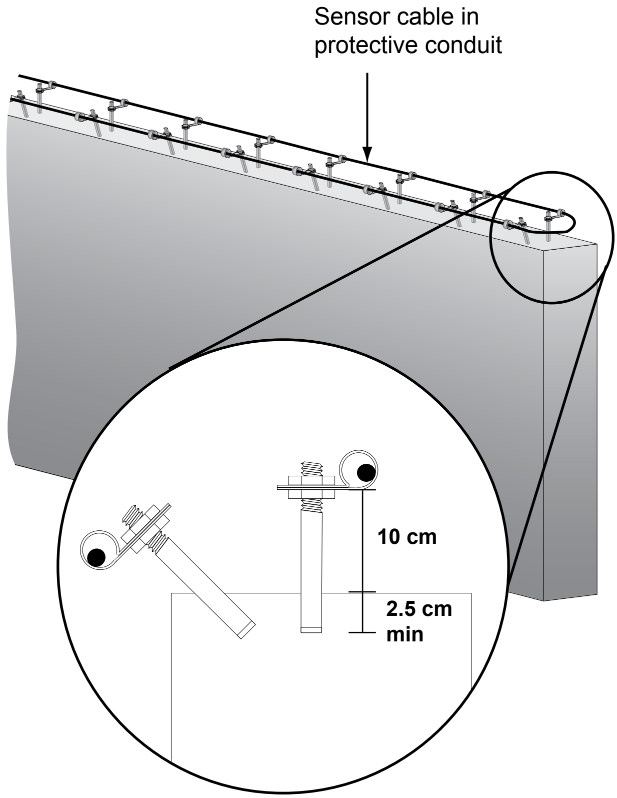


Figure 3-12: Protecting a concrete perimeter wall

All sensor cable should be deployed in protective conduit with this configuration.

Chain Link Fence Specifications

In order for a chain link fence to be most effective against intrusion, there are 8 specifications it should conform to:

Fabric. The fence fabric should be composed of steel chain with a mesh thickness of at least 9 gauge with openings not larger than 25 cm (2 inches). Additionally, the fabric should be tensioned consistently across its length throughout the protected zone.

Fabric ties. Only 9 gauge steel or larger ties are recommended. The fabric ties should be electrolytically compatible with the fence fabric to prevent corrosion. The fence fabric should be attached to the post using at least 4 evenly-spaced ties. All ties should be tight enough against the post to eliminate (or significantly reduce) mechanical noise.

Top guard outrigger. Outriggers, when used, should angle out in the direction of the unprotected area. At least three strands of barbed wire should be installed perpendicular to, and attached to, the top guard. The barbed wire should be well-tensioned and fastened where needed to eliminate mechanical noise.

Height. The height of the fence should be at least 2.1 meters (7 feet).

Fence posts, supports and hardware. All posts, supports and hardware should be pinned or welded to prevent disassembly of the fencing or removal of its gates. All posts and structural supports should be located on the inner side of the fencing. Posts should be secured in the soil with cement to prevent shifting, sagging or collapse. Additionally, posts should be placed every ten feet or less.

The use of “hog rings” and aluminum wire is not recommended.

Reinforcement. Taut reinforcing wires should be installed and interwoven or affixed with fabric ties along the top and bottom of the fence for stabilization of the fabric.

Ground clearance. The bottom of the fence fabric should be within 5 cm (2 inches) of firm soil or buried sufficiently in soft soil.

Culverts and openings. Culverts under or through a fence should consist of pipe 25 cm (10 inches) in diameter or less. If a larger pipe must be used, it should be properly grated and equipped with sensors to prevent access.

For more information on these requirements, refer to *Security Fence Construction Requirements*, a document available through Fiber SenSys.

Non-Fenced Perimeters

Possible Threats

There are 4 basic threats to any area that is not guarded by a fence:

- Walking across the area
- Running into the area
- Crawling
- Tunneling

These intrusions can each be detected by a proper buried deployment of the sensor cable around the perimeter of the area.

Buried Cable Deployment Guidelines

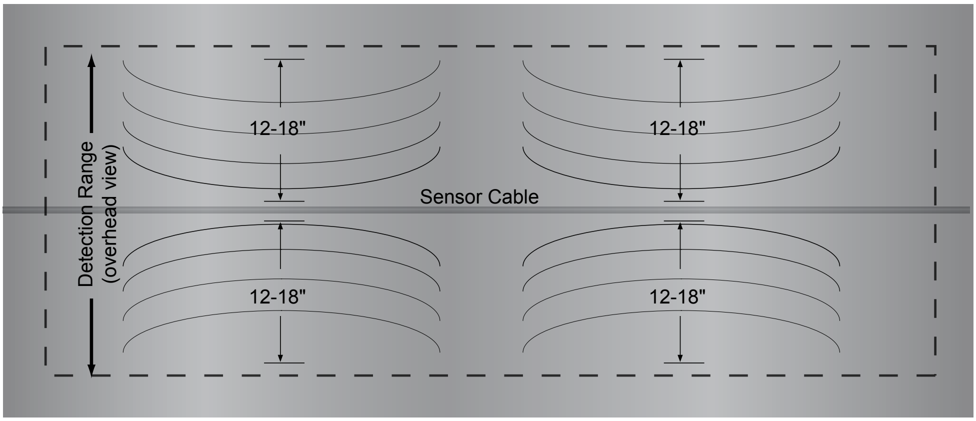
A buried sensor cable application is used to detect threats against an open, unfenced boundary or area. This includes areas unprotected by a fence across which an intruder may walk, run, crawl or attempt to tunnel under. With the buried application, the sensor cable is deployed in a serpentine pattern between 7 to 10 cm (3 to 4 inches) under a medium such as sod or gravel. An intruder walking across or moving into the area exerts bending and vibration that are then sensed by the cable, triggering an alarm state in the APU.

The best type of medium for buried applications is one that readily transmits vibrations from an intruder directly to the sensor cable. Generally, Fiber SenSys recommends using gravel for this reason. However, both sand and sod are acceptable mediums provided some fundamental buried application guidelines are followed.

NOTE:
The FD-348R sensor cable is not rated for burial in asphalt or concrete.

Under ideal circumstances (when the cable is buried in gravel) the sensor cable detects vibrations in a detection range up to 30-46 centimeters (12-18 inches) surrounding the cable. However, in a less fluid medium, such as sod, the detection range drops below 30 centimeters (12 inches) around the cable. This is because in less fluid mediums like sod, the sensor cable detects more bending than vibration.

Figure 3-13: Detection range around the buried sensor cable



The SC-4 sensor cable is designed for direct burial. It is not recommended to enclose the sensor cable in conduit for buried applications.

The following sections outline recommended buried cable deployment strategies for different medium types.

Gravel

When using gravel as the burial medium, the sensor cable should be laid atop a bed of gravel measuring at least 7 to 15 cm (3 to 6 inches) deep (F4igure 3-14). The cable should be deployed in a serpentine pattern, with the distance between loops measuring between 12-18 inches (the detection range in gravel is generally 12-18 inches).

NOTE:
Recall that the detection range surrounding the sensor cable in gravel is between 12 and 18 inches.

The gravel used should be smooth, round and approximately 2 cm (¾ inch) diameter or larger for best conduction of movement. The absence of sharp edges in round gravel also prevents damage to the sensor cable in the event the gravel is compacted.

All gravel should be clean of dust and sand to prevent absorption or dampening of vibration. Water should not be allowed to accumulate if the gravel is deployed in a region where temperature falls below the freezing level. This is because the formation of ice dampens vibration.

When creating a buried zone in gravel, a minimum of 4 passes (or 3 loops - see Figure 3-15) is recommended in order to create a zone wide enough that potential intruders cannot step or leap across it.

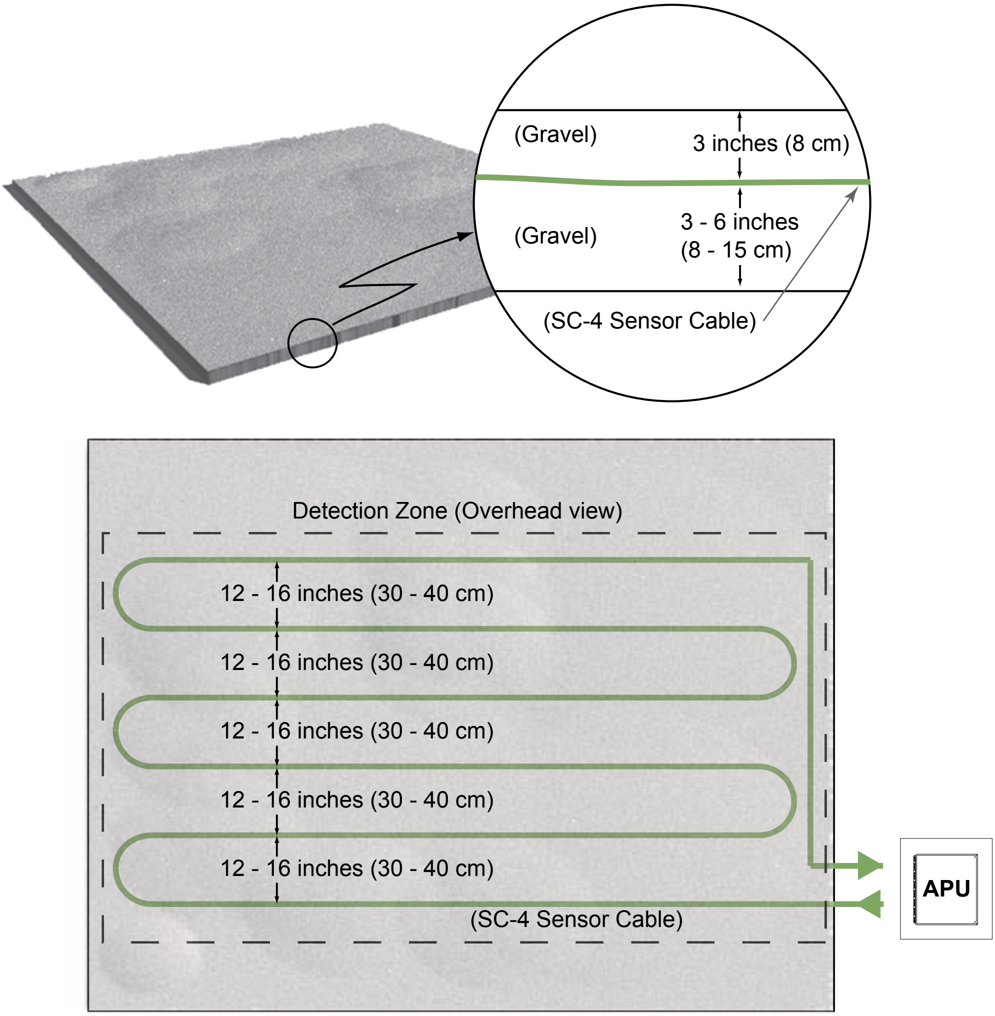


Figure 3-14: Sensor cable layout in gravel

Lawn or Sod

The cable should be placed far enough below the surface to avoid becoming entangled in the roots. This can be accomplished by pulling up the layer of sod and placing the cable directly underneath, or digging through the sod and covering the cable over with at least 5 - 8 cm (2 - 3 inches) of new sod. Once the cable is deployed, the sod must be kept reasonably moist in order to ensure vibrations are transmitted. Hardened sod will not likely transmit vibrations from an intruder.

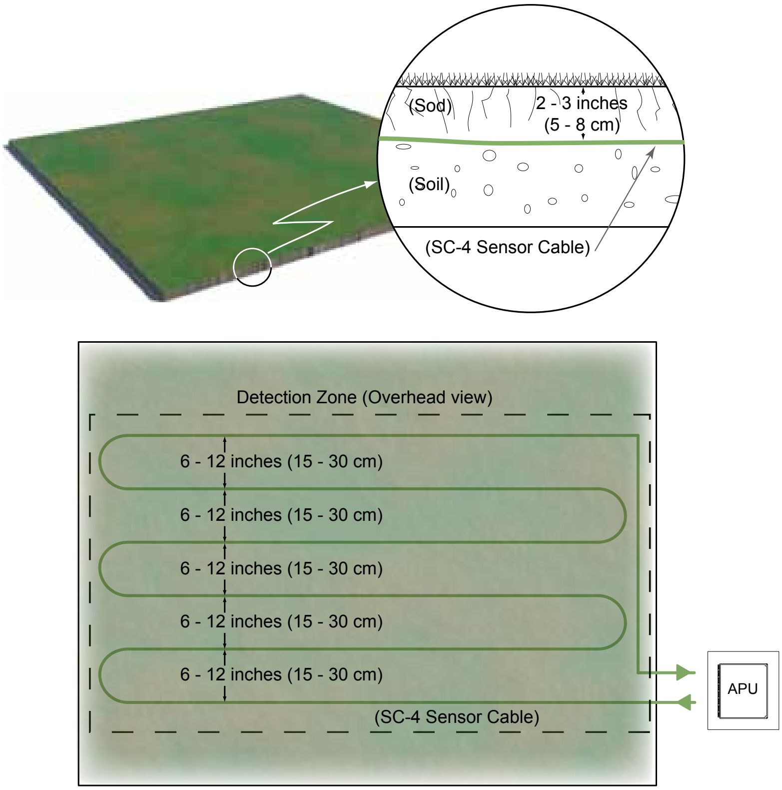


Figure 3-15: Sensor cable layout using sod

Laying the sensor cable in or on the clay beneath the sod is not recommended because the clay is generally too hard to transmit vibration. To avoid this, place a layer of sand directly under the cable to provide a cushion.

Sand

Because sand shifts with the weather, sensor cable buried in sand should first be attached to a layer of construction mesh with zip ties before being laid down and covered over with at least 10 cm (4 inches) of sand. This will ensure that the cable depth remains constant and sand-shifting remains minimal.

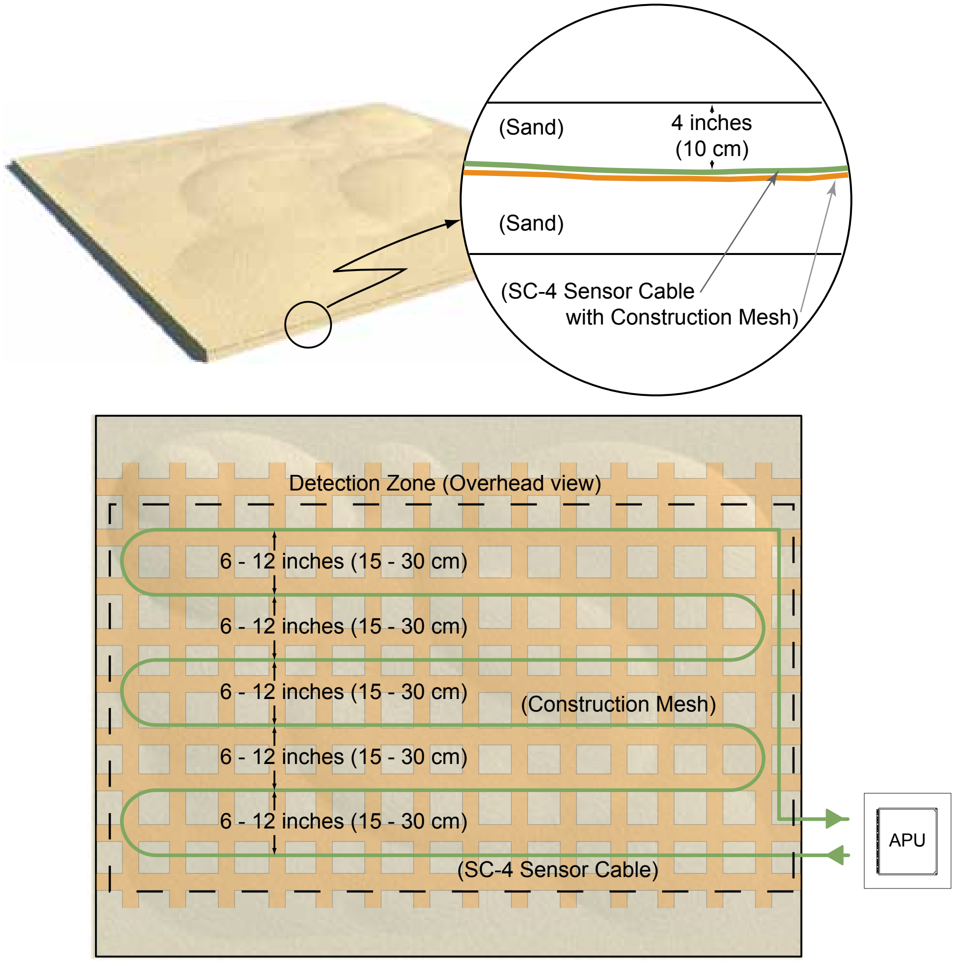


Figure 3-16: Buried installation using sand

If the buried cable is used to protect against tunneling, regardless of the medium it is used with, it should be used in combination with a layer of construction mesh and buried to the necessary level.

The SC-4 sensing cable cannot be used in solid mediums such as pavement.

Nuisances

As part of the assessment of an area, possible nuisances should be taken into account and adjusted for. *Nuisances* are non-threatening trespasses that could trigger an alarm. Small animals, the wind and tree limbs are all examples of nuisances that might cause an alarm. To avoid or significantly reduce the number of nuisance alarms, nuisance factors should be considered and steps taken to combat them. Such steps include trimming tree branches or shrubs back from the fence line, removing oversized signs on the fence fabric that could act as a "sail" when hit with a high wind and restricting the travel of guard dogs or small animals in the area.

Example Site Assessment

The following example illustrates the considerations to take into account when assessing a site.

A large, isolated area is to be protected using the FD-348R and a perimeter fence. Because the area is so large and spread out, the fence must be divided into multiple “zones” for monitoring purposes. Each zone will be monitored from centrally-located, rack-mounted FD-348R APUs in the guardhouse. A large natural rock formation in the back corner of the area forms a natural protective boundary. Behind it lies a small lake that touches up against the rock formation. A collection of trees sits to one corner of the site. In addition, a small hill of loose, sandy soil sits right at the perimeter of the site. Figure 3-17 shows the layout of the site.

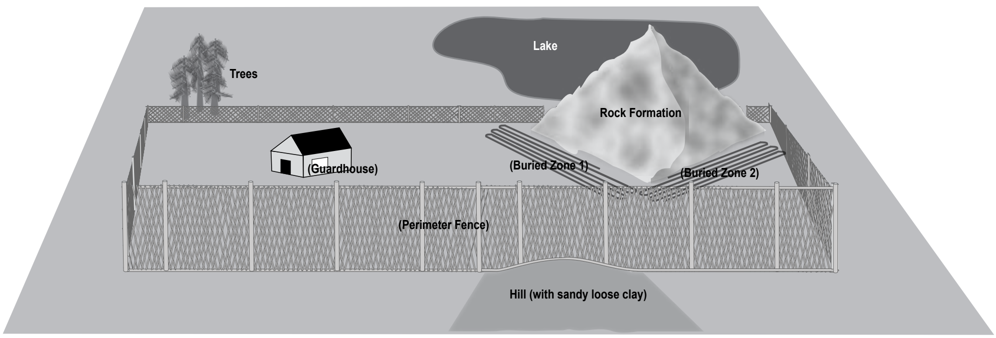


Figure 3-17: Site Example Drawing

Points to Consider

The fence. A chain link fence can form a satisfactory boundary around the protected site; however, steps must be taken to prevent digging under the fence, especially in areas where the ground soil is sandy and loose. One of the best protective measures to take is to embed a concrete “skirt” around the bottom of the fence all the way around the perimeter – making digging difficult – or burying a layer of fiber along the bottom of the fence. The loop-back deployment also protects against digging or tunneling under the fence.

The gate. A strategy must be created for ensuring the gate is protected. This strategy will depend greatly on the type of gate involved. For detailed information on protecting a gate, see *Protecting Gates* in Chapter 4.

The rock formation. While the rock formation provides the perfect natural barrier, it is conceivable for a climber to scale the rocks and drop down into the protected site, making a fence impractical for protection at the base of the formation. Instead, steps must be taken to ensure that intruders coming down from the rocks are detected. Separate protection zones can be created at the base of the rock formation using buried sensor cable and audible alarms or other indicators triggered off the APU's alarm relays. Loose gravel at the base of the rock formation makes it a suitable medium for the buried cable provided it is smooth and round in shape.

The lake. While the lake helps protect the rock against climbing, it is still possible for an intruder to swim or paddle across the lake and scale the rock formation. Therefore, the lake itself should be protected with either a fence or a buried cable around its perimeter. If a buried cable is used, it should be installed far enough away from the water's edge that the ground is not saturated with lake water (because the water will freeze in cold weather, making vibration detection difficult).

If a fence is deployed and sensor cable is added to it, a separate APU can be used to trigger a remote video camera and other protective devices.

The trees. Because the trees overhang the fence, they must be cut back and kept trimmed in order to prevent them from creating nuisance alarms.

The environment. Wind, weather and wildlife are all factors that can possibly create nuisance alarms. As one of the last steps in the installation process, each protected FD-348R "zone" should be calibrated and tested to ensure maximum sensitivity to intruder detection and immunity to nuisance alarms.

4

INSTALLATION

Fence Line Sensor Cable Installation

As mentioned previously, the sensor cable is used to detect threats against a fence line boundary such as climbing or fabric cutting. Under most circumstances, the sensor cable is deployed in the “loopback” configuration, with one strand of the loop running along the top and bottom half of the fence height. In many cases, the cable is also run along outriggers and fence posts for increased perimeter protection.

Ultimately, how the FD-348R is installed and deployed is up to the end user. Fiber SenSys does not recommend or mandate one particular installation setup over another. However, the general procedure for installing the FD-348R is:

1. Survey the site to be protected
2. Create a strategy for protecting the site. This includes planning the location of the APU, provision of electrical power and routing of sensor cable and insensitive leads
3. Determine the number of zones required
4. Create a strategy for protecting any gates in the site
5. Determine the amount of cable needed
6. Deploy the cable
7. Connect the sensor cable to the appropriate APUs

For detailed information on connecting the sensor cable to the APU, see *Alarm Processor Unit (APU) Installation* later in this chapter.

1. Surveying the Site to be Protected

As discussed in Chapter 3, the site to be protected should be surveyed thoroughly and a risk assessment performed, including accounting and compensating for prospective alarm sources. The strategy for deploying the cable is based on the results of the survey. For detailed information on site assessment, see Chapter 3.

2. Creating a Strategy for Protecting the Site

Chapter 3 contains detailed guidelines on developing a strategy for fence line sensor cable deployment. Refer to Chapter 3 for more information.

When developing the deployment strategy, also take note of and record:

- The length of the fenced perimeter (not including the gates)
- The number of gates and the length of each
- The number of reinforced sections and their lengths
- Distance from the fence to the APU
- The width of roadways or walkways through the gate(s)

Keep a detailed list of these factors and their associated numbers. They will be used to calculate the amount of cable required later on in the procedure.

3. Number of Required Zones

Protected sites requiring more than 5 kilometers (3.1 miles/16,400 feet) of sensor cable will require a multiple zone system. The number of zones required to protect a site is determined in part by the size of the site and the ability to respond quickly to one or more intruders.

Other factors determining the number of zones required can include whether or not video surveillance is used (requiring a separate zone for each camera), or whether there are one or more remote sections of the site that need to be monitored in addition to the main site.

4. Protecting Gates

Gates pose a unique problem to fence line sensor cable deployment because they are designed to move. While this does pose a challenge, sensor cable can still be deployed to protect a gate if the following points are kept in mind:

- Gates are sources of nuisance alarms during high wind conditions when they are allowed to swing on their hinges and bang into restraining posts, locking mechanisms or their own latches. Therefore, secure all gates against as much unintended movement as possible.
- Install and use an alarm disabling circuit whenever a gate equipped with sensor cable is opened or closed for authorized access.
- Establish a separate zone for any gate to maintain a secure perimeter while a gate is open. In addition, use care to reinforce sections of the fence leading to the gate(s) by adding additional structural support or posts. Separate the gate hinge post and fabric supporting posts as necessary. This is recommended to prevent or reduce vibrations transmitted from the gate to the sections of the fence with active sensor cable.

There are a number of ways to deploy the sensor cable to protect the gate. Some of the most common methods are discussed in the following sections.

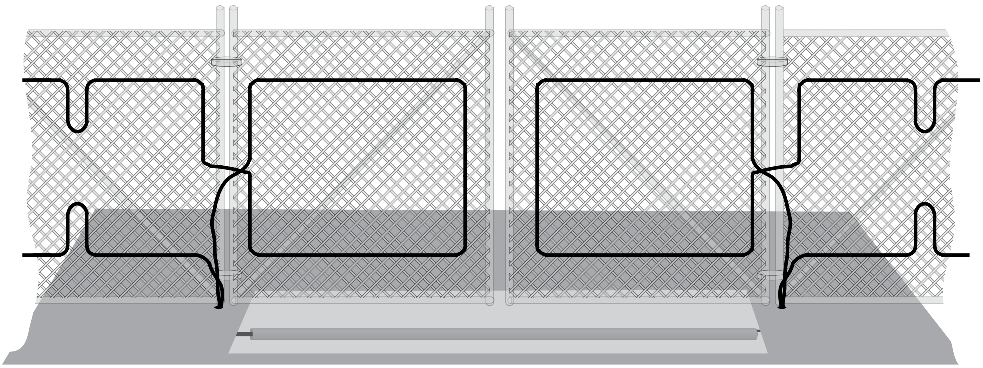


Figure 4-1: Sensor cable deployed on swinging gates

Single or Double Swinging Gates

For a swinging gate, the simplest method is to run the sensor cable from the fence fabric to the gate and loop it back. There is no danger in using the sensor cable as a hinge provided it is adequately shielded in EZ-300NSS or similar flexible conduit. The sensor cable is then routed below the gate and buried in hardened PVC conduit 0.3 meters (1 foot) below the roadway surface to make it insensitive to vibrations from the roadway.

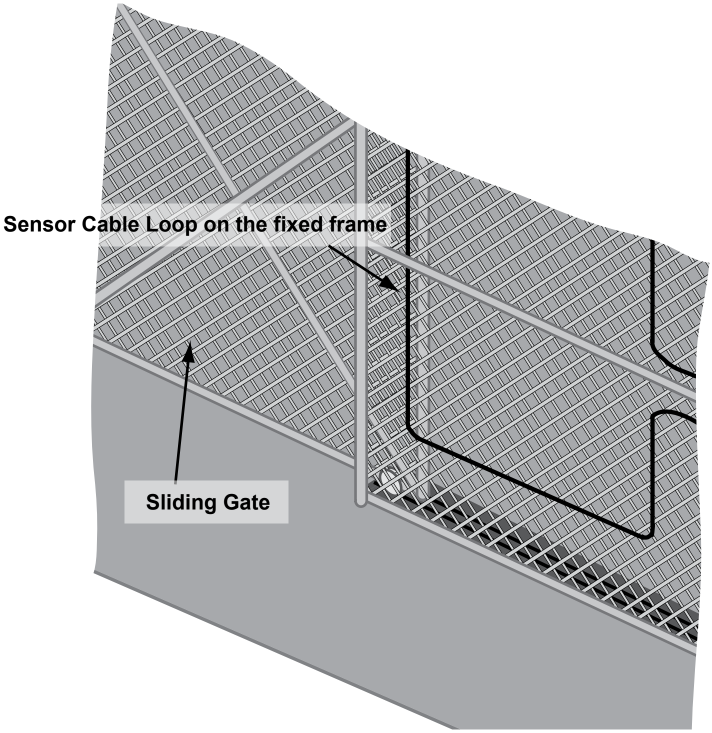


Figure 4-2: Sensor cable deployment on a sliding gate

Sliding Gates

Although sensor cable cannot be mounted practically on the sliding gate itself, it can be mounted on the support rail (Figure 4-2) to detect movement of the gate. The support rail conducts any disturbance from the gate to the sensor.

As with the swinging gate application, the sensor cable is routed below the gate and buried at least 0.3 meters (1 foot) below the roadway surface to make the cable insensitive to vibrations from the roadway before continuing on with the deployment.

In some instances where traffic from heavy vehicles is expected, the cable may need to be buried a full meter (3 feet) blow the surface.

Gates Not Requiring Protection

For gates that do not require protection, it is recommended that the cable be routed and buried 0.3 meters (1 foot) or more below the roadway in rigid PVC conduit (as shown in Figure 4-1). This creates a gate bypass that is insensitive to vibration from the roadway.

5. Determining the Amount of Cable Needed

In order to determine how much sensor cable is needed, the installer should know:

- The length of the fenced perimeter (not including the gates)
- The number of gates and the length of each
- The number of reinforced sections and their lengths
- Distance from the fence to the alarm processor
- The width of the roadways or walkways through the gate(s)

These numbers should have been generated in Step 2. The following sections illustrate how to use the numbers to determine the amount of cable needed.

Single Zone Site Example

Suppose that an area to be protected has a fence measuring 45 meters x 61 meters (147.6 feet x 200.1 feet) with a single swinging gate measuring 5 meters (16.4 feet) across. There are reinforced sections at each corner and next to the gate for a total of 10 sections, each measuring 3 meters (9.84 feet) across. An office where the RK-348 rack with one FD-348R APU module resides sits 6 meters (19.7 feet) back from the fence and 11 meters (36.1 feet) to one side from the gate (refer to Figure 4-3). For this example, the sensor cable will be deployed along the fence in a single pass (non loopback configuration)

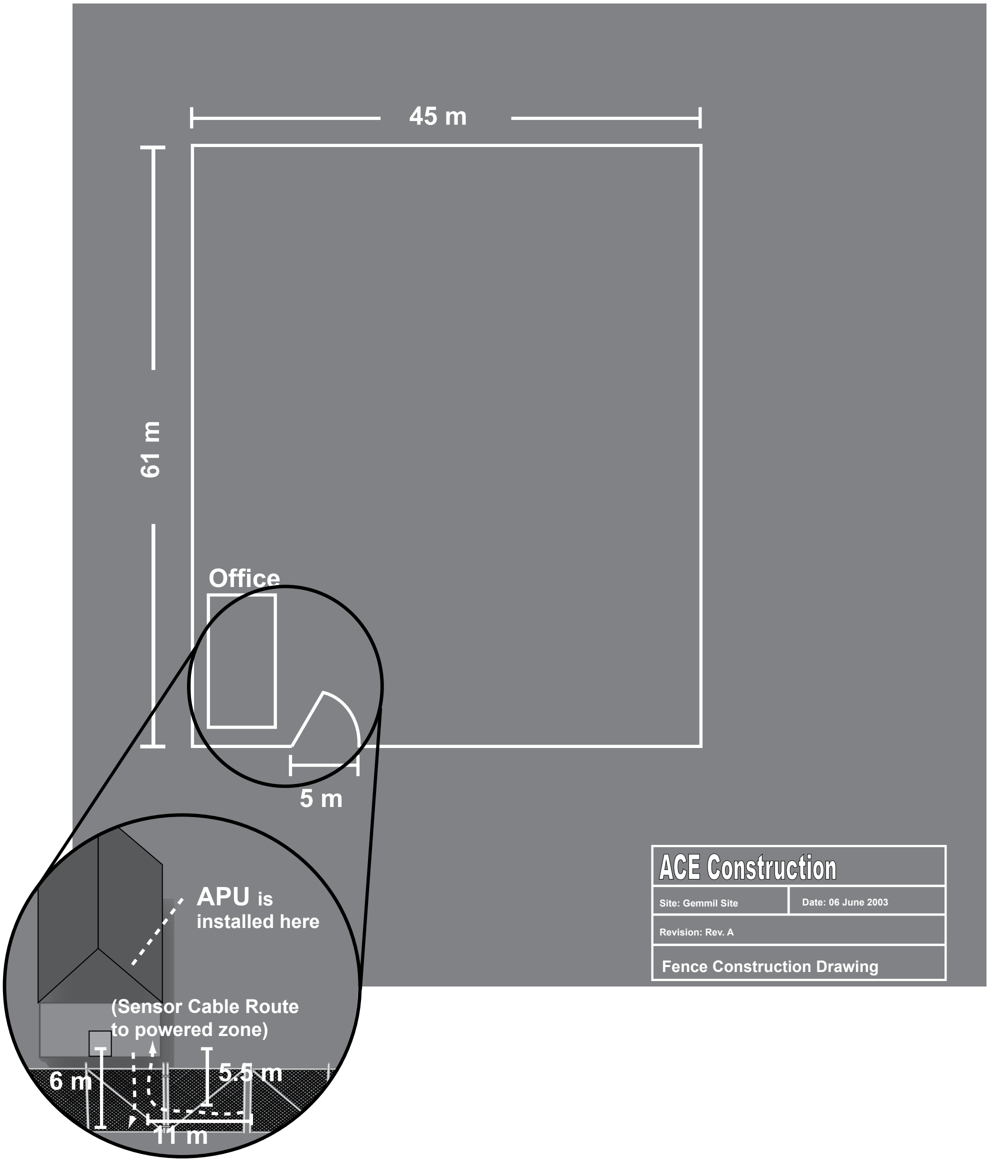


Figure 4-3: Single zone site drawing

To determine how much cable is needed:

1. Record the length of the fenced perimeter, not including the gate(s). In this example, the length is:

   [(45 m + 61 m) x 2] - 5 m = 207 meters or 679 feet

2. Calculate and record the length of cable required for the reinforced sections. Reinforced sections require 1.5 times the section length to account for extra sensor cable. This extra sensor cable is needed to create a small "loop" and increase the sensitivity at the local area. Multiply the length of each section by 1.5 and multiply the result by the number of sections:

   10 sections x 3 meters x 1.5 = 45 meters required

3. Record the amount of cable needed for the gates. This number is found by multiplying the length of each gate by 3.5 and adding the results together:

   5 meters x 3.5 = 17.5 meters required

   Three and a half times the normal amount of cable is required to allow sufficient length to create a loop on the gate fabric and leave enough to route the cable under the roadway – the most common method of protecting a gate. Use this method of calculation for all gate types, including swinging, sliding and unprotected gates.

4. Calculate and record the length of cable needed to connect the sensing cable from the fence to the APU. In this example, the installer chooses to run insensitive leads from the APU to the fence, around to the gate and back to the APU. Thus, a total of 22.5 meters of insensitive leads will be required:

   6 meters + 5.5 meters + 11 meters = 22.5 meters required

5. Calculate and record extra cable length to allow for service loops. To get this number, add 1.5 meters of cable for every 100 meters of perimeter fence. In our example, this would be:

   fence length divided by 100 x 1.5 m = 207 divided by 100 x 1.5 = 3.1

6. Add all recorded lengths together. This is the total amount of cable needed for a single pass of sensor cable. *This number is doubled for a loopback deployment.*

An example record depicting these numbers is shown in Figure 4-4.

Cable Site Survey Data

Length of Perimeter Fencing	207
Reinforced Sections	45
Gates	17.5
Cable Length to NEMA Enclosure	22.5
Extra Service Length	3.1
Total	295.1 meters (967.9 feet)

Figure 4-4: Single zone site example calculations

Multiple Zone Site Example

Figure 4-5 illustrates the site to be protected in this example.

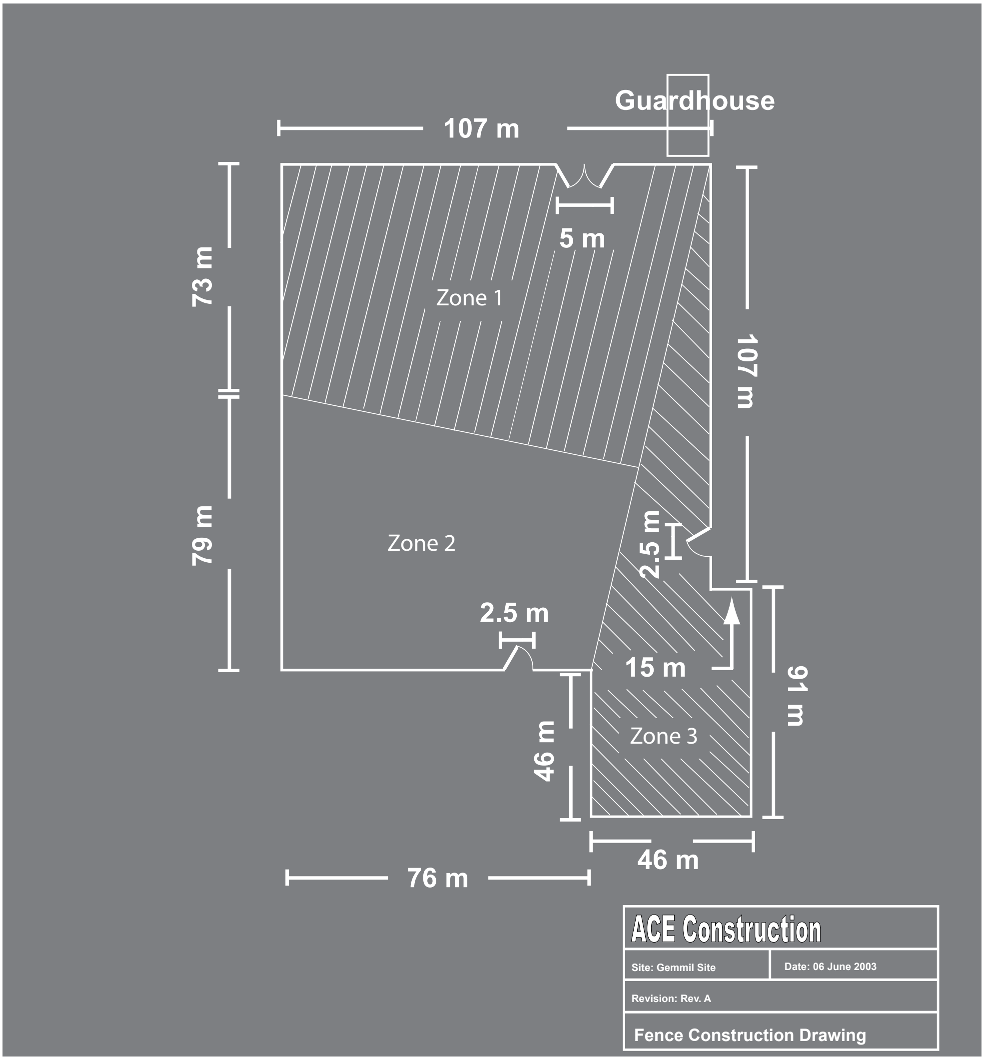


Figure 4-5: Multiple zone site drawing

Because the system will be linked to 3 surveillance video cameras monitoring 3 different zones, this is being set up as a multiple zone system. A single pass of sensor cable will be made (versus a loopback deployment) for this example. Insensitive leads will be routed back from the protected zones to three rack-mounted APU modules in the guardhouse. These insensitive leads will run from the sensor cable along the fence line back to the guardhouse as shown in Figure 4-6.

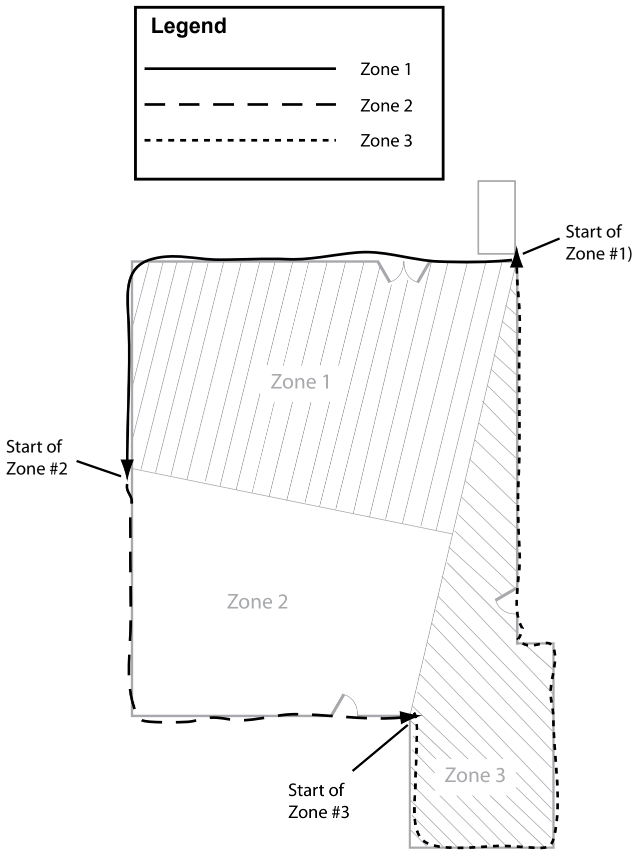


Figure 4-6: Sensor cable perimeter routing

Note that while the proximity of the guardhouse to the main gate preempts the need for the gate to be protected with sensor cable, the rule of multiplying the length of the gate by 3.5 still applies to ensure there is enough length to route the cable below the roadway. The length of the main gate is 5 meters (16.4 feet) while the length of the two personnel gates is 2.5 meters (8.2 feet).

There are reinforced sections on either side of each corner and gate. Each reinforced section is 3 meters (9.84 feet) in length.

Determining how much cable is required is done much the same way as it is for a single zone system. Cable requirements for the individual zones are added together for the total cable requirement. An example record depicting these numbers is shown below:

Cable Site Survey Data

	Zone 1	**Zone 2**	**Zone 3**
Length of Perimeter Fencing	175	152.5	287.5
Reinforced Sections	22.5	22.5	54
Gates	17.5	8.75	8.75
Extra Service Length	2.6	2.3	4.3
Cable Length to NEMA Enclosure	n/a	n/a	n/a
Subtotal	217.6	186.1	354.6
Total	758.3 meters (2487.2 feet) sensing cable		

Figure 4-7: Multiple zone site example calculations

The total length of sensor cable reported in Figure 4-7 is for this single pass setup. For a loopback configuration deployment, the number would double. In addition, the required amount of insensitive cable would be cut roughly in half.

For details on how to calculate the individual line items, see *Single Zone Site Example* on page 4-6 of this chapter.

In addition to knowing the length of cable required for ordering purposes, it’s important to know this number to know how much cable conduit is required. Fiber SenSys offers EZ-300SS split cable conduit or EZ-300NSS non-split cable conduit. Prior to deploying sensor cable in fence line applications, it is required that the cable be enclosed in the protective cable conduit. This rule of thumb applies to both sensor cable and insensitive leads.

6. Deploying the Cable

The FD-348R sensor cable can be deployed in any manner suitable to best protect a particular site. This section outlines the basic steps and provides some basic tips for preparing and deploying the sensor cable in a fence line application.

Fiber Handling Precautions

Optical fiber is fragile because it is made of glass. It will break if it is twisted or bent into too tight a radius. The following precautions should be kept in mind when handling fiber optic cable:

CAUTION
Failure to follow these precautions may result in damage to the fiber and degraded or poor system performance.

- The cable should not be pulled by the connectors. This could damage the connectors and result in degraded performance
- Avoid twisting the cable or bending it into a radius tighter than 5 cm (2 inches). This could damage the fiber or break it
- In order to keep the connectors free of dirt and dust, keep the connectors capped until you are ready to make a connection
- Connectors should be cleaned prior to making a connection. If dirt gets onto the tip of the connector, remove it using isopropyl alcohol and dust-free air or a clean, lint-free cloth

Inserting the Cable into Conduit

Prior to deploying the sensor cable, it must be inserted into conduit for protection.

NOTE:
The sensor cable must be pulled through the conduit before the conduit is attached to the fence.

SC-3 cable is not designed to be placed directly against the fabric of a fence. Conduit such as the Fiber SenSys EZ-300NSS conduit provides protection against intentional cutting, vandalism and extreme weather. It also provides uniform support of the sensor cable. Fiber SenSys recommends the following components and tools for inserting every 100 meters (328 feet) of sensor cable into protective conduit:

- 1 EZ-300NSS Non-Split Conduit Kit or 1 EZ-300SS Split Conduit Kit
- SC-3 Sensor Cable
- 1 EZ-350 Insertion Tool (not required for non-split conduit)

Each of these components is available from Fiber SenSys. One conduit kit includes 100 meters of flexible split or non-split conduit, 500 stainless steel wire ties and a conduit-to-box coupler. A conduit kit also contains either 4 expansion joints for connecting sections of split conduit together or 1 barrel coupler for connecting non-split conduit sections.

To insert the sensor cable into the conduit:

1. Begin by unrolling one or more of the required lengths of cable conduit. Place sections of conduit that must be connected together end-to-end
2. Connect the sections of conduit together as required. For detailed information on connecting sections of conduit together, see Appendix A

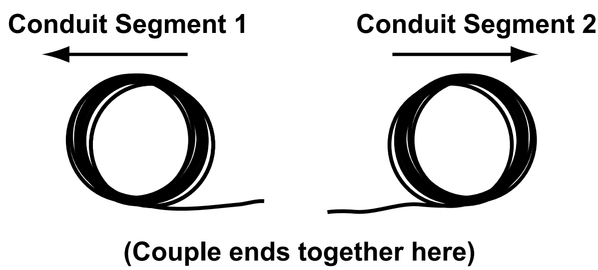


Figure 4-8: Coupling conduit

NOTE:
If you are using non-split conduit, use care to ensure the pull cord is not lost while performing this step.

3. Insert the cable into the conduit. For non-split conduit, this is done by tying the pull string to the cable at a point close to one end (if the fiber has already been terminated, do not tie the pull string to the connector itself) and pulling the cable through the conduit. For split conduit, an insertion tool must be used. An EZ-350 Insertion Tool (shown in Figure 4-9) is offered by Fiber SenSys for this purpose

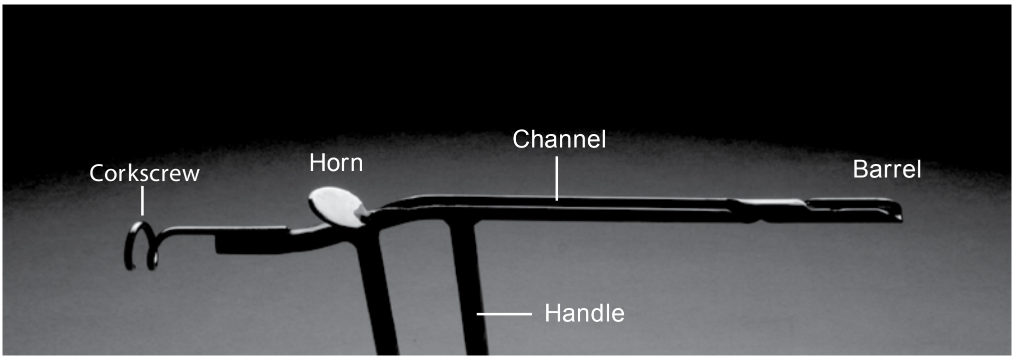


Figure 4-9: The EZ-350 insertion tool

To use the insertion tool, thread the sensor cable through the "corkscrew" at the front end and lay it into the channel along the top of the tool. Lay the end of the cable so that it points out the barrel. Insert the horn into the conduit and push the tool forward (with the corkscrew in front) through the entire length of conduit. The horn forces the split end apart and allows the insertion tool to advance, leaving the sensor cable trailing in the conduit behind.

NOTE:
Secure the trailing end of the cable to ensure it is not unintentionally pulled into the conduit and lost.

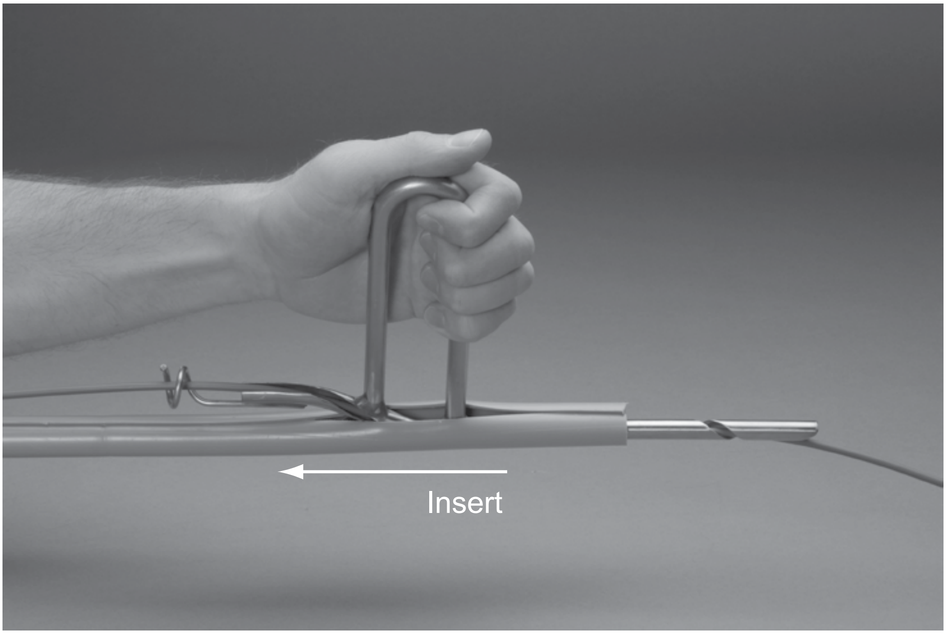


Figure 4-10: Inserting cable into conduit

It is recommended that at least two people be used to insert the sensor cable: one person to pull or insert the sensor cable and another to help feed it smoothly.

Terminating the Cable

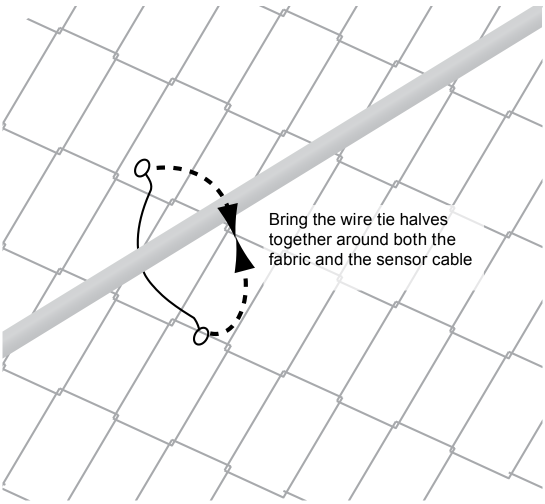
Whether or not a sensor cable is terminated before or after it is inserted into the conduit depends upon the preference of the installer. Either method is acceptable. The FD-348R APU uses industry-standard ST-type connectors; therefore, it is required that the insensitive leads and sensor cable also be outfitted with ST connectors. Connector kits are available from Fiber SenSys for connecting SC-3 and SC-4 sensor cables and IC-3 and IC-4 insensitive leads.

Detailed instructions are provided in each connector kit. Additional information on using ST-type connectors is found in Appendix B.

Attaching the Sensor Cable to the Fence

Where and how the cable is attached depends upon the type of fence and the possible threats against it. Generally, the sensor cable is attached in such a way that it detects vibration from intruders but remains insulated against nuisances as much as possible. In addition, the cable is also attached in a secure enough fashion to prevent granting intruders easy access to it. This is accomplished by following Fiber SenSys' recommended practices.

Once enclosed in conduit, the sensor cable/conduit assembly is attached to a fence using secure, non-corrosive wire ties. Stainless steel wire ties are available from Fiber SenSys. In the case of a chain link fence, for example, the sensor cable is attached to the fabric by threading the wire tie through the fence square and bending it back around the cable and mesh as shown in Figure 4-11.



A tool is then used to twist the tie so that the conduit/cable assembly is secure on the fence but isn't so tight it inhibits proper operation of the sensor or excessively compresses the conduit.

Figure 4-11: Attaching cable to the fabric

When attaching the sensor cable to chain link fence fabric, secure the cable to the fabric every 30 cm (12 inches or about 4 squares of most meshes). The sensor cable should be secured on the joint or intersection between links of the mesh in order to prevent movement of the cable and minimize any susceptibility to tampering (refer to Figure 4-12).

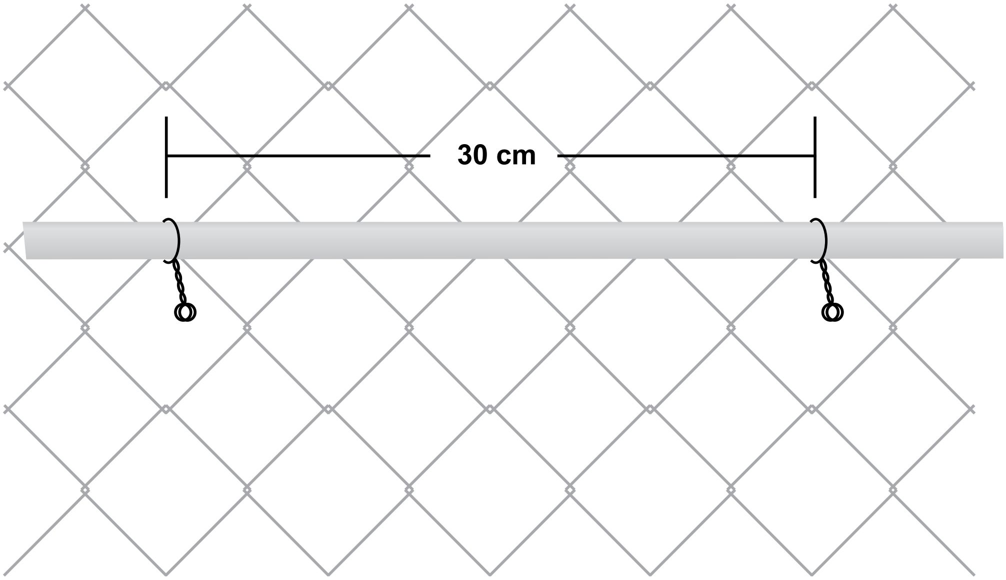


Figure 4-12: Wire tie placement

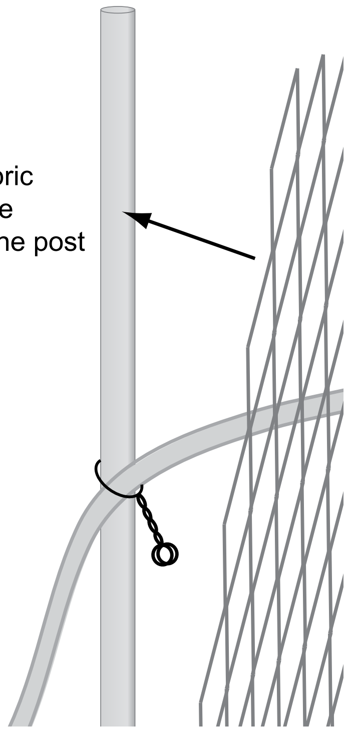


Figure 4-13: Cable placement

When bending the sensor cable to form loops, ensure the cable is not bent into a radius tighter than 5 cm (2 inches) to avoid damaging the optical fiber inside.

The sensor cable is also attached to wrought iron fences, barbed wire or razor wire using wire ties. In each case, it is necessary to consider how best to attach the cable so it is less likely to be disturbed by minor nuisances without sacrificing its receptivity to detect the movements or vibrations of an intruder. In the case of wrought iron fences, the cable is attached to either the top or bottom rail (or both) using wire ties every two vertical fence stakes or so.

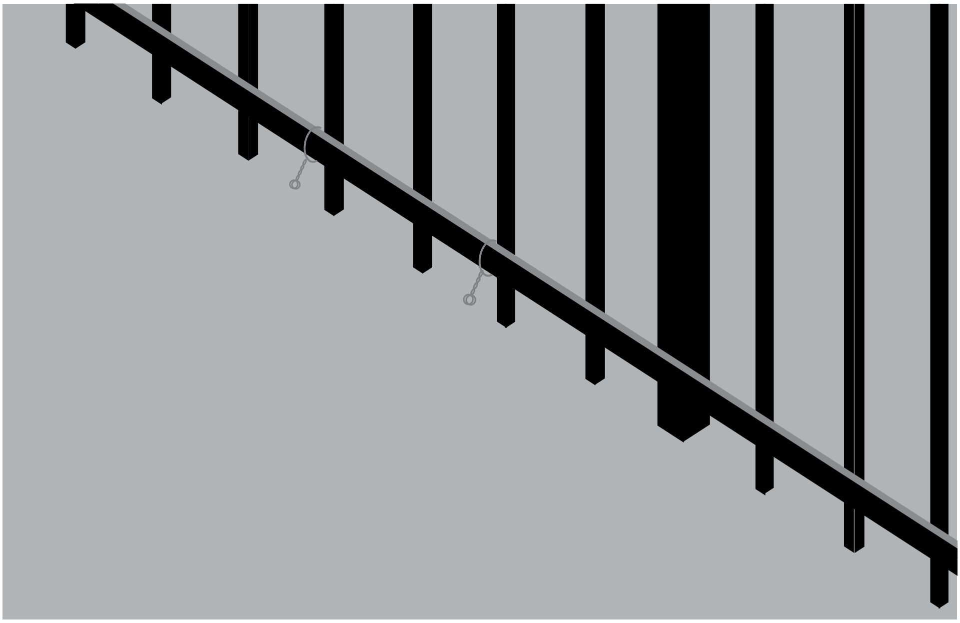


Figure 4-14: Attaching sensor cable to wrought iron fence

7. Connecting the Sensor Cable to the APU

Once the sensor cable has been deployed along the fence line, it must be connected to the APU. The sensor cable is connected via insensitive leads; therefore, how the insensitive leads are deployed depends ultimately upon where and how the APU is deployed in relation to the sensor cable.

NOTE:
The difference in the lengths of any two cables (length defined as the distance between any two end connectors) in the system should be greater than 1.5m. The length of any cable in the system must also be greater than 1.5m

The FD-348R APU uses industry-standard ST-type connectors; therefore it is required that the sensor cable and insensitive leads also be terminated with ST-type connectors throughout its length rather than mixing connector types.

Insensitive leads can be routed back to the APU either above or below ground.

While the insensitive leads are insensitive to vibration, it is necessary to protect the optical fiber by enclosing the leads in conduit. Because the leads are insensitive, they can be enclosed in either flexible or rigid conduit.

For detailed information on connecting to the APU, see *Alarm Processor Unit (APU) Installation* later in this chapter.

Buried Sensor Cable Installation

A buried sensor cable is used to detect threats against an open, unfenced boundary or area. This includes areas unprotected by a fence across which an intruder may walk, run, crawl or attempt to tunnel under. A sensor cable buried in the ground next to a protected fence can also create a secondary layer of detection.

With the buried application, the sensor cable is deployed between 7 to 10 cm (3 to 4 inches) under a medium such as sod or gravel. An intruder walking across the sensor cable exerts pressure that bends or vibrates the cable, triggering an alarm condition in the APU.

The general procedure for installing the FD-348R in a buried application is much the same as it is for a fence line application:

1. Survey the site to be protected
2. Create a strategy for protecting the site
3. Determine if the site will be a multiple zone or single zone system
4. Determine the amount of cable needed
5. Deploy the cable
6. Cover the cable
7. Connect the sensor cable to the appropriate APU

While the steps are largely the same as they are for a fence line application, there are some notable differences as detailed in the following sections.

Creating a Strategy for Protecting the Site

The strategy for deploying the cable depends on the medium being used (i.e. sod, sand, gravel, etc.).

NOTE:
Sensing cable should not be encased in conduit for most buried applications.

Chapter 3 lists guidelines for burying the cable under different mediums (see *Buried Cable Deployment Guidelines* in Chapter 3). To ensure a buried sensor cable successfully detects against intrusions into non-fenced perimeters, take the following additional considerations into account:

Medium for deployment. The sensor cable works best in buried applications when buried in gravel. Sod and sand are also acceptable mediums; however, items to consider when deciding upon a medium include determining its freezing point and the ability of the medium to conduct vibration. This is because a solid medium (such as frozen sod) conducts fewer vibrations than a fluid one (such as gravel). The depth at which the cable is buried is determined according to these factors.

Gravel is also the recommended medium in areas where burrowing animals are a concern.

Layout of the cable. The layout of the sensor cable depends upon the size of the area it is intended to protect. The best way to protect an open area is to lay the cable out in “loops” or “switchbacks.” The size of the area to be protected determines how much distance sits between each loop as well as how much cable is required.

Accumulation of rainwater. Accumulated rainwater freezes, damping vibration.

Accumulation of dust and dirt. Dust and dirt gathering over top of the medium ultimately dampen the transmission of vibration.

Determining the Amount of Cable Needed

In most cases, an area is best protected by laying the cable down in a serpentine pattern, forming "loops" with the sensor cable and leaving at least 30 cm (12 inches) of space between each one. Deployed under ideal circumstances, the sensor cable has a detection range between 30 and 46 cm (12 and 18 inches) around each pass of the cable.

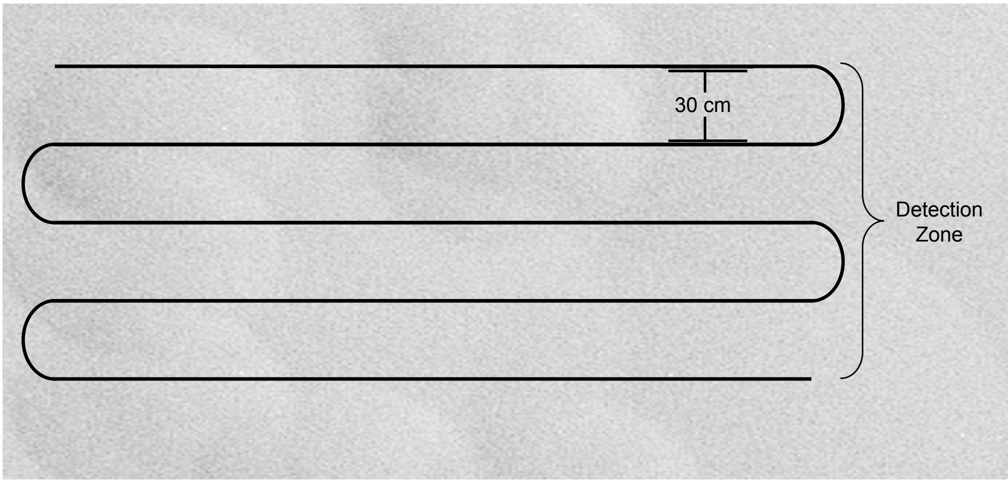


Figure 4-15: Sensor cable loop spacing

The distance between loops and the number of loops required varies with the type of medium used. Refer to *Buried Cable Deployment Guidelines* in Chapter 3 for more information on cable layout with each medium type.

The procedure for calculating the amount of cable required is different for a buried application. The differences are detailed in the following example.

Buried Application Site Example

Suppose a site measuring 300 meters (984 feet) by 250 meters (820 feet) needs to be protected by a buried cable. The medium in which the cable will be placed is sod. Because the cable will be buried in sod, the detection zone around the perimeter must be at least 2.1 meters (7 feet) in width (following the minimum recommended practice for sod outlined in Chapter 3 - see *Buried Cable Deployment Guidelines* for more information), requiring six passes of sensor cable (Figure 4-16). The area to be protected has a single gate measuring 5 meters (16.4 feet) across.

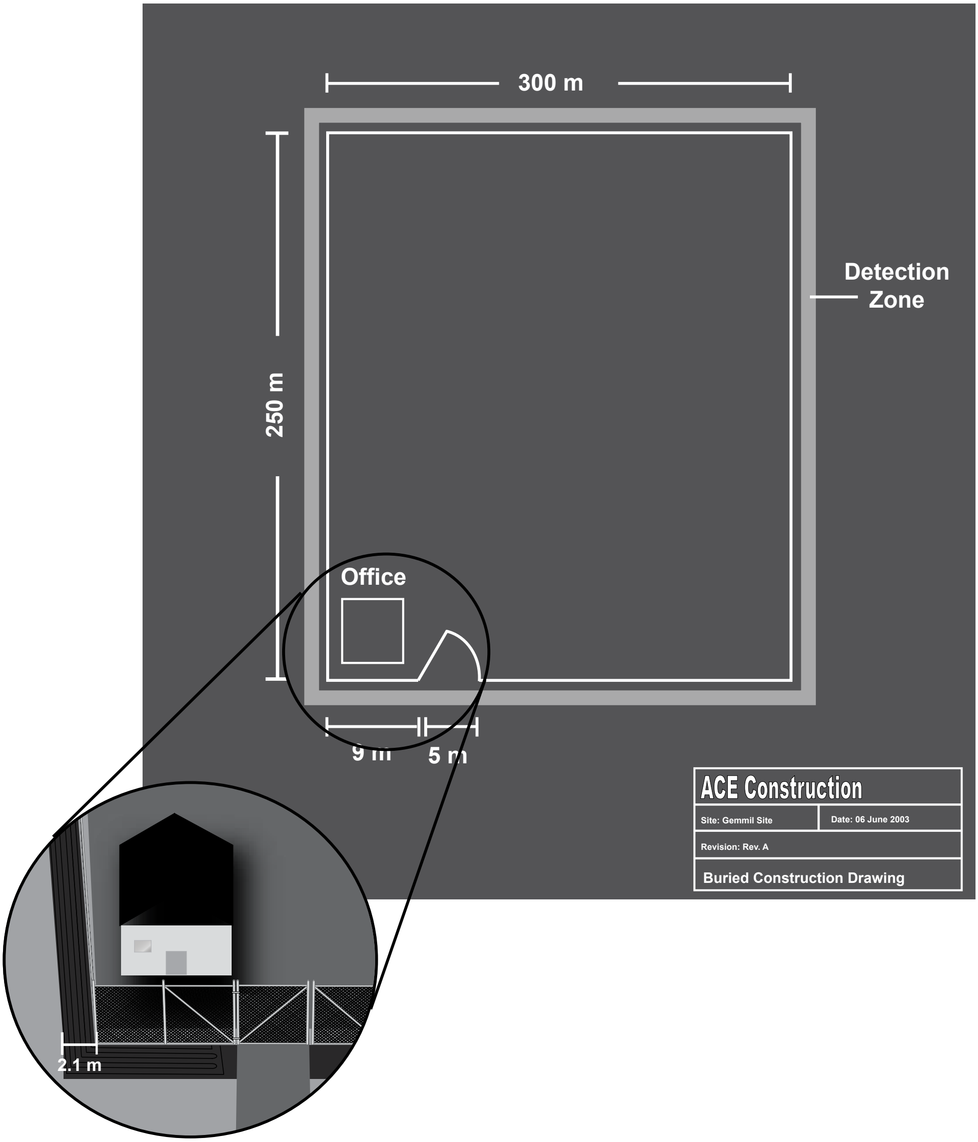


Figure 4-16: Buried application site drawing

To determine the amount of cable required:

1. Determine how many loops are required to form the desired detection zone. In this case, assuming the loops are spaced 30 cm (12 inches) apart, the 2.1 meter (7 foot) wide detection zone is formed with 6 passes
2. Multiply the number of required loops by the number of feet in the perimeter. Thus, the 1100 meter (3608 feet) perimeter in this example, multiplied by 6 loops, requires approximately 6600 meters (21,648 feet) of cable
3. Determine the number of zones required. As with a fence line application, since more than 5 kilometers (16,400 feet) of sensor cable is required (see *Number of Required Zones* on page 4-2 of this chapter), the site has to be broken up into at least 2 zones.
4. Determine the location and length of sensor cable required for each zone. For this example, an RK-348 with two rack-mounted FD-348R APU modules will be set up in the office. We can divide the site roughly in half as shown in Figure 4-17:

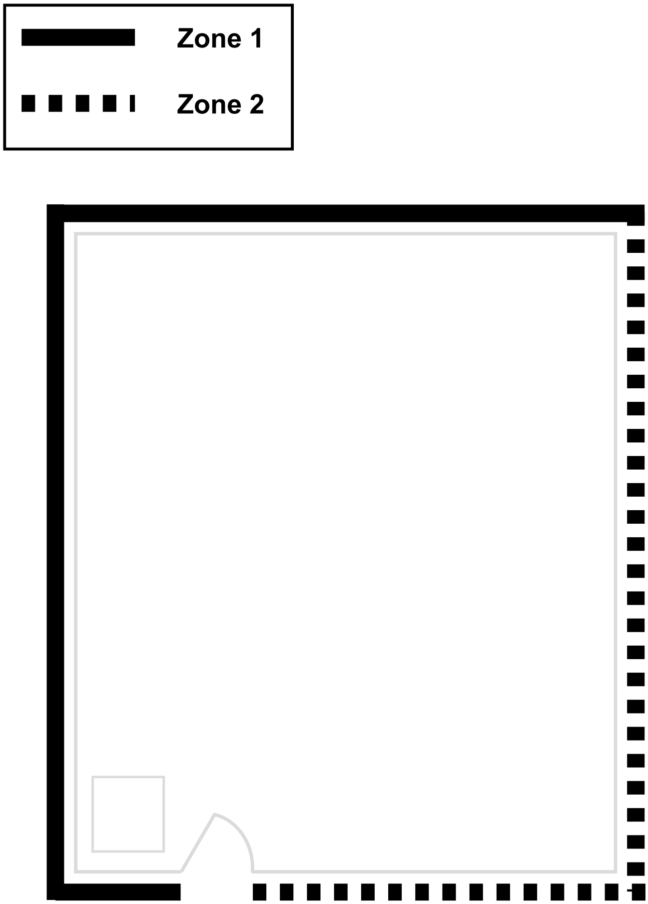


Figure 4-17: Buried application site drawing

5. Determine the length of sensor cable required for each zone. Using Figures 4-16 and 4-17, the length for each zone in this example is figured out by calculating the length of the perimeter by the number of passes. The calculations for determining the sensor cable length in each zone comes out as shown in the example worksheet in Figure 4-18

Cable Site Survey Data

Zone	Zone Length		Cable Length
1	(9 + 250 + 300) x 6	=	3354.0 m (11,001 ft)
			+ 50.3 m (for service)
			3404.3 m (11,166 ft)
2	(250 + 300 - 9 - 5) x 6	=	3216.0 m (10,548 ft)
			48.2 m (for service)
			+ 17.5 m (gate bypass)
			3281.7 m (10,763 ft)

Figure 4-18: Site example calculations

6. The length of the insensitive leads must also be calculated. Based upon Figures 4-16 and 4-17, the total length of insensitive lead-in cable required for Zone 1 is 10 meters (2 leads are required for each zone). For Zone 2, the requirement is 20 meters.

Deploying the Cable

The FD-348R sensor cable can be deployed in any manner suitable to best protect a particular site. This section outlines the basic steps and provides some basic tips for preparing and deploying the sensor cable in a buried application.

Fiber Handling Precautions

Optical fiber is sensitive because it is made of glass. It will break if it is twisted or bent into too tight a radius. The following precaution should be kept in mind when handling optical fiber cable:

CAUTION
Failure to follow these precautions may result in damage to the fiber and degraded or poor system performance.

- The cable should not be pulled by the connectors. This may damage the connectors and result in degraded performance
- Avoid twisting the cable or bending it into a radius tighter than 5 cm (2 inches). This may damage the fiber or break it
- Keep the connectors capped until a connection is made in order to keep them free of dirt
- Connectors should be cleaned prior to making a connection. If dirt gets onto the tip of the connector, it can be removed using isopropyl alcohol and dust-free air or a clean, lint-free cloth

Laying Down the Cable

For nuried applications, the sensor cable is not enclosed in flexible or rigid conduit prior to deployment. The SC-4 cable is left bare in order to maximize its vibration-detecting ability.

Lay the cable down in accordance with the deployment strategy developed for the site along with the guidelines discussed previously in Chapter 3 (see *Buried Cable Deployment Guidelines*). Lay the fiber down in “loops” with at least 30 cm (12 inches) of space between each loop. Take extra care to ensure the sensor cable is not bent at an angle with a radius of less than 5 cm (2 inches).

Terminating the Cable

Whether or not a sensor cable is terminated before or after it is laid down depends upon the preference of the installer. Either method is acceptable. The FD-348R APU uses industry-standard ST-type connectors; therefore, it is required that the sensor cable be outfitted with ST connectors. Crimp-on type connector kits are available from Fiber SenSys for connecting SC-3 and SC-4 sensor cable and IC-3 or IC-4 insensitive lead-in cable.

Detailed instructions are provided in each connector kit. In addition, general instructions for terminating the fiber with ST-type connectors can be found in Appendix B.

Covering the Cable

Sand or gravel must be deposited over the sensor cable in a layer at least 7 cm (3 inches) thick for optimal sensor performance. Gravel used should be clean, round in shape and ideally be at least 2 cm (¾ inches) in diameter for best performance.

A layer of sod can be put down in place over the cable but the sensor cable must be down far enough that the roots of the sod do not interfere with it. As mentioned in Chapter 3, the sensor cable should not be buried in or laid atop hard clay. See *Buried Cable Deployment Guidelines* in Chapter 3 for more information.

Alarm Processor Unit (APU) Installation

CAUTION
Use of controls or adjustments or performance of procedures other than those described herein may result in hazardous radiation exposure.

Once the sensor cable has been deployed, the APU must be installed and connected to it. When using the FD-348R, the method of connection is through the RK-348.

Using the RK-348

The 19 inch rack-mount chassis (RK-348) can hold up to 8 APU modules. The chassis has its own power supply and accepts 110 or 240 VAC, 50 or 60 Hz input power. The chassis also supplies the necessary 12-24 VDC to each installed APU module. Prior to plugging in the rack assembly, the proper input voltage range must be selected. For more information, see *Setting the Input Voltage Range* on page 4-36.

Warning!
A protective ground connection by way of the power cord is essential for safe operation. If the ground connection is lost, or if the plug is not plugged into a proper receptacle, all conductive parts of the instrument can render an electric shock.

To set up the rack-mounted APU assembly for operation:

1. Set the rack-mount chassis power supply for the correct input voltage. See *Setting the Input Voltage Range* following this section.
2. When installing APU modules into the rack begin by plugging each APU module into an open channel on the chassis. This is done by sliding each APU module card carefully into position using the ECB guides at the top and bottom of each channel. Press on each module's face firmly until the connector in back locks into place. Secure the module in the rack-mount chassis using the two 4-40 captive screws on the face.
3. Connect the optical cables (sensor cable or insensitive leads – See *Rack-Mounted APU Module Connections and Indicators* in Chapter 2 for connection details). All optical cables should be routed through the strain reliefs found on the back of the rack-mount chassis to prevent stress at either the input or output optical connectors. Ensure there are no bends in the cable tighter than 5 cm (2 inches).
4. If you are using the Fiber Security Network (FSN) communication mode, connect the optical cables to/from the appropriate hardware (usually the FCA-284 and FCA-285). The light gray connector is for connecting data output to the network. The dark gray connector is for connecting data input from the network.
5. Connect the alarm and fault relay contacts. See *Rack-Mounted APU Module Connections and Indicators* in Chapter 2 for connection details.

Setting the Input Voltage Range

Prior to connecting AC power, the rack-mount chassis must be configured for the proper voltage. This is done by changing the orientation of the fuse module in the back of the power supply.

Warning!
The proper input voltage range must be set prior to connecting electrical power. Failure to do so may result in damage to the instrument.

To set the input voltage range:

1. Locate the power entry module on the back, left-hand side of the rack-mount chassis
2. Insert a flat-bladed screwdriver into the opening at the top of the fuse module (refer to Figure 4-19) and gently pry the fuse module out. Remove the fuse module
3. Install two [2] 250 V, 1 Amp fuses in the fuse module as shown (Figure 4-21)
4. Re-insert the fuse module so that the proper voltage range on the label is reading right-side up. The arrow next to the desired voltage range (on the label) should be pointing at the arrow on the power entry module when installed correctly

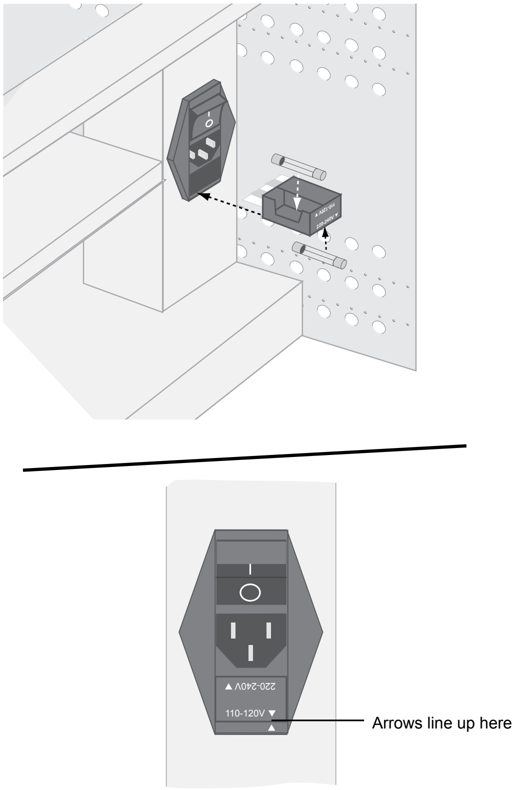


Figure 4-19: Fuse Module Location

Adding Supervisory Resistors

Adding a **series resistor** to the normally-closed alarm relay contacts ensures a closed contact condition cannot be simulated by shorting the external alarm relay contact leads, preventing an alarm. A series resistance value of 2.74 kilohms is recommended.

Adding a **parallel resistor** to the normally-open alarm relay contacts ensures an open contact condition cannot be simulated by cutting the external alarm relay contact leads, preventing an alarm. A parallel resistance value of 2.74 kilohms is recommended.

The sockets for installing the supervisory resistors can be found on the circuit board near the RS232 connector and are labeled "Supervisory Resistors". Figure 4-20 below illustrates the normally-open and normally-closed supervisory resistor sockets that are present on the FD-348R. By default there is a jumper in the "NC" socket,

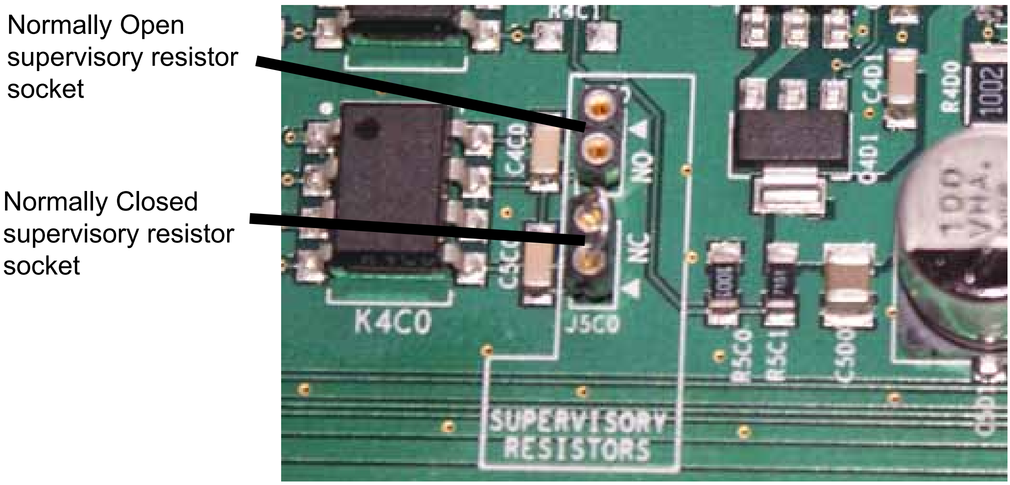


Fig 4-20: Sockets for supervisory resistors on the FD-348R

With the FD-348R properly installed, it is now ready for calibration.

5

SYSTEM CALIBRATION

Overview

Calibration of the FD-348R is a crucial component of its success in detecting the presence of an intruder. A properly calibrated system will not only detect threats from an intruder, but will ignore most or all nuisances as well. This chapter provides detailed information on the parameters to be calibrated as well as possible settings for each.

System calibration should always follow physical installation of the FD-348R hardware and should precede any attempt to use the system. Each Alarm Processing Unit (APU) must be calibrated and its associated zone must be tested separately. Calibration of the APU can be performed using the Hyperion Hand-held Calibrator or a PC with terminal emulation software such as HyperTerminal® or Fiber SenSys' SpectraView®.

Hyperion Hand-held Calibrator

The Hyperion Hand-held Calibrator is a portable calibration tool designed for outdoor use in all-weather environments. Basically, it is a calibration software package installed on a rugged, MIL-STD-rated pocket PC. Touch screen controls plus an included soft plastic stylus make the Hyperion unit easy to operate. Communication between the APU and Hyperion takes place through an RS-232 serial cable. The Hyperion, and additional detailed documentation about operating the hand-held calibration unit, is available from Fiber SenSys.

Figure 5-1: The Hyperion Hand held Calibrator

To connect the Hyperion:

1. Connect the RS-232 cable to the pocket PC’s RS-232 serial port and then to the RS-232 interface of the APU

2. Connect power to the APU and verify the green “**Power**” LED illuminates

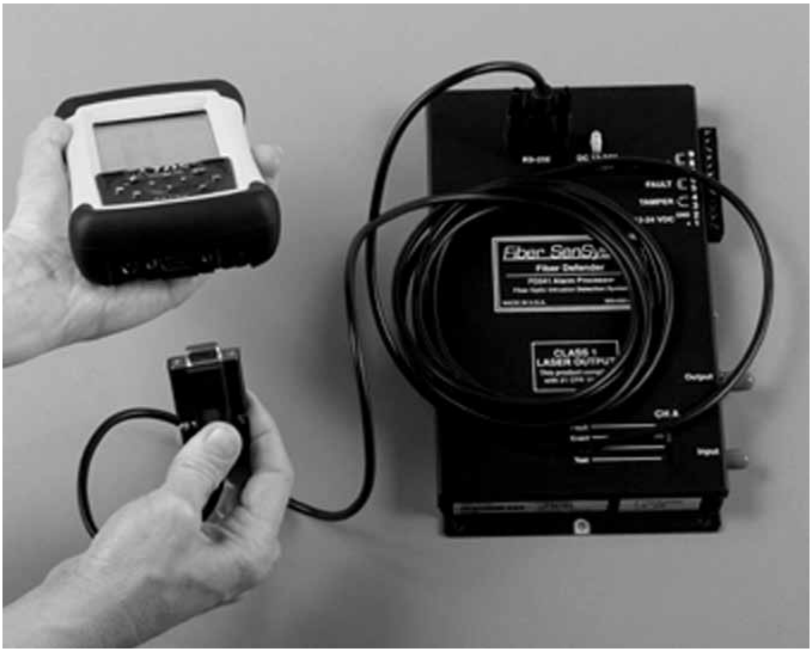


Figure 5-2: Connecting the Hyperion to the APU

3. Turn the Hyperion's pocket PC on by pressing the power button. If the calibration software is not accessed immediately from this point, simply press the Hyperion hotkey to proceed. Operation of the unit is conducted with Windows Mobile® software platform

Connecting With a PC

Any PC with terminal emulation software (such as SpectraView® or HyperTerminal®) can be used to interface with an APU. This includes laptop portable PCs. To use the PC, connect a 9-pin RS-232 cable between the PC serial port and the RS-232 connector of the APU. Launch the terminal emulation software and establish communication between the two instruments. Although the emulation software can vary greatly from one PC to the next, the following general guidelines are recommended for SpectraView® or HyperTerminal® (for Windows 95® or newer Windows-based software).

1. Connect the PC to the RS-232 port of the APU

NOTE:
A PC with a straight-through, 9-pin RS-232 port or a straight-through, 25-pin port with a 25-to-9 pin converter must be used for the procedure.

2. From the desktop, click on the **Start** button and select **Programs >> Accessories >> Communications >> HyperTerminal** to launch the HyperTerminal software

3. When the Connection Description window comes up, enter "Fiber SenSys" (or other connection name) in the Name box

4. When the Connect To window comes up, select "Direct to Com1" (or appropriate port) from the Connect Using drop-down list. Click on the **OK** button. The COM1 Properties box appears

5. Set the following properties using the drop-down lists:

   Bits per Second: 9600
   Data bits: 8
   Parity: None
   Stop bits: 1
   Flow control: Hardware

   Press the **OK** button

6. When the Hyper Terminal window comes up, press the **Enter** key. This brings up the system's password prompt, which reads:

   "Unit is LOCKED, Enter Password"

7. Hit the caps lock. All instructions must be entered in capital letters

8. The system is now ready for operation

NOTE:
SpectraView® or SpectraView® LT is a software package designed to monitor APU performance, as well as analyze recorded sensor signals. The GUI program is designed to work in conjuntion with a remote PC. Operating details are available through Fiber SenSys' SpectraView® User's Manual.

Programmable Calibration Parameters

This section provides details for all programmable FD-348R system calibration parameters. Each FD-348R is calibrated independent of the other APUs in the RK-348.

Upon establishing communication with the APU, the system displays the password prompt:

"Unit is LOCKED, Enter Password"

There are 5 user-definable "passwords" that provide the user with access to related APU parameters or submenus. For instance, the "GAIN" password provides users with access to the gain setting. After entering the password, "GAIN," users can make adjustments to the setting as desired. The defaults for these 5 parameter passwords are:

- Gain
- Setup
- Hist
- Status
- Version

A sixth password ("DIR") is for factory use only and is not covered by this manual.

NOTE:
The GAIN and SETUP passwords can be customized by the user.

Each password, and its associated calibration parameters, is explained in detail in the following pages. Factory default settings for fence line settings were chosen based upon the performance of an FD-348R used in tandem with a seven foot chain link fence having a three-strand barbed wire outrigger. Default settings for buried or non-fence line settings were chosen based upon the performance of an FD-348R in a buried application, with gravel used as the burial medium.

NOTE:
Press the **Enter** *key at any time to exit from any menu, submenu or parameter in the terminal emulation software.*

Gain

The "GAIN" password allows access to the gain setting of the APU. The default setting is **20** and the range is **1** to **50**. The gain setting adjusts the sensitivity of the system to events, with higher settings meaning a higher sensitivity. For example, a gain setting of 30 is more likely to register an event than a gain setting of 10. For systems installed in areas where nuisance alarms are likely (from wind, etc.), a lower gain setting is recommended.

Setup

Access this menu using the “SETUP” password. There are 4 submenus available.

- Wind [1]
- Comment [2]
- Date [3]
- Calibrate [4]

These submenus are accessed by entering their corresponding submenu numbers (“1” for the Wind submenu, “2” for the Comment submenu, etc.).

Wind [1]

This submenu allows the enabling and scaling of the internal wind rejection algorithms. When enabled this function helps your FD-348R APU cope with environmental disturbances caused by wind.

The adjustable parameters for wind rejection are as follows:

Parameter	Range	Default	Description
Enable Wind Rejection Software	Y / N	Y	Enables the wind rejection software. When enabled, the APU continually monitors the effects of wind on the cable and compensates for it based upon the detected load and the wind rejection value

Parameter	Range	Default	Description
Wind Rejection	20 - 80	50	A selectable parameter that determines how much the APU will dampen the signal received from the sensor cable during windy conditions. A higher wind rejection factor means more dampening, requiring a signal higher in magnitude to create an alarm condition

Comment [2]

This submenu allows users to enter comments of up to 15 characters maximum. Comment text is stored in the APU and is displayed each time this submenu is accessed until / unless the text is changed.

Date [3]

From this submenu, users can enter the date of the last calibration (15 characters maximum) or change the time and date setting of the APU's real-time clock.

Real Time Clock [1]

Select option [1] and enter the new time in 24 hour format followed by the current date in the format mm/dd/yy.

Calibration Date [2]

Select option [2] to change the calibration date.

Calibrate [4]

The calibrate submenu gives the user access to parameters affecting 5 areas:

- Processor 1 [1]
- Processor 2 [2]
- Details [3]
- Passwords [4]
- Reset [RS]

NOTE:
The default value for most parameters described in this section changes depending upon whether the user sets the APU for fence line or buried (other) applications.

Processor 1 [1]

Parameter	Range	Default	Description
Enable	Y / N	Y (Fence) Y (Buried)	Enables the processor

Parameter	Range	Default	Description
Level of Signal	1 to 40 (dB)	10 (Fence) 10 (Buried)	Sets the level above which the signal from a sensor cable must meet or exceed before an event is generated by the processor

Parameter	Range	Default	Description
Lowest Frequency	10 to 600 (Hz)	200 (Fence) 10 (Buried)	The lowest allowable frequency used by the processor to evaluate the presence of an intruder. This may be used to eliminate alarms caused by low-frequency signals from vibrations of nearby structures or roadways.

Parameter	Range	Default	Description
Highest Frequency	10 to 600 (Hz)	600 (Fence) 120 (Buried)	The highest allowable frequency used by the processor to evaluate the presence of an intruder. This may be set to eliminate nuisance alarms caused by high-frequency signals from the fence fabric rattling in the wind, etc

Parameter	Range	Default	Description
Duration of Signal	1 to 25 (sec / 10)	3 (Fence) 3 (Buried)	Time interval during which any signal above the *Level of Signal* setting must remain to qualify as an event

Processor 1 (continued)

Parameter	Range	Default	Description
Low Level Tolerance	1 to 10 (dB)	5 (Fence) 5 (Buried)	An allowance that permits a signal lower than the *Level of Signal* setting to generate an event as long as it lasts for the period of time automatically set by the processor. The higher the tolerance, the longer the signal must last. If the signal is outside the tolerance setting, it cannot generate an event regardless of how long it lasts

Parameter	Range	Default	Description
Event Count	1 to 100	3 (Fence) 2 (Buried)	The number of times that an event must be registered for an alarm condition to occur

Parameter	Range	Default	Description
Event Window	1 to 200 (sec / 10)	50 (Fence) 90 (Buried)	Length of time after an event occurs during which another event must be registered for it to count toward an alarm condition. See *Event Count* above

Parameter	Range	Default	Description
Event Mask Time	0 to 100 (sec / 10)	2 (Fence) 0 (Buried)	A period of time after an event during which the sensor signal is ignored. This setting is useful for setting the system to mask or ignore the effects of oscillations from a single event, such as a bird striking a fence. Oscillations from such nuisances usually die down within 0.5 seconds

Processor 2 [2]

NOTE:
The default value for most parameters described in this section changes depending upon whether the user sets the APU for fence line or buried (other) applications.

Parameter	Range	Default	Description
Enable	Y / N	Y (Fence) N (Buried)	Enables the processor

Parameter	Range	Default	Description
Level of Signal	1 to 40 (dB)	10 (Fence) N/A (Buried)	Sets the level above which the signal from a sensor cable must meet or exceed before an event is generated by the processor

Parameter	Range	Default	Description
Lowest Frequency	10 to 600 (Hz)	300 (Fence) N/A (Buried)	The lowest allowable frequency used by the processor to evaluate the presence of an intruder. This may be used to eliminate alarms caused by low-frequency signals from vibrations of nearby structures or roadways.

Parameter	Range	Default	Description
Highest Frequency	10 to 600 (Hz)	600 (Fence) N/A (Buried)	The highest allowable frequency used by the processor to evaluate the presence of an intruder. This may be set to eliminate nuisance alarms caused by high-frequency signals from the fence fabric rattling in the wind, etc

Parameter	Range	Default	Description
Duration of Signal	1 to 25 (sec / 10)	1 (Fence) N/A (Buried)	Time interval during which any signal above the *Level of Signal* setting must remain to qualify as an event

Processor 2 (continued)

Parameter	Range	Default	Description
Low Level Tolerance	1 to 40 (dB)	3 (Fence) N/A (Buried)	An allowance that permits a signal lower than the *Level of Signal* setting to generate an event as long as it lasts for the period of time automatically set by the processor. The higher the tolerance, the longer the signal must last. If the signal is outside the tolerance setting, it cannot generate an event regardless of how long it lasts

Parameter	Range	Default	Description
Event Count	1 to 100	2 (Fence) N/A (Buried)	The number of times that an event must be registered for an alarm condition to result

Parameter	Range	Default	Description
Event Window	1 to 200 (sec / 10)	80 (Fence) N/A (Buried)	Length of time after an event occurs during which another event must be registered for it to count toward an alarm condition. See *Event Count* above

Parameter	Range	Default	Description
Event Mask Time	0 to 100 (sec / 10)	7 (Fence) N/A (Buried)	A period of time after an event during which the sensor signal is ignored. This setting is useful for setting the system to mask or ignore the effects of oscillations from a single event, such as a bird striking a fence. Oscillations from such nuisances usually die down within 0.5 seconds

Details [3]

Parameter	Range	Default	Description
(Fence / Buried) Sensor on Fence	Y or N	Y	Configures the APU for fence line or buried (other) applications. A "Y" value sets the system for fence line operation

Parameter	Range	Default	Description
Alarm Relay Time	1 to 10 (sec)	1	Specifies the length of time, in seconds, that the alarm will remain active once an alarm condition is set

Parameter	Range	Default	Description
Enable User Controlled Relay Mode	Y or N	N	Allows the user to directly operate the fault and alarm relay through FSN or XML. This disables relay stimulus upon an APU alarm/fault

Parameter	Range	Default	Description
Sensitivity Factor	1 to 100	10	Scales the unprocessed signal from the protected zone. Typically used to increase signal amplitude in Spectraview for improved signal visibility

Parameter	Range	Default	Description
Communication Mode	0 to 2	1	Selects the communication mode that the APU will use to provide alarm and status information. Choose between Relay Only(0), FSN(1), or XML(2)

When XML mode is enabled (see Chapter 7, page 7-13) the following additional menu option becomeS available within the Details menu.

Parameter	Range	Default	Description
XML Report Interval	1 to 600 (.1sec)	10	Adjusts the maximum frequency with which XML reports are output

Passwords (4)

Parameter	Range	Default	Description
Gain Menu Password	15 characters maximum	GAIN	Sets the password to access the Gain menu

Parameter	Range	Default	Description
Setup Menu Password	15 characters maximum	SETUP	Sets the password to access the Setup menu

When XML mode is enabled (see Chapter 7, page 7-13) the following additional menu options become available within the Passwords menu.

Parameter	Range	Default	Description
Device Name	31 characters maximum	APUNAME	The alias under which the device will communicate through the XML protocol

Parameter	Range	Default	Description
Channel Name	31 characters maximum	CHA	The name under which the channel will communicate through the XML protocol

Reset (RS)

Selecting this choice will clear all user-defined parameter settings (except passwords) and restore them to the factory default. From this selection, users can also reset the FSN device address if the unit is equipped with the FSN option.

If the unit is equipped with the FSN option, selecting the Reset option brings up the prompt:

CH Select reset type. FSN Address [1]
or APU Settings [2]:

Select option 1 to reset the FSN device address. Select option 2 to reset the APU settings to the factory default.

Hist

This is a read-only menu that provides a history of alarms beginning with the most recent alarm first. Alarms are read off according to how long ago they occurred. In addition, each alarm entry is date/time stamped. For instance, if the alarm history is read after three alarms occurred, the first report in the alarm history might read:

#3 Alarm, Processor 2 (W=0)
16:41 11/04/06

One can note from this example that the alarm history is provided for each alarm that occurs for each processor. From this report, the #3 indicates the alarm report number, Processor 2 indicates the processor in which the alarm occurred and the date and time on the bottom line of text indicates when the alarm was received. The “W=” parameter indicates the estimated wind speed at which the alarm occurred (determined by the internal wind rejection algorithms).

Up to 128 of the most recent alarm events will be stored in volatile APU memory. Each alarm event exceeding the allowable 128 will overwrite the oldest entry. If at any point you wish to exit this menu then enter "Q".

Status

This is a read-only command that provides a real-time system diagnostic of conditions such as system loss, laser current, power supply voltage (to the APU) and any present fault, event or alarm conditions. The Status menu also provides wind speed indication. When this menu is chosen, for example, the display reads:

Loss: 10 Las(mA): 17.5 Pwr(V): 15.0
[Evnt1][Evnt2][Alarm][Fault] Wnd:0

"Evnt1" and "Evnt2" refer to event conditions at Processor 1 and Processor 2.

Version

This read-only menu gives the APU model number, serial number, firmware version, date of manufacture and the number of days the unit has been in operation.

Table 5-1 summarizes all menus and their associated programmable calibration parameters.

Table 5-1

Password	Menu	Submenu	Parameters	Default (Fence)	Default (Buried)
GAIN			Gain (1 to 50)	**20**	**20**
SETUP			*Enter 1, 2, 3 or 4*		
	1	**Wind**	Enable Wind Rejection Software	**N**	**N**
			Wind Rejection (20 to 80)	**50**	**50**
	2	**Comment**	(15 characters max)		
	3	**Date**	Select Real Time Clock [1] or Calibration Date [2] (15 characters max for calibration date)		
	4	**Calibrate**	*Enter 1, 2, 3, 4 or RS*		
		(1) Processor 1	Enable (Y or N)	**Y**	**Y**
			Level of Signal (1 to 40 dB)	**10**	**10**
			Lowest Frequency (10 to 600 Hz)	**200**	**10**
			Highest Frequency (10 to 600 Hz)	**600**	**120**
			Duration of Signal (1 to 25 sec/10)	**3**	**3**
			Low Level Tolerance (1 to 10 dB)	**5**	**5**
			Event Count (1 to 100)	**3**	**2**
			Event Window (1 to 200 sec/10)	**50**	**90**
			Event Mask Time (0 to 100 sec/10)	**2**	**0**

Table 5-1 (continued)

Password	Menu	Submenu	Parameters	**Default (Fence)**	**Default (Buried)**
		(2) Processor 2	Enable (Y or N)	**Y**	**N**
			Level of Signal (1 to 40 dB)	**10**	**10**
			Lowest Frequency (10 to 600 Hz)	**300**	**10**
			Highest Frequency (10 to 600 Hz)	**600**	**120**
			Duration of Signal (1 to 25 sec/10)	**1**	**1**
			Low Level Tolerance (1 to 40 dB)	**3**	**3**
			Event Count (1 to 100)	**5**	**2**
			Event Window (1 to 200 sec/10)	**80**	**90**
			Event Mask Time (0 to 100 sec/10)	**7**	**0**

Password	**Menu**	**Submenu**	**Parameters**	**Default (All)**
		(3) Details	CH (Fence/Buried) Sensor on Fence? (Y or N)	**Y**
			Alarm Relay Time (1 to 10 sec)	**1**
			Enable User Controlled Relay Mode (Y or N)	N
			Sensitivity Factor (1 to 100)	**10**
			Communication Mode (0 to 2)	**1**
			Available only in XML mode XML report interval (0.1s) (1 to 600)	**10**

Table 5.1 (continued)

Password	Menu	Submenu	Parameters	Default (All)
		(4) Passwords	Gain Menu: 15 characters max	**GAIN**
			Setup Menu: 15 characters max	**SETUP**
			Available only in XML mode	
			Device Name: 31 characters max	APUNAME
			Channel Name: 31 characters max	CHA
		(RS) Reset	CH reset type. FSN Address [1] or APU Settings [2]: (FSN enabled units only)	
			- OR-	
			Destroy all preset settings and restore factory settings? (Y or N)	
HIST	Read Only		Note date and time and hit Enter for alarm history	
STATUS	Read Only		System light loss, laser current, power supply voltage, real time displays of Event 1, Event 2, Alarm and fault	
VERSION	Read Only		Model number, serial number, mfg. date, firmware revision, days of operation	

Calibrating and Testing the System

Once the system is fully installed and communication is established between the APU and the programming device (either the Hyperion or PC with terminal software), the system needs to be calibrated and tested.

Calibration begins by checking system loss, adjusting the gain and then making adjustments to other system parameters as necessary to ensure the FD-348R operates at top effectiveness. After each adjustment is made, the system should be tested at length to verify performance.

Checking System Loss

The integrity of the system connections is checked first to ensure the optical circuit is complete and optical loss is acceptable. This is done by powering up the APU and observing the total loss to the system.

To observe the total system loss:

1. Ensure power is being applied to the APU and the APU is properly connected to the sensor cable under test
2. At the password prompt, type *"STATUS"* into the programming device and press the **Enter** key, or if using Hyperion, once the software is launched, select Real-Time mode, then the *"Status"* tab. The system power, laser current and loss parameters are displayed
3. Verify system loss is less than 15 (dB). The APU measures system loss by comparing received input power versus a factory-set output power; therefore, this number is provided only as a rough test/troubleshooting means. If the system loss is greater than 15 dB, check the cleanliness of the connectors and any optical splice joints along the sensor cable and insensitive leads from the input of the APU back to the laser power source. Ensure the cable is not being crimped by any obstacles such as tree limbs

4. Verify the other displayed parameters:
   - LAS (mA)## Laser current. Normal operating range is 10 to 35 mA
   - PWR (V)## Input voltage at the APU. 11 to 13 VDC is acceptable

Setting the Gain

As mentioned previously, adjusting the gain affects the system sensitivity. A higher gain is more likely to detect the presence of an intruder; however, a higher gain is also more likely to allow nuisances to trigger an alarm. A balance needs to be met when adjusting the gain that can only be determined through adjustment and subsequent system testing.

NOTE:
An adjustment to the gain affects both Processor 1 and Processor 2 simultaneously. The gain cannot be adjusted independently for each processor. To adjust each processor individually, use level of signal described on page 5-25.

To adjust the gain:

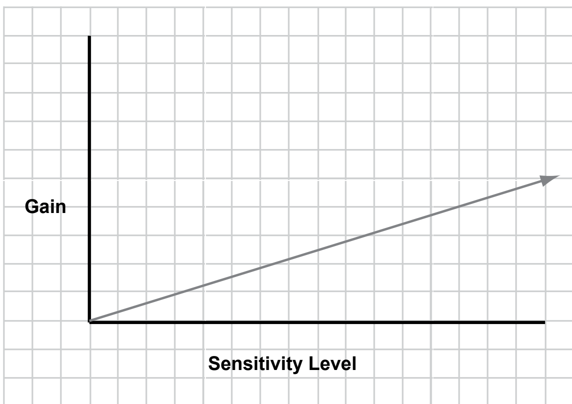


Figure 5-3: Gain adjustment principle

1. At the password prompt, type “GAIN” (or its current password) into the programming device and press the **Enter** key. The current system gain will be displayed
2. Simulate the desired level of intrusion for which the FD-348R should protect against and verify that an alarm condition occurs. Adjust the gain as necessary until an alarm occurs

Ensure the system is tested at all areas and ways where intrusion is likely and is difficult to detect (such as the corner post of a fence). The cutting of chain link fence can be simulated by temporarily attaching a spare section of fence fabric to the fence and securing it using cable ties. Cut the squares of the spare fabric section and check the response of the system.

To minimize nuisance alarms the gain should be adjusted to the *minimal level* that will adequately detect the intrusions simulated during calibration (see *Testing the System* later in this chapter). This ensures the system is no more sensitive than it needs to be.

Adding Wind Processing and Event Processing

The manner in which events are processed can be refined to ensure nuisances (such as wind) have a minimal effect on the APU processors while genuine intrusions are detected each time. Wind processing and event processing parameters provide a way to calibrate the APU and make the necessary refinements in the detection processing system.

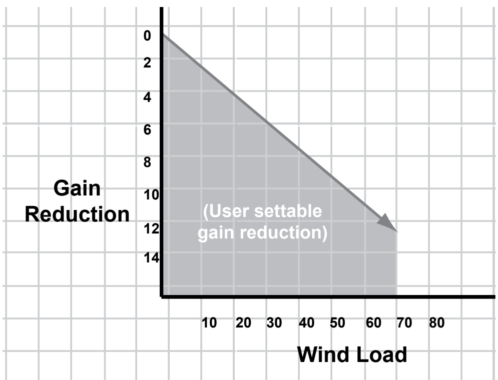
NOTE:
Unlike the gain and wind processing parameters, event processing parameters can be adjusted individually for Processor 1 and Processor 2.

As is done when the gain is adjusted, system testing should follow each adjustment made to the wind processing or event processing to verify system performance.

Wind Processing

The effects of wind must be considered and compensated for in all fence line applications. These effects can be dampened with the use of the wind processing software and proper adjustment of the wind rejection factor.

1. Ensure the system is configured for fence line operation by accessing **SETUP >> CALIBRATE >> DETAILS** and selecting "**Y**" for the fence-mounted sensor configuration
2. Enable wind processing by accessing the **SETUP** menu and entering the wind processing submenu (see *Programmable Calibration Parameters* earlier in this chapter)
3. Set the *Enable* parameter to "**Y**". Wind processing is now enabled
4. Set the wind rejection factor as needed so that the wind has a minimal effect



As the wind load picks up, the APU will automatically scale back (or "dampen") the gain in accordance with the wind rejection factor. A higher wind rejection factor means more dampening, requiring a signal higher in magnitude to create an alarm condition.

The minimum wind rejection factor is 20 and the maximum is 80.

Figure 5-4: Wind reduction principle

Event Processing

Event processing can be refined by accessing the event parameters through the SETUP menu and “Calibrate” submenu. Event parameters that can be programmed or adjusted are:

- Lowest and highest frequency
- Level of signal
- Duration of signal
- Level tolerance
- Event count
- Event window
- Event mask

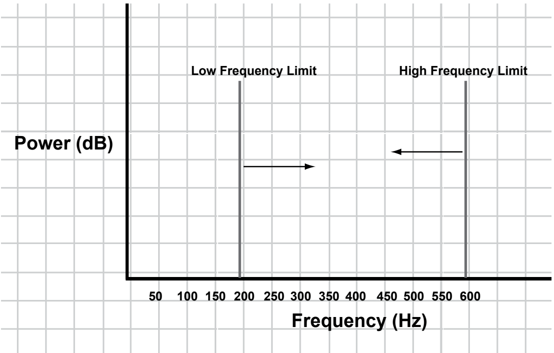
Adjustment of the event parameters defines what sensor cable signals constitute events. Therefore, the typical or expected threats against a system can be characterized by the event processing setup.

NOTE:
Accurate setting of event parameters is usually determined through experimentation and testing of the system following installation.

Frequency Filters (lowest and highest). These filters determine the frequency range at which sensor cable signals will be allowed to pass to the processor.

Recall from Chapter 1 that incoming optical signals from the sensor cable are converted into electrical signals, digitized and transformed from the time domain to the frequency domain. This is done to help determine whether a phase shift in the propagating light has occurred as the result of a disturbance in the sensor cable.

An intruder or nuisance will leave its own signature frequency as it disturbs the sensor cable. For instance, the footsteps of an intruder walking across a buried cable might make a disturbance that oscillates at a frequency of 10 Hz. Selecting the right frequency range will help filter out events made at frequencies caused by nuisances.



Determining the best frequency range is a matter of experimentation and testing the system following installation.

Figure 5-5: Frequency limit principle

Signal Level. The signal intensity of a nuisance is generally lower than that of an intruder. Setting this level means that a signal from the sensor cable must be higher than the set level to be counted as an event.

Signal Duration. The duration of the signal can also help to distinguish a disturbance from an intruder versus a disturbance from a nuisance. Most nuisances cause disturbances that are generally longer in length than those caused by a determined intruder but are of lower magnitude. On the other hand, some disturbances, such as the popping a metal fence makes in changing temperature, are high in magnitude but very short. In the figure to the right, this setting combines with the signal level setting to mean a signal must be higher than the set signal level for at least 3/10ths of a second or longer to qualify as an event.

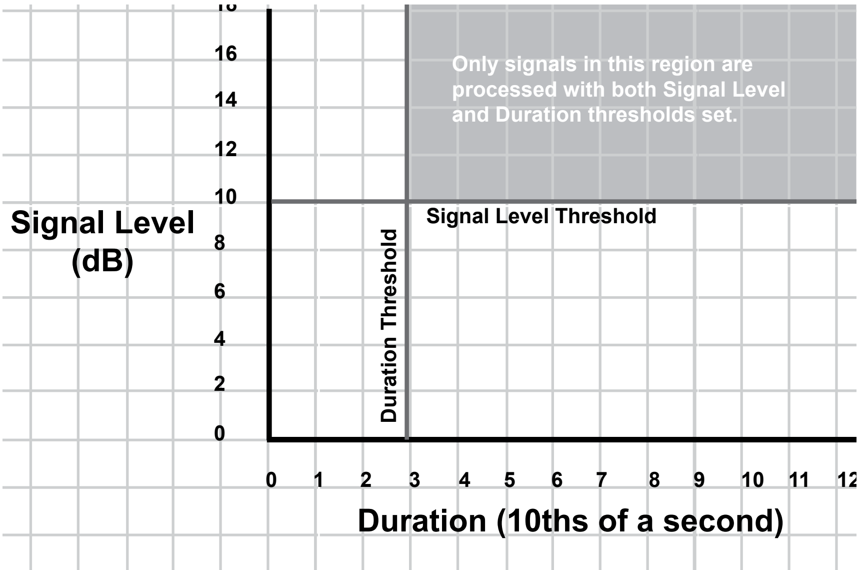


Figure 5-6: Signal duration illustration

Level Tolerance. The tolerance level specifies a lower level tolerance for incoming signals. This allows a signal at a level lower than the signal level setting to be considered an event *if it lasts for a period of time automatically set by the processor*. The higher the tolerance, the longer the processor will set the duration for the lower signal.

Event Count, Window and Mask Time. One of the best ways to differentiate signals generated by an intruder from those of a nuisance is by the number of times a signal is generated in a given period of time. Generally, a nuisance such as an animal or tree branch doesn't make consistent disturbances of the fiber as an intruder does.

The *Event Count* parameter specifies the number of times an event must be received for an alarm to occur. This parameter is used in tandem with the *Event Window* parameter.

An *Event Window* specifies a window of time following an initial event during which it is possible to increment the alarm counter. Each event has its own associated event window, but unless at least one event occurs within the event window of another, the event counter resets. In other words, if the event window is set for 5 seconds and the event counter is set for 3, this means at least 3 events must occur no more than 5 seconds apart (a total time of 15 seconds) for an alarm to occur. If an event window expires before another event occurs, the event counter resets and a new event window begins with the next event.

For example, in Figure 5-7, the event window from the first event expires before the second event occurs. Thus, the event counter resets and the second event simply sets the event counter from 0 to 1.

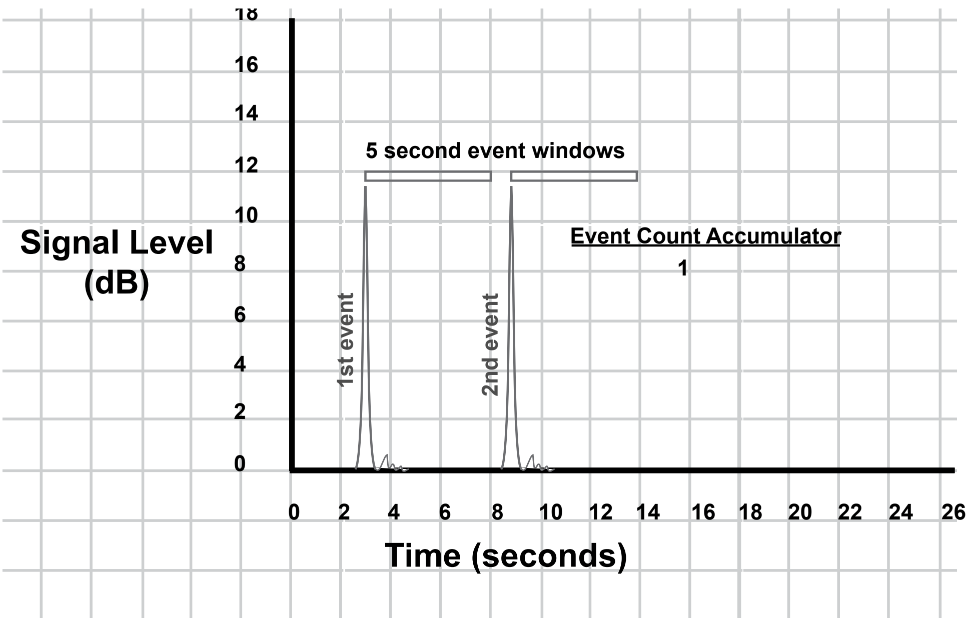


Figure 5-7: Event Windows

If, however, the second event occurs before the first event window expires, the event counter increments and remains active throughout the event window of the second event. In Figure 5-8, even though the third event falls outside the event window of the first event, the event counter is still active; thus, it counts toward an alarm.

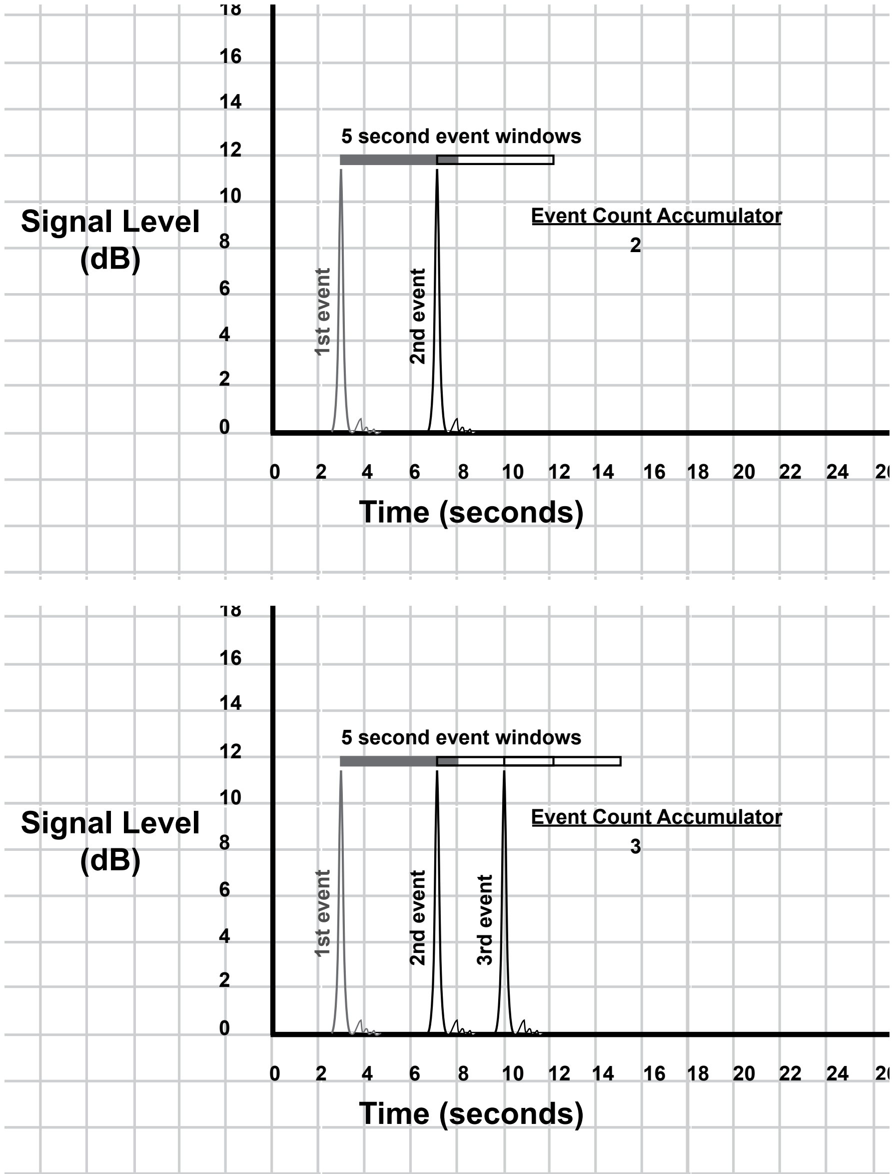


Figure 5-8: Creating an alarm condition

Each event also has a *mask time* associated with it. A mask time is a period of time following an event during which no subsequent events will be counted. The mask time parameter is included to account for oscillations made after an initial strike against a fence by a bird or other nuisance.

Putting all three event counting parameters together:

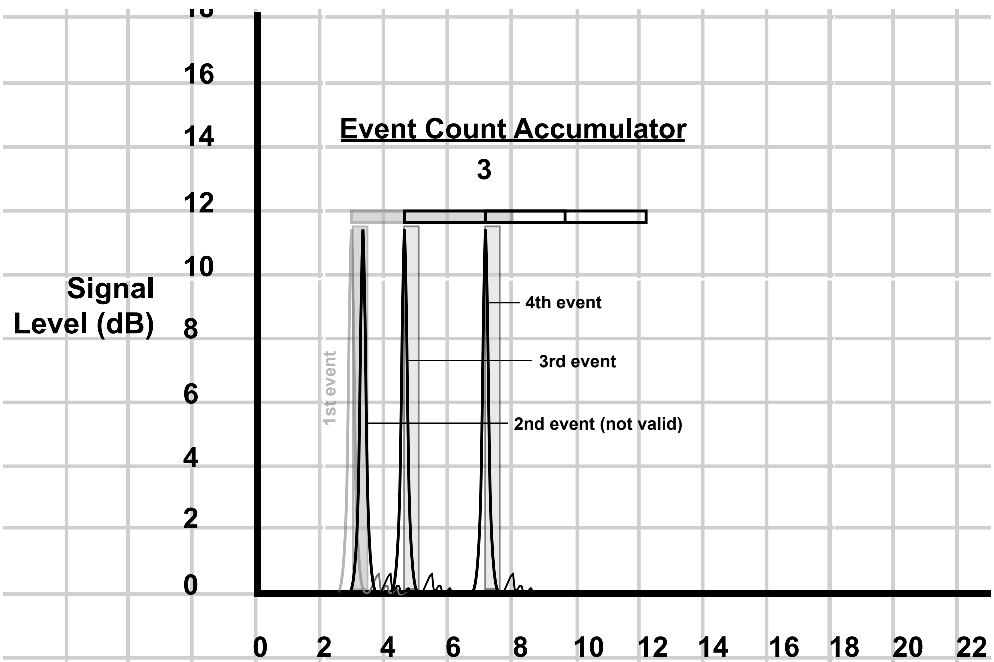


Figure 5-9: Counting valid events

Here, we see that four events occur. Each has its own associated mask time. The second event is not counted toward the event counter because it falls within the mask time of the first event. Combined together, at least three valid events occur within the same event window (counting the first event) and an alarm condition occurs.

Testing the System

As the last step of the calibration/installation process, the FD-348R should be tested to determine its effectiveness.

Fence Line Applications

System testing begins with reviewing the list of threats against the site. To determine the Probability of Detection (PD) for those threats, begin by simulating each threat. Perform each threat simulation 20 times and monitor the response of the FD-348R. For example, to determine the PD of an intruder climbing over the fence, have a volunteer climb over the fence in the same manner 20 times. Do not give the individual any knowledge of whether or not an alarm is being generated (to prevent him or her from changing the manner in which he or she climbs the fence). Record the number of climbs that produce an alarm. Tally up the number of climbs that generated an alarm and divide by 20. Multiply the result by 100 to calculate the PD (in percent). If the PD is too low, adjust the Gain, Event Count and Signal Level parameters as necessary until the PD reaches the desired level (see *Setting the Gain* and *Adding Wind Processing and Event Processing* earlier in this chapter).

Repeat this test for each installed zone or APU at the protected site.

Figure 5-10 provides a sample log for calculating the PD of some basic fence line threats. The list of threats in this log is not exclusive; therefore some or none of the threats in this log may be applicable to your fence line setup.

Location											Date
FSI Intrusion Detection Test Data											Project No.
Processor Serial No.	Zone No.	Pass No.	Intrusion Detection Fabric Climb Test		Intrusion Detection Ladder Climb Test		Intrusion Detection Fabric Cut Test		Intrusion Detection Fabric Lift Test		Comments
			Pass	Fail	Pass	Fail	Pass	Fail	Pass	Fail	

Figure 5-10: Fence Line Application Detection Data Sheet

Buried Application

The principles and procedure for testing the FD-348R with a buried application is generally the same as it is for a fence line application. The types of threats will be different. To simulate the walk intrusion, it is recommended that the volunteer "intruder" crouch while walking (or "duck walk") to simulate the stealth likely to be used by a walking intruder. As a separate test, it is also recommended that the same individual attempt to jump across the detection zone as well. Do not let the individual know how far the detection zone extends when performing this latter test.

Figure 5-11 provides a sample log for calculating the PD of some basic threats against a buried application. The list of threats in this log is not exclusive; therefore some or none of the threats in this log may be applicable to your setup.

For some buried applications, if the cable is buried too close to the fence, it may pick up vibrations from the fence when the wind blows against it, causing nuisance alarms. If this is discovered to be the case during the testing process, either deploy the cable further from the fence or raise the Signal Level (see *Event Processing* earlier in this chapter) until the disturbance no longer causes an alarm.

Repeat this test for each installed zone or APU.

Location											Date
FSI Intrusion Detection Test Data											Project No.
			Intrusion Detection Walk Test		Intrusion Detection Crawl Test		Intrusion Detection Run Test		Intrusion Detection Jump Test		
Processor Serial No.	Zone No.	Pass No.	Pass	Fail	Pass	Fail	Pass	Fail	Pass	Fail	Comments

Figure 5-11: Buried Application Detection Data Sheet

Line Test

This test verifies that a loss of return optical power to the APU results in a “Fault” condition indicator on the APU.

1. Proceed to the first APU. Ensure that no fault or alarm indicating LEDs are lit on the APU
2. Disconnect the optical cable from the APU input connector. Verify that a Fault alarm is generated
3. Record the test results in the FSI Test and Acceptance Log (a sample log is provided in figure 5-12)
4. Reconnect the cable. The Fault alarm should clear
5. Repeat these steps for all remaining FD-348R APUs

Location				Date
FSI Line Supervision Test and Acceptance Log				Project No.
Processor Serial No.	Zone No.	Fiber Optic Cable Fault Test		Comments
		Pass	Fail	

Figure 5-12: Test and Acceptance Log

6

MAINTENANCE & TROUBLESHOOTING

Maintenance

General

Operational site maintenance consists of routine preventative maintenance inspections, fault isolation and removal and replacement of faulty equipment.

Support Equipment

Maintenance equipment is listed as follows:

Table 6-1: Maintenance Tools

Item	Fiber SenSys Part No.	Notes
Hand-held Calibrator	Hyperion	Optional
Laptop PC with RS-232 serial port connection and MSN HyperTerminal emulation software or equivalent	N / A	Optional substitute for Hyperion
DB-9 Serial port cable (straight 9-pin)	N / A	Required with laptop PC
Loopback test cable	N / A	Locally fabricated as illustrated in this chapter
6 inch screwdriver	N / A	
SpectraView® advanced programming and maintenance software	SpectraView®	Optional

Preventative Maintenance

Task	System Visual Inspection
Required Tools	None
Recommended Performance Interval	90 days

Procedure

1. Carefully inspect the sensor cable conduit for integrity. Verify there are no cracks or kinks in the conduit. Also verify the cable is not pulled into a radius tighter than 5 cm (2 inches) at any point
2. Ensure the conduit is attached firmly to the fence (fence line applications only). Add or replace wire ties as needed
3. Inspect the integrity of the fence. Tighten any loose fence hardware and remove any foreign material from the fence fabric
4. Ensure all APU LED indicators are normal ("Power" indicator only is lit)
5. Check the optical connectors at the APU and ensure they are properly seated.

Task System Performance Test

Required Tools None

Recommended Performance Interval 90 days or as required

Procedure

1. Perform the Intrusion Detection **Fabric Climb Test** (fence line applications) by having an individual climb to the top of the fence fabric. Verify that an alarm is generated at the annunciator equipment
2. Record the test results
3. Reset the annunciator equipment
4. Repeat Steps 1 through 3 at various locations throughout the zone to verify zone protection
5. Perform the Intrusion Detection **Ladder Climb Test** (fence line applications) by having an individual attempt to use a ladder to climb over the fence fabric. Verify that an alarm is generated at the annunciator equipment
6. Record the test results
7. Reset the annunciator equipment
8. Repeat Steps 5 through 7 throughout the zone to verify zone protection
9. Perform the Intrusion Detection **Fabric Cut Test** (fence line applications) by having an individual attempt to cut through the fence fabric. This can be simulated by tapping on the fence with a screwdriver to simulate each cut. Verify that an alarm is generated at the annunciator equipment

10. Record the test results
11. Reset the annunciator equipment
12. Repeat Steps 9 through 11, tapping the screwdriver on the fence at various locations to verify zone protection. The number of taps or “cuts” should correspond to the current Event Count setting
13. Perform the **Walk Test** (buried applications) by having an individual walk slowly across the zone. Verify that an alarm is generated at the annunciator equipment
14. Record the test results
15. Reset the annunciator equipment
16. Repeat Steps 13 through 15 at various locations throughout the zone to verify zone protection
17. Perform the **Run Test** (buried applications) by having an individual run and jump into the zone. The person should jump as high into the air as possible before coming down into the zone. Verify that an alarm is generated at the annunciator equipment
18. Record the test results
19. Reset the annunciator equipment
20. Repeat Steps 17 through 19 at various locations throughout the zone to verify zone protection
21. Refer to the troubleshooting section of this chapter if the alarm fails to activate during testing

Task APU Status Check

Required Tools Hyperion Hand held Calibrator or PC with SpectraView® or terminal emulation software

Recommended Performance Interval 180 days

Procedure

1. Connect the Hyperion directly to the APU utilizing the RS-232 cable (Figure 6-1)
2. Once the Hyperion is activated, select the Real-Time mode to proceed
3. Select the “STATUS” tab at the bottom of Hyperion's screen to display the following summary of the APU's operational status:
   - LOSS: Less than 15 dB
   - LAS (mA): Between 17 and 35 mA
   - PWR: Between 12 and 24 VDC

-- OR --

1. Launch SpectraView® from the PC. Select the "Modes" tab at the left hand side of the screen. From the pop-out menu, select "Terminal", which launches the TerminalMode screen for checking "Status"

NOTE:
For more detailed instructions about Hyperion's "Status" tab or SpectraView's® "Terminal" tab, please refer to the respective user's reference manuals available through Fiber SenSys.

Task	1 meter "loopback" cable creation
Required Tools	CK-600 or equivalent connector kit
Recommended Performance Interval	As needed

Procedure

1. Obtain a 1 meter section of single-mode optical fiber. Only single mode optical fiber can be connected directly to the FD-348R
2. Following the instructions found in the CK-600 connector kit, terminate the ends of the fiber with ST connectors
3. Test the loopback cable by connecting it to the optical connectors of a known good APU. There should be no fault or alarm indicators illuminated (see Figure 6-1)
4. Run a "STATUS" check on the APU and verify the LOSS number is acceptable

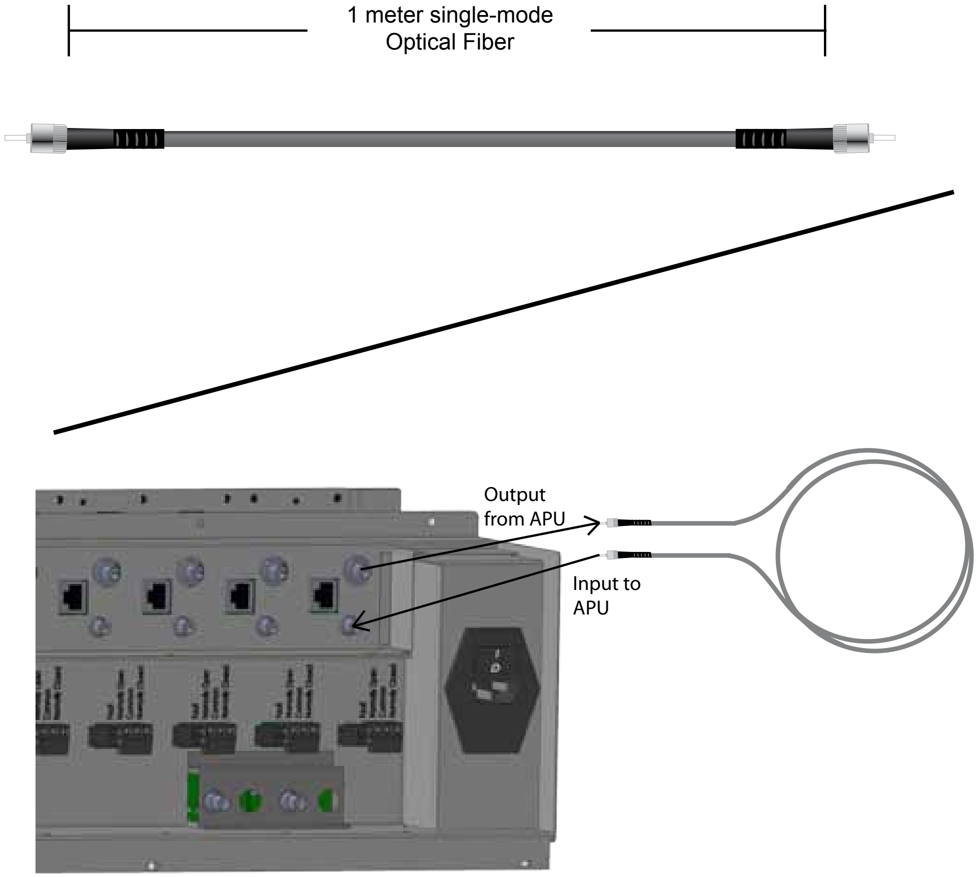


Figure 6-1: The loopback cable

Troubleshooting

SYMPTOM: No alarm at the annunciator panel

RESPONSE: Troubleshoot the system in accordance with the flow chart found in figure 6-2

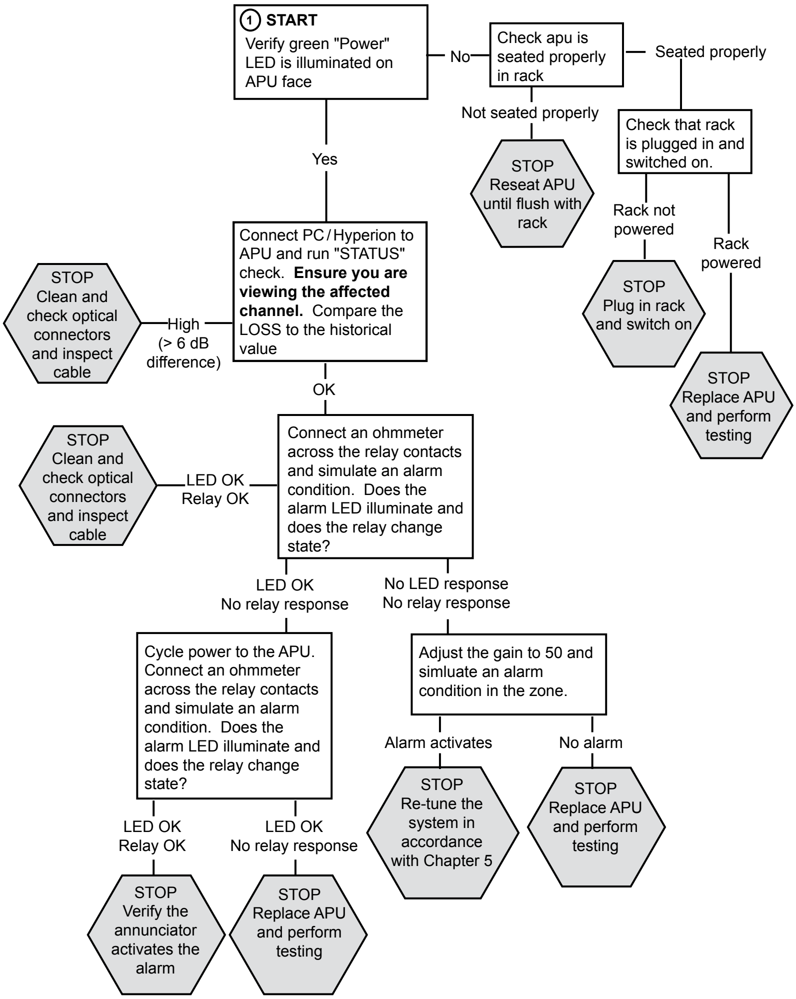


Figure 6-2: Troubleshooting flow chart for a Lack of Alarm

SYMPTOM: Constant alarm at the annunciator panel

RESPONSE: Troubleshoot the system in accordance with the flow chart found in figure 6-3

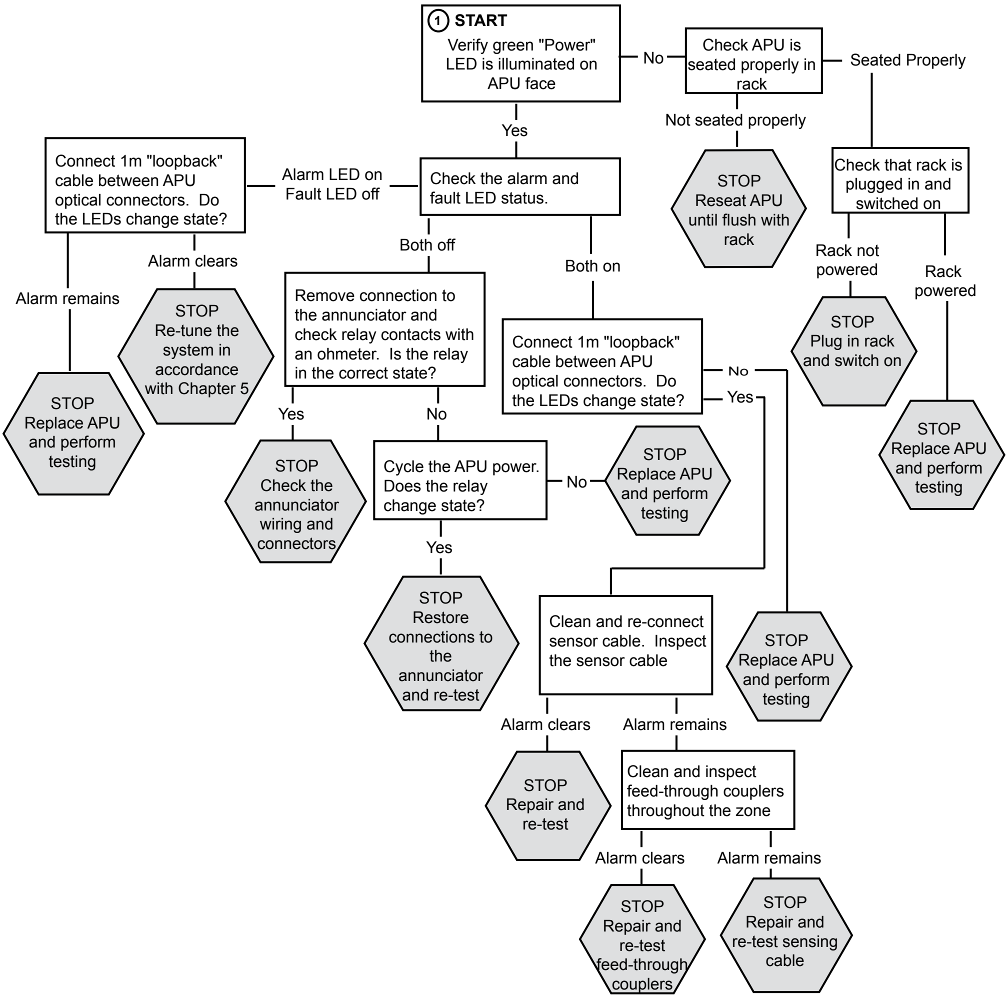


Figure 6-3: Troubleshooting flow chart for a Constant Alarm

SYMPTOM: Intermittent, unexplained alarms

RESPONSE: There may be multiple causes. Troubleshoot the system in accordance with figure 6-4

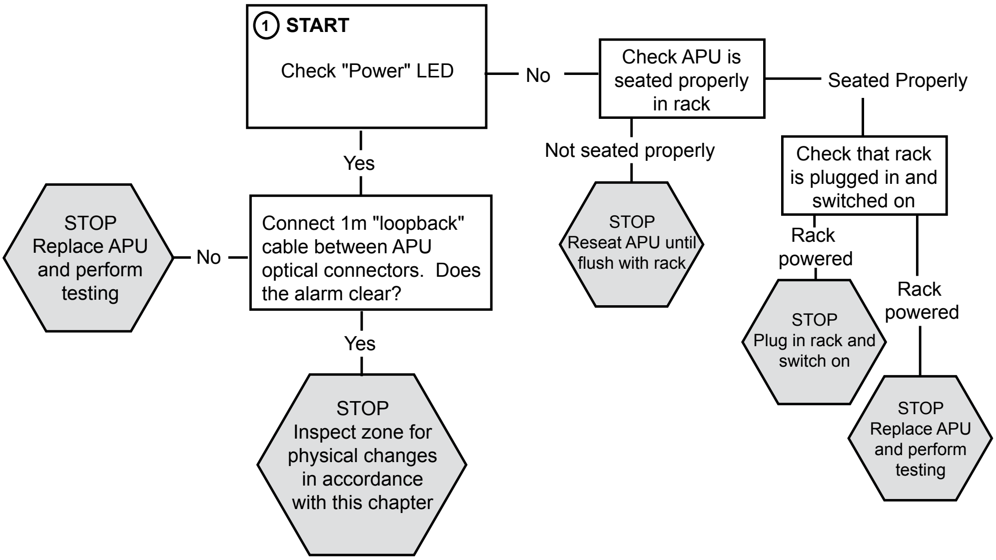


Figure 6-4: Troubleshooting flow chart for Intermittent Alarms

If the flowchart indicates the need to inspect the zone and adjust the APU sensing parameters, the system may be receiving nuisance alarms from one or more sources. As a first step, check the system gain and adjust it for the lowest possible gain that still allows for complete intruder detection. This is determined through experimentation and testing (see *Setting the Gain* in Chapter 5).

Possible nuisance sources that should be considered include:

- Wind
- Animals
- Birds
- Loose cable ties
- Loose fence fabric or a clanging gate
- Nearby aircraft
- Large towers or structures that can resonate with the wind and create low frequency oscillations

One of the most difficult steps in countering nuisance alarms is identifying the source. A tool that can help assist you in this process is the Fiber SenSys SpectraView® software, which can help by providing visual identification of the nuisance signal frequency and waveform. For more information on this tool, contact Fiber SenSys.

Investigate and determine where the source of nuisance is coming from. Once the source is identified, measures should be taken to reduce the effects of the source, including recalibration and retesting of the FD-348R system.

In addition to recalibration, some other steps that can be taken include making the sensor cable less susceptible to vibrations from the nuisance source. If alarms are being generated by groups of birds resting on a fence-mounted sensor cable, for instance, the cable can be insulated by being placed in UV resistant PVC pipe along the affected section.

Some electrical harmonics can be induced into heavy electrical equipment. If this equipment is located near a sensor cable, vibrations from the equipment may be transmitted to the cable. Knowing the frequency and waveform of the signal from the suspected nuisance would help isolate it in this case. Use the frequency filter to filter out all signals at the suspected frequency.

In addition, a "comb" filter can be employed to filter out harmonics from the electrical waveform. For more information on setting up a comb filter, contact Fiber SenSys.

7

NETWORK INTEGRATION

Introduction

The FD-348R incorporates communication options intended to increase the ease with which users can communicate with the system. The capability exists to plug an FD-348R APU directly into a LAN network. Alternatively, users can employ the FD-348R with embedded Fiber Security Network (FSN) compatibility enabled.

XML Communication

XML, or eXtensible Markup Language, is a protocol which focuses on preserving the content of data transferring across a network from one component to the next. With XML, users “tag” various pieces of data or messages to indicate the associated semantics, thus creating what are referred to as XML “documents”. These tags accompany the information in the document as it is passed between components. When one computer receives the data from another, for example, it is able to reassemble the message or document content accurately.

With the FD-348R, XML communication allows a network to receive status messages from an FD-348R (such as alarm / intrusion, tamper or fault conditions, etc.) and allows a controller to send device configuration commands to an APU.

XML documents can be created in any text editor (such as Microsoft Word®) and sent via any program or utility capable of addressing the appropriate network port. A number of alarm annunciator programs already have IP addressing capability embedded. For users without such programs, any terminal emulation software may be used.

IP Communication

Each FD-348R comes fitted with an RJ45 connector for TCP/IP network connection. This connector is located on the back of the APU and is exposed at the back of the RK-348 when the APU is installed (Figure 7-1).

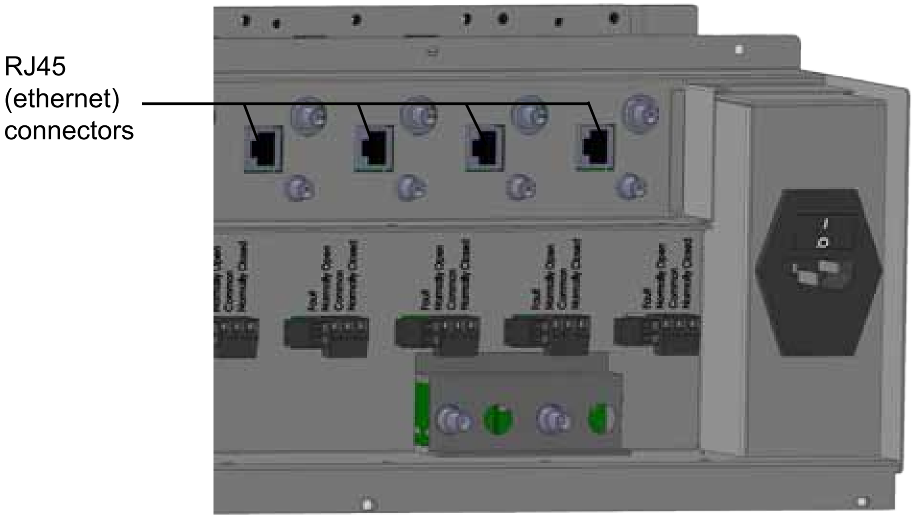


Figure 7-1: Ethernet connections on the back of the RK-348

Data is sent to and from the APU using XML communication.

Connecting the APU to the LAN

NOTE:
This section assumes readers have an operating knowledge of networks and network administration.

Each FD-348R APU comes from the factory with a default IP address of **0.0.0.0**, making it ready for insertion into a Dynamic Host Communication Protocol (DHCP) type network. Once connected, the network server will assign an IP address to the APU.

If the APU is not being connected to a DHCP type network, an IP address will have to be assigned to the APU. For instructions on assigning an IP address manually, refer to *Setting the IP Address of the APU* on this page.

The local port number of the APU is **10001**.

NOTE:
A default value of **10001** *is assigned to the APU port at the factory. For help in changing this port number, contact Fiber SenSys.*

Setting the IP Address of the APU

For networks which are not based upon the DHCP scheme, the IP address of the APU must be set manually using any PC with the Lantronix® DeviceInstaller Software or through telnet port 9999).

To set the IP address using DeviceInstaller:

1. Connect a CAT 5 network cable from the APU to a host PC

NOTE:
Lantronix® DeviceInstaller installation software and help files are included with the APU product components.

2. Power the APU

3. Launch Lantronix® DeviceInstaller from the host PC

4. The software may automatically detect Xport devices. If not, clicking the Search button, Figure 7-2, will allow the program to locate and display, as in Figure 7-3, the Xport connected devices

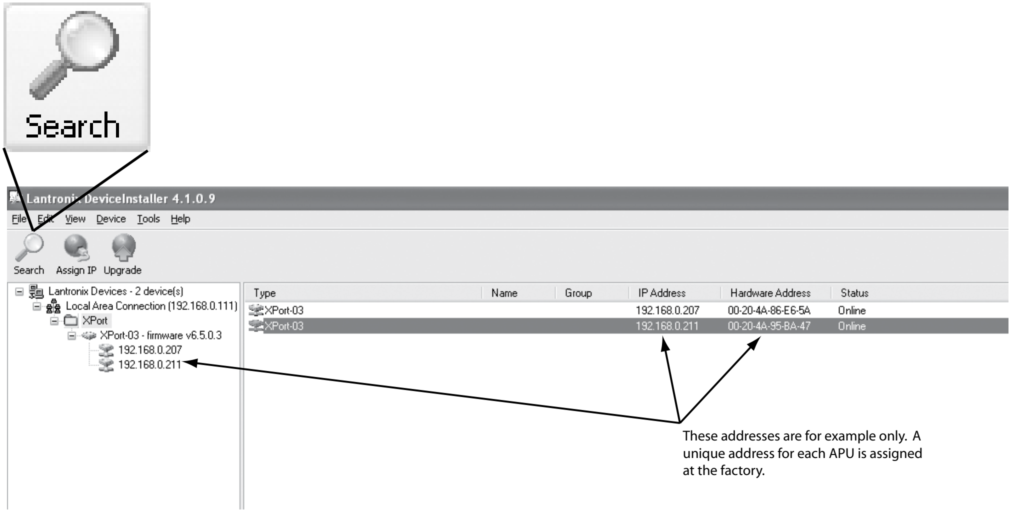


Figure 7-2: Lantronix® DeviceInstaller screen with Xport devices identified and the Search button

NOTE:
The MAC address *of the APU is found on a removable label which covers the RJ45 connector upon shipment from the factory. It also appears on the serial number label of the APU (the Hardware Address noted in Figure 7-2).*

5. By clicking on the Xport device, it is then selected for configuration with details about the device displayed

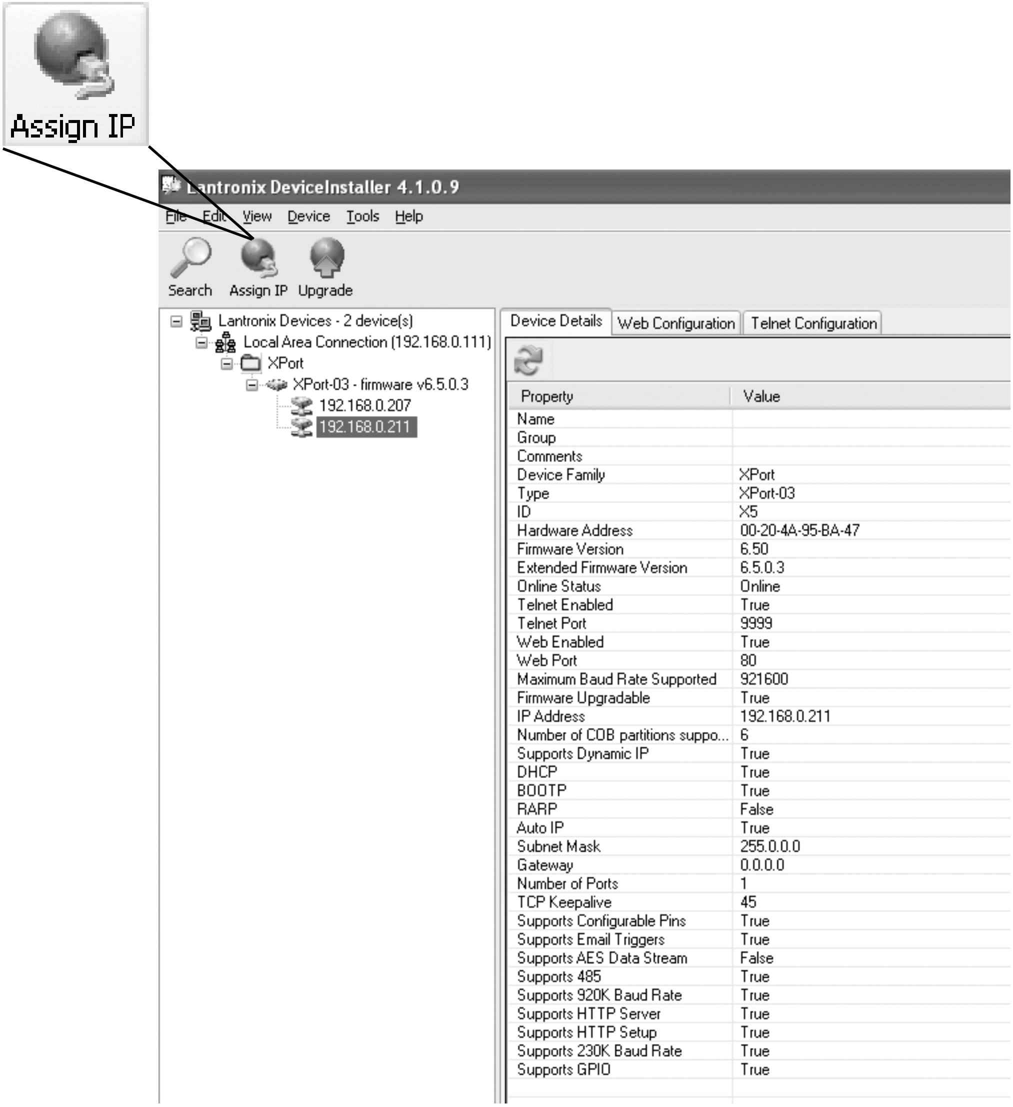


Figure 7-3: Device Details screen for selected Xport device

6. Select the **Assign IP** button, Figure 7-3, from the upper right hand side of the screen

7. The "Assignment Method" screen displays, from here select "Assign a specific IP address", as shown in Figure 7-4, then select the **Next >** button

Figure 7-4: Assignment Method screen for assigning a specific IP address

8. When the "IP Settings" screen displays, enter the assigned IP address, at which point the Subnet mask and Default gateway fields are filled in automatically, as displayed in Figure 7-5, then select the **Next >** button

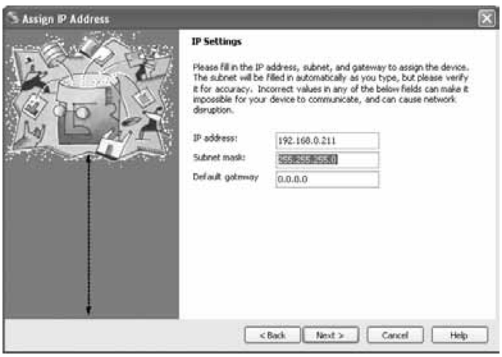


Figure 7-5: IP Settings screen

9. When the "Assignment" screen displays, Figure 7-6, press the **Assign** button to begin the process of assigning the new IP address. The Assignment status screen displays, showing the progress of the current task, as seen in Figure 7-7

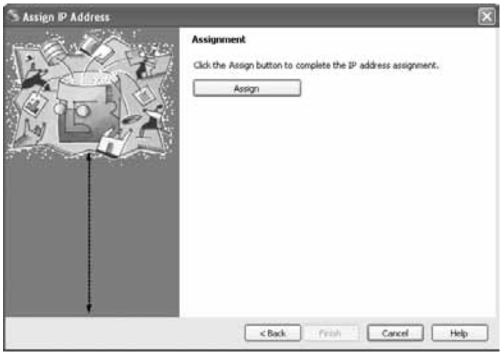


Figure 7-6: Assignment screen with the Assign button

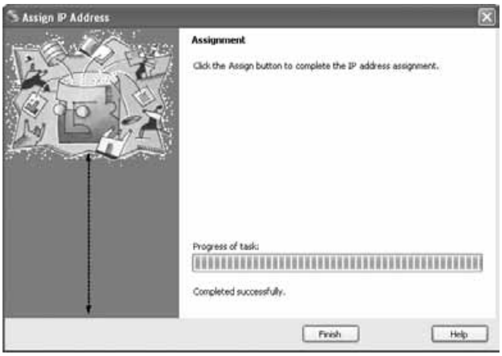


Figure 7-7: Assignment screen with "Progress of task:" bar

10. Once the task has been successfully completed, click the **Finish** button

11. To assign the "Subnet mask" and "Default gateway identifiers", repeat steps 3 through 9, from the Search function

CAUTION
CHANGING ANY OTHER SETTINGS MAY DISRUPT OPERATION OF THE DEVICE. FOR ASSISTANCE WITH THIS, CONTACT THE FACTORY.

Network and Serial Setup

The steps in this process are used to correctly assign Network and Serial connections once an IP address has been assigned per the *Setting the IP Address* procedures outlined earlier in this chapter.

NOTE:
Changes are accepted ONLY after the **Apply Settings** *button is pressed. Simply pressing the* **OK** *button will not apply the changes.*

1. Start Internet Explorer or other internet browser
2. In the address box at the top of the internet browser screen, enter the IP address just assigned during the Lantronix® DeviceInstaller program setup, as in Figure 7-8

Figure 7-8: Address bar where to enter newly assigned IP address

3. When the Xport login screen appears, Figure 7-9, simply click the **OK** button, leaving the “User name” and “Password” fields empty

Figure 7-9: The login screen with blank data fields

4. From the left-hand side menu that appears at the home screen, Figure 7-10, select "Channel 1, Serial Settings". Verify, or change if necessary, the “Baud Rate” to 230400. Do not change any of the other parameters

Figure 7-10: Menu options for the Device Server Configuration Manager

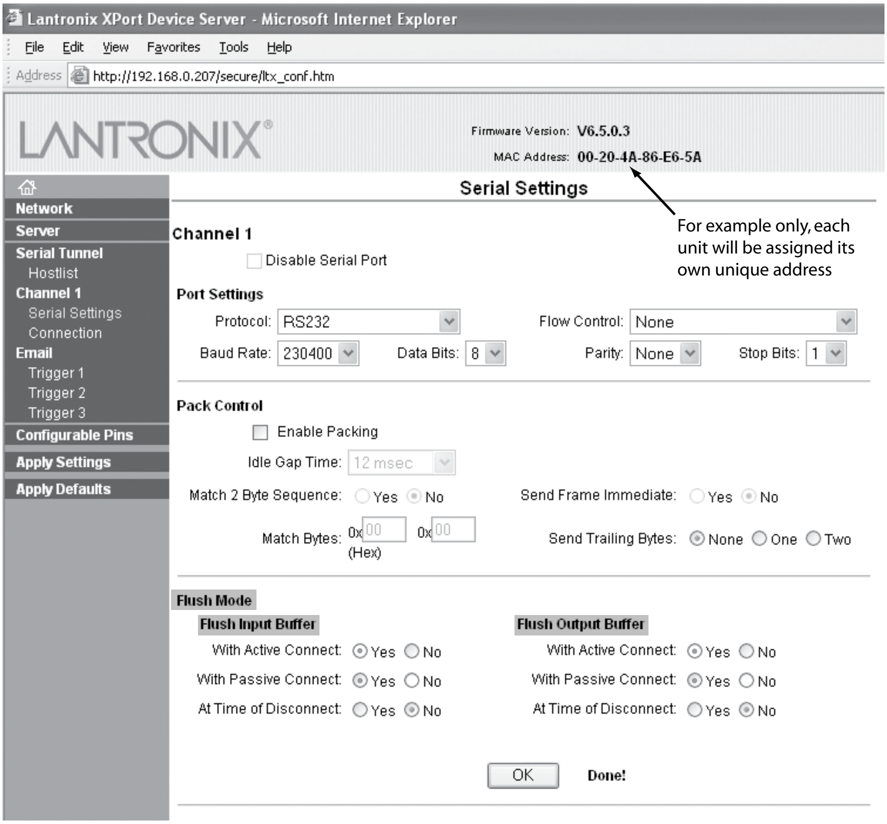


Figure 7-11: Serial settings screen

NOTE:
Flush both Input *and* Output *buffers with* “Passive”*, as well as* “Active Connect” *shown in Figure 7-11.*

5. Click the **OK** button to confirm the changes. A “Done!” notation will appear immediately to the right of the button to indicate changes have been applied

6. From the menu again, select "Channel 1, Connection, Channel 1". When the "Connection Setting" screen appears, Figure 7-12, verify or change the "Active Connection" drop down menu to “Auto Start”

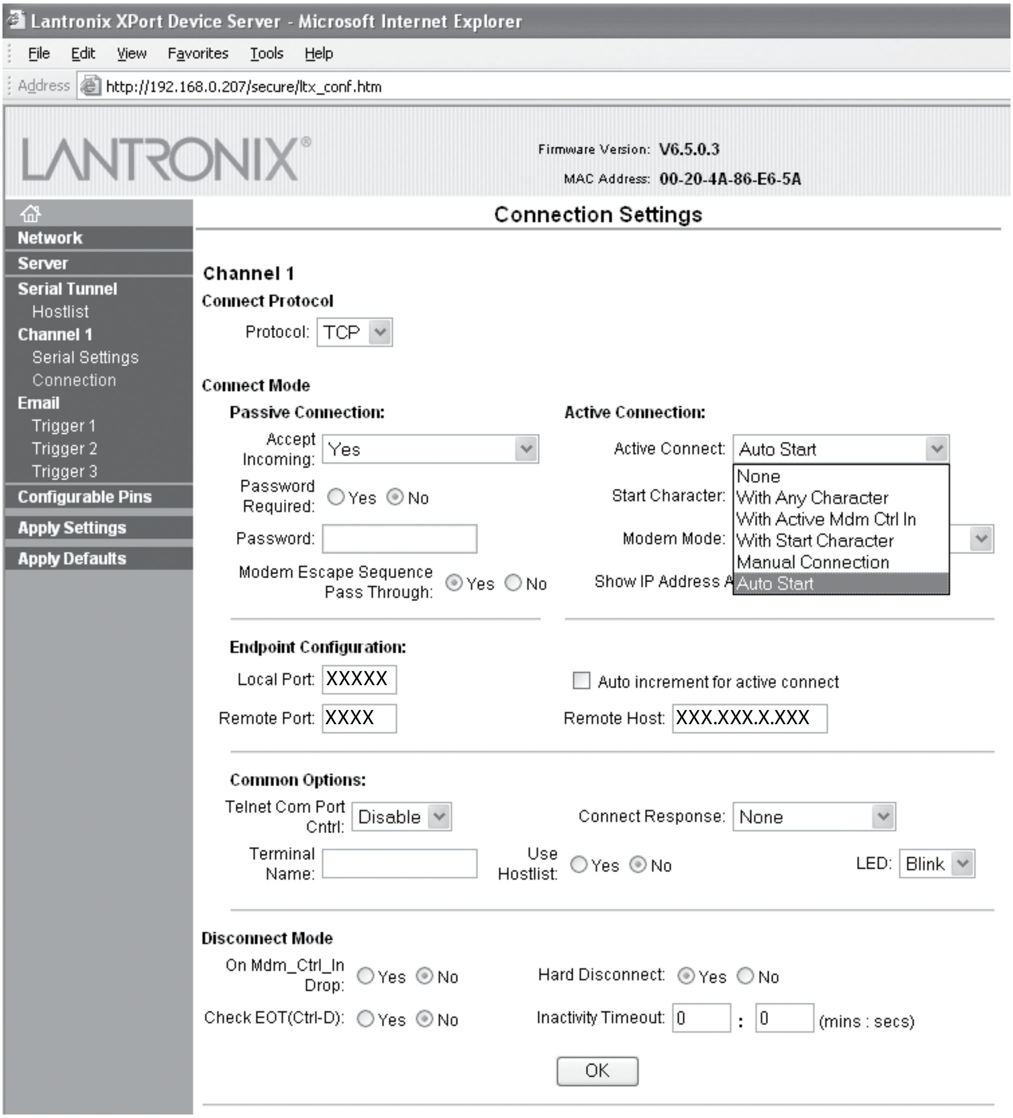


Figure 7-12: The Connection Settings screen

7. From the same screen seen in Figure 7-12, move to the "Endpoint Configuration" section and verify or enter the corresponding data as follows:

"Local Port"	**XXXXX**
"Remote Host"	**XXX.XXX.X.XXX**
"Remote Port"	**XXXX**

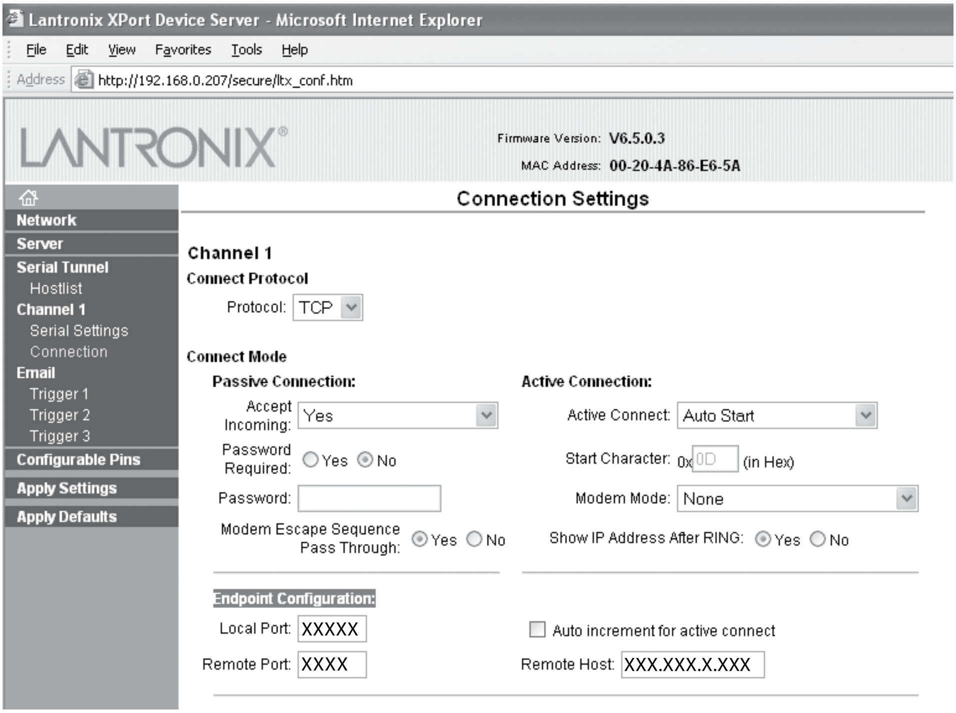


Figure 7-13: "Endpoint Configuration" section of the "Connection Settings" screen

NOTE:
The data for Local Port, Remote Host and Remote Port is user dependent.

8. Click the **OK** button to apply the changes. The "Done!" notation, as seen earlier, appears indicating the changes have been accepted, as seen earlier in Figure 7-11

9. In order for the changes to be applied and saved, refer to the left-hand side menu again. Click "Apply Settings" to save the recently updated information. The new settings will not be applied until this step has been completed. A status screen, as shown in Figure 7-13, will display. Once the process has completed, the home page will be displayed, and at this time, Internet Explorer can be closed, completing the assignment of correct Serial and Network settings

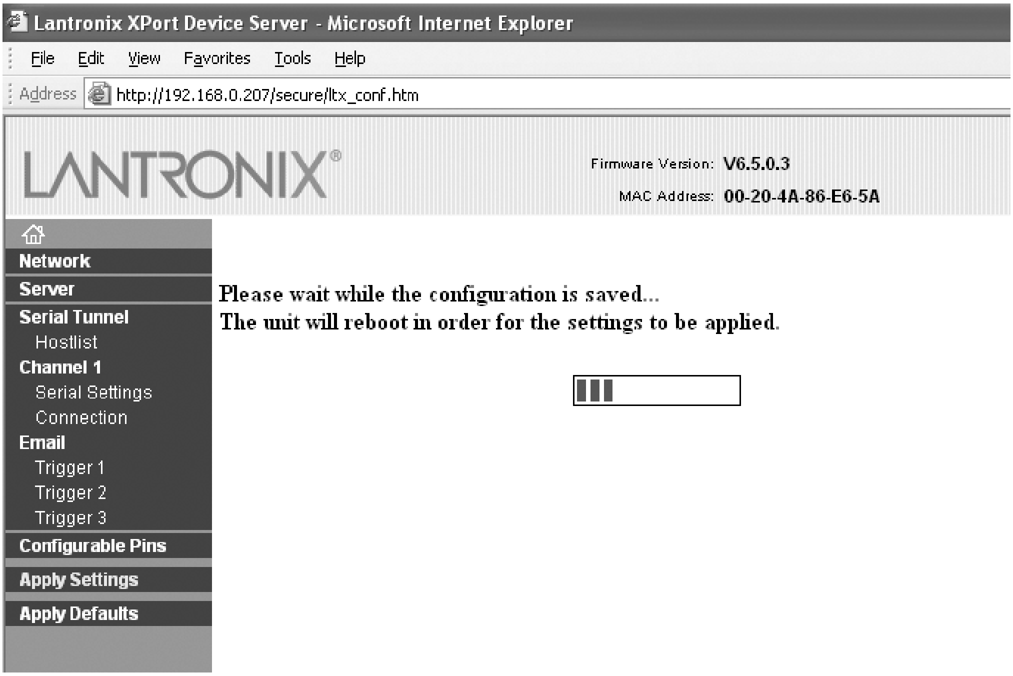


Figure 7-14: The status page for applying the newly assigned settings

10. The final step for enabling IP communication is to enable it in the settings for the device. Using terminal emulation software such as HyperTerminal® or Fiber SenSys' SpectraView® navigate to the details menu and select "XML" for the communication mode.

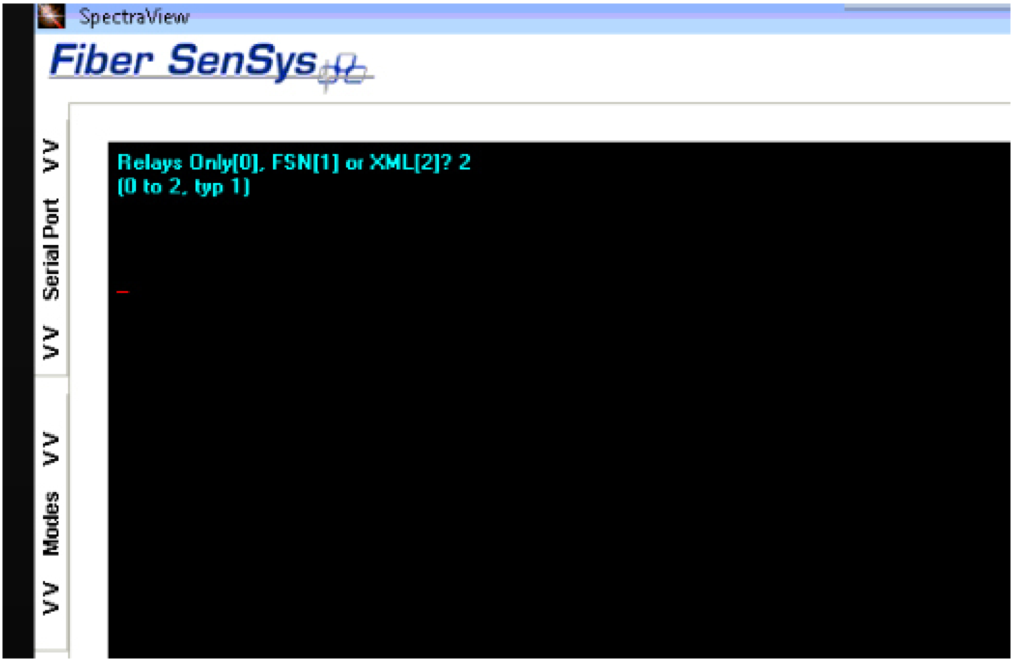


Figure 7-15: Enabling the XML communication mode in the setup menu of the device using Spectraview®

The APU is now ready for TCP/IP network operation.

Should assistance be required during this process, contact Fiber SenSys.

XML Input / Output Messages

NOTE:
The XML documents shown below, as well as others used in the remote system - APU communication process, are in full compliance with ICD-100 guidelines.

NOTE:
XML Input / Output messages are provided on the CD accompanying the APU's system components.

The flowchart in Figure 7-15 displays the systematic approach to input and output message documents to ensure that the system is communicating without interruption.

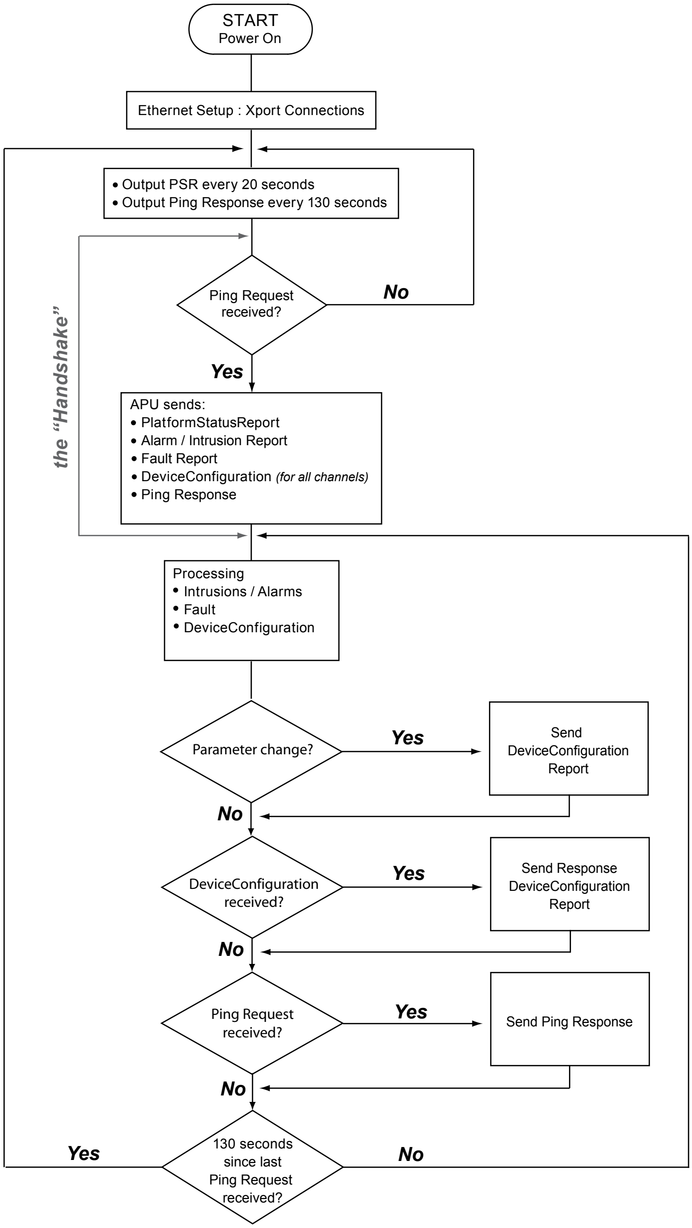


Figure 7-16: Remote system – APU communication structure

Initialization

Once the APU is powered and network connections are established, actual "dialog" with XML messages will occur. As noted in the flowchart, a Platform Status Report (PSR), Figure 7-18, is sent every 20 seconds, while a Ping Response, Figure 7-20, is sent every 130 seconds. This is done in order for the remote system to identify what is connected, and to determine whether or not to communicate with the device.

NOTE:
In order for the APU to respond to incoming messages, the **<DeviceName>** *field in the* **<DeviceIdentification>** *block must correspond with the name of the APU.*

Where the situation exists for multiple units to function within the same network, users may need to change the **<DeviceName>** for each of the units. The following procedures for changing device names, channel names and XML report intervals are as follows:

1. Launch SpectraView® and select Terminal Mode from the Modes menu, figure 7-16. This brings up the screen shown in Figure 7-17

2. Key in **SETUP** and press the **Enter** key. The following options appear:
   Select Wind[1], Comment[2], Date[3], or
   Calibrate (CAUTION!)[4] (1-4)

3. To select **Calibrate,** press the **4** key and then press the **Enter** key. The following options appear:
   Select Proc. 1[1], 2[2], Details[3], Passwords[4] or
   RESET(!)[RS] (1-4, RS)

4. Select **Passwords** by keying in **4**, which brings up the following:
   Device Name: APUNAME *(31 characters max)*

5. Key in the new name and press the **Enter** key

6. Pressing the **Enter** key again brings up:
   Channel A name: CHA *(31 characters max)*

7. Pressing the **Enter** key once again brings up the XML interval option screen, displaying the following:
   XML report interval (sec/10) = 10 (1 to 600, typ 10)

NOTE:
The FD-348R only has one channel which is channel "A"

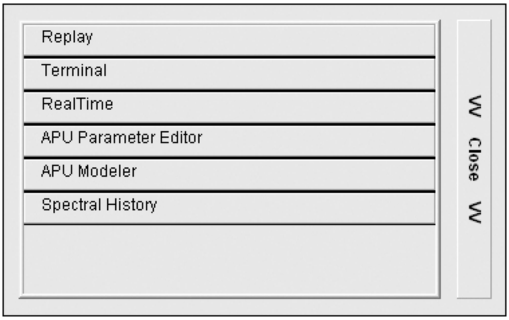


Figure 7-17: SpectraView® Modes menu

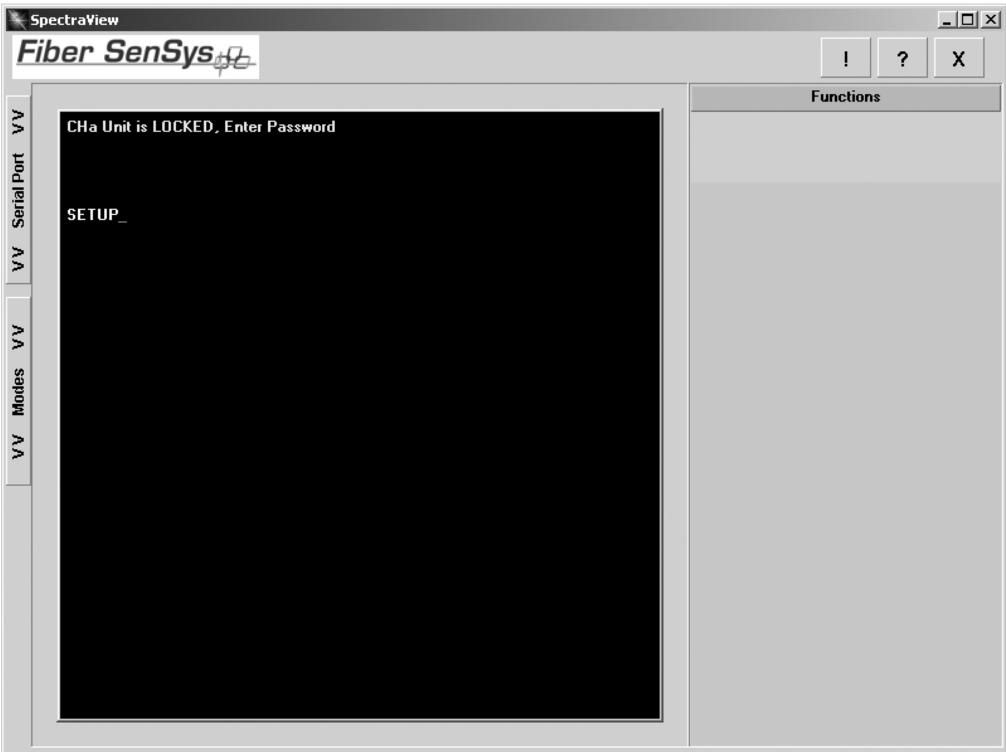


Figure 7-18: SpectraView® Terminal Mode

FD-348R_”Handshake”.xml


```xml
<?xml version="1.0" encoding="UTF-8"?>
<PlatformStatusReport>
    <PlatformIdentification>
        <DeviceName>APUNAME</DeviceName>
        <DeviceCategory>Sensor</DeviceCategory>
        <DeviceType>FD34X APU</DeviceType>
    </PlatformIdentification>
    <DeviceStatusReport>
        <DeviceIdentification>
            <DeviceName>APUNAME.CHA</DeviceName>
            <DeviceCategory>Sensor</DeviceCategory>
            <DeviceType>FD34X Channel</DeviceType>
        </DeviceIdentification>
        <Status>
            <DeviceState>Secure</DeviceState>
            <CommunicationState>OK</CommunicationState>
            <UpdateTime Zone="GMT">2007-09-21T13:43:07.000</UpdateTime>
        </Status>
    </DeviceStatusReport>
</PlatformStatusReport>

<?xml version="1.0" encoding="UTF-8"?>
<DeviceConfiguration MessageType="Report">
    <DeviceIdentification>
        <DeviceName>APUNAME.CHA</DeviceName>
        <DeviceCategory>Sensor</DeviceCategory>
        <DeviceType>FD34X Channel</DeviceType>
    </DeviceIdentification>
    <ConfigurationSetting Name="Gain" Units="None" MinimumValue="1" MaximumValue="50"
    CurrentValue="30"/>
    <ConfigurationSetting Name="Wind Reject Factor" Units="MilesPerHour" MinimumValue="20"
    MaximumValue="80" CurrentValue="50"/>
    <ConfigurationOptionBlock Name="Wind Processing" Units="None">
        <ConfigurationOption Option="Enabled" Selected="true"/>
        <ConfigurationOption Option="Disabled" Selected="false"/>
    </ConfigurationOptionBlock>
</DeviceConfiguration>

<?xml version="1.0" encoding="UTF-8"?>
<CommandMessage MessageType="Response" Status="OK">
    <DeviceIdentification>
        <DeviceName>APUNAME</DeviceName>
    </DeviceIdentification>
    <Command>
        <SimpleCommand>Ping</SimpleCommand>
    </Command>
</CommandMessage>
```


Figure 7-19: The “handshake”

FD348R_Ping_Request.xml


```
<?xml version="1.0" encoding="UTF-8"?>
<CommandMessage MessageType="Request">
   <DeviceIdentification>
      <DeviceName>APUNAME</DeviceName>
   </DeviceIdentification>
   <RequestorIdentification>
      <DeviceName>eTASS-001</DeviceName>
   </RequestorIdentification>
   <Command>
      <SimpleCommand>Ping</SimpleCommand>
   </Command>
</CommandMessage>
```


Figure 7-20: A Ping_Request.xml is answered with a Ping_Response.xml message

FD348R_Ping_Response.xml


```
<CommandMessage MessageType="Response" Status="OK">
   <DeviceIdentification>
      <DeviceName>APUNAME</DeviceName>
   </DeviceIdentification>
    <Command>
      <SimpleCommand>Ping</SimpleCommand>
   </Command>
</CommandMessage>
```


Figure 7-21: A sample Ping_Response.xml message

The Ping In message, figure 7-19, should be received by the APU within every 130 seconds. If it is not, the process is diverted back to the beginning where the system awaits the initial PSR and responding Ping Response messages. Once the Ping In is received, the APU will send the PlatformStatusReport, Intrusion / Alarm, Fault, DeviceConfiguration and Ping Response messages. This successful round of communication is known as the “handshake” and once it has taken place the "DATA" LED on the front of the APU will illuminate green and normal processing operations will continue, uninterrupted.

Events

There are 2 types of events noted by the FD348R APU:

- Intrusion or alarm
- Fault (broken fiber or hardware malfunction)

When an event occurs, whether intrusion/alarm, or fault, an ID field index, **<ID>SZ0001</ID>**, is updated. This ID field acts as an event counter.

Intrusion or Alarm

An alarm message, such as seen in figure 7-21, signals an intrusion for either Channel A.

FD348R_Alarm_CHa.xml


```
<?xml version="1.0" encoding="UTF-8"?>
<DeviceDetectionReport>
   <DeviceDetectionRecord>
      <DeviceIdentification>
         <DeviceName>APUNAME.CHA</DeviceName>
         <DeviceCategory>Sensor</DeviceCategory>
         <DeviceType>FD34X Channel</DeviceType>
      </DeviceIdentification>
      <Detection>
         <ID>SZ001</ID>
         <DetectionEvent>Intrusion</DetectionEvent>
         <UpdateTime Zone="GMT">2007-09-21T13:43:17.000</UpdateTime>
      </Detection>
    </DeviceDetectionRecord>
</DeviceDetectionReport>
```


Figure 7-22: Alarm message for the FD348R APU

The message clearly indicates the type of detection that occurred in the xml block **<DeviceDetectionReport>**. The **<DetectionEvent>** field displays the value, “Intrusion”, indicating that the cable has been sufficiently disturbed to incur an Intrusion or Alarm message.

Channel Fault

A fault may occur when, for example, a cable is bent into too tight a radius, less than 5 cm (2 inches) or in a situation where the cable has been severed.

The 2 messages, shown in figure 7-22, Fault_CHa_partA_DDR.xml, followed by Fault_CHa_partB_DSR.xml, figure 7-23, signal a fault. The tag **<DeviceDetectionReport>** identifies the type of detection, where the **<DetectionEvent>** field contains the value “Fault”. A **<DeviceStatusReport>** always follows the first message, Fault_CHa_partA_DDR.xml. The primary function of the second report is to indicate that the affected channel is in a fault state and cannot detect an intrusion any longer. The field **<DeviceState>** indicates that this channel is in fault condition and the field **<CommunicationState>** reflects the status of the “communication” through the fiber: “Fail” in this instance.

Fault_CHa_partA_DDR.xml


```
<?xml version="1.0" encoding="UTF-8"?>
<DeviceDetectionReport>
   <DeviceDetectionRecord>
      <DeviceIdentification>
         <DeviceName>APUNAME.CHA</DeviceName>
         <DeviceCategory>Sensor</DeviceCategory>
         <DeviceType>FD34X Channel</DeviceType>
      </DeviceIdentification>
      <Detection>
         <ID>SZ003</ID>
         <DetectionEvent>Fault</DetectionEvent>
         <UpdateTime Zone="GMT">2007-09-21T13:43:17.000</UpdateTime>
      </Detection>
   </DeviceDetectionRecord>
</DeviceDetectionReport>
```


Figure 7-23: Channel Fault alarm message for Fault_CHa_partA_DDR.xml

Fault_CHa_partB_DSR.xml


```
<?xml version="1.0" encoding="UTF-8"?>
<DeviceStatusReport>
      <DeviceIdentification>
            <DeviceName>APUNAME.CHA</DeviceName>
            <DeviceCategory>Sensor</DeviceCategory>
            <DeviceType>FD34X Channel</DeviceType>
      </DeviceIdentification>
      <Status>
            <DeviceState>Fault</DeviceState>
            <CommunicationState>Fail</CommunicationState>
            <UpdateTime Zone="GMT">2007-09-21T13:43:17.000</UpdateTime>
      </Status>
</DeviceStatusReport>
```


Figure 7-24: Channel Fault alarm message for Fault_CHa_partB_DSR.xml

Once the cable is straightened, the fault condition is eliminated, and the message, FaultRestore_CHa_DSR.xml, indicates the removal of the fault condition. The **<Detection>** block in the DeviceStatusReport of figure 7-24 is used to signal the detected event. The **<Status>** block before basically performs the same function, but provides more information, especially in the case of fault restore, where the zone can be seen as secure once again.

FaultRestore_CHa_partB_DSR.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<DeviceStatusReport>
   <DeviceIdentification>
      <DeviceName>APUNAME.CHA</DeviceName>
      <DeviceCategory>Sensor</DeviceCategory>
      <DeviceType>FD34X Channel</DeviceType>
   </DeviceIdentification>
   <Status>
      <DeviceState>Secure</DeviceState>
      <CommunicationState>OK</CommunicationState>
      <UpdateTime Zone="GMT">2007-09-21T13:43:27.000</UpdateTime>
   </Status>
   <Detection>
      <DetectionEvent>Other</DetectionEvent>
      <Details>Internal line fault</Details>
      <UpdateTime Zone="GMT">2007-09-21T13:43:27.000</UpdateTime>
   </Detection>
</DeviceStatusReport>
```

Figure 7-25: FaultRestore_DSR (Device Status Report)

NOTE:
The DDR signifies the tag **<DeviceDetectionReport>***, while the DSR indicates a* **<DeviceStatusReport>***.*

Adjusting Device Configuration Options

Options that can be changed via XML are found in DevConfig_CHa.xml. These are typical messages that a host system would send to an APU. It is important that the **<DeviceName>** is set to the actual name of the unit, or the unit will not respond, thereby disabling any proposed changes. Should one of the settings be out of range or a **<ConfigurationSettingName>** field is found with a name that does not exist, the unit will respond with a **<DeviceConfiguration>** response message with the message heading:

<DeviceConfiguration MessageType=”Response” RequestId=”X” Status=”Failed”>

NOTE:
The RequestId= field, displayed as X here, is dependent on the incoming RequestId.

The current settings of the APU are contained in this response message, but only the settings before the error line will be changed. Important to note is that the only other differences between an incoming message and returned message are the MessageType= value and the missing Status= parameter. Upon successful configuration adjustment, an identical message will be retuned with all the actual parameters and the message heading:

<DeviceConfiguration MessageType=”Response” RequestId=”X” Status=”OK”>

Platform Status Report

This section describes tags for the Platform Status Report document, figure 7-26, from the APU.

Events and other changes affect the status of the FD-348R APU. Whenever the state is affected, a Platform Status Document is immediately sent to notify the system and users.

Platform_Status_Report.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<PlatformStatusReport>
   <PlatformIdentification>
      <DeviceName>APUNAME</DeviceName>
      <DeviceCategory>Sensor</DeviceCategory>
      <DeviceType>FD34X APU</DeviceType>
   </PlatformIdentification>
   <DeviceStatusReport>
      <DeviceIdentification>
         <DeviceName>APUNAME.CHA</DeviceName>
         <DeviceCategory>Sensor</DeviceCategory>
         <DeviceType>FD34X Channel</DeviceType>
      </DeviceIdentification>
      <Status>
         <DeviceState>Secure</DeviceState>
         <CommunicationState>OK</CommunicationState>
         <UpdateTime Zone="GMT">2007-09-21T13:43:07.000</UpdateTime>
      </Status>
   </DeviceStatusReport>
</PlatformStatusReport>
```

Figure 7-26: PlatformStatusReport.xml document

Each status report document received from the APU contains the basic information of the schema outlined in figure 7-26. Bold text indicates fields which content may vary depending upon the APU model, type of status change and time the status changed.

<DeviceName>FD348R</DeviceName>. This tag indicates the name of the APU, and must correspond with the actual device name.

<DeviceState>Secure</DeviceState>. The status of an APU channel is indicated by this tag. Possible event states are outlined earlier in this chapter.

<UpdateTimeZone=”GMT”>2007-06-20T08:31:10.000</UpdateTime>. This tag indicates the time and time zone of the APU when the change-of-state occurred.

Device Configuration Report

Device Configuration documents, shown in Figure 7-27, are generated by the user and sent to the FD-348R via the network. Device Configuration XML documents are created using any text editor and transmitted using any program capable of accessing the proper TCP/IP port. Device software examples include the annunciator.

DC-CHa_ResponseOK.xml


```
<?xml version="1.0" encoding="UTF-8"?>
<DeviceConfiguration MessageType="Response" RequestId="1" Status="OK">
   <DeviceIdentification>
      <DeviceName>APUNAME.CHA</DeviceName>
      <DeviceCategory>Sensor</DeviceCategory>
      <DeviceType>FD34X Channel</DeviceType>
   </DeviceIdentification>
   <RequestorIdentification>
      <DeviceName>ETASS-001.SCP1</DeviceName>
   </RequestorIdentification>
   <ConfigurationSetting Name="Gain" Units="None" MinimumValue="1"
   MaximumValue="50" CurrentValue="32"/>
   <ConfigurationSetting Name="Wind Reject Factor" Units="MilesPerHour"
   MinimumValue="20" MaximumValue="80" CurrentValue="50"/>
   <ConfigurationOptionBlock Name="Wind Processing" Units="None">
      <ConfigurationOption Option="Enabled" Selected="true"/>
      <ConfigurationOption Option="Disabled" Selected="false"/>
   </ConfigurationOptionBlock>
</DeviceConfiguration>
```


Figure 7-27: Device configuration document

In the example in Figure 7-27 the FD-348R is having calibration parameters set. Device Configuration documents must include the following tags as a minimum:

DeviceIdentification. All APUs use a platform.device notation. The <DeviceName> parameter is what the platform designation is set to.

ConfigurationSetting Name. The APU parameter being changed is added to this line of text. A list of usable APU parameters and associated command syntax is found in the following section.

Device Configuration Parameters

Refer to Chapter 5 for a full description of these parameters and their associated principles of operation.

Gain			
"Gain"			
Units	**Low Limit**	**High Limit**	**Default Value**
"None"	"1"	"50"	"32"
Syntax			
<ConfigurationSettingName="Gain" Units="None” MinimumValue="1" MaximumValue="50" CurrentValue="32"/>			

Wind Reject Factor			
"Wind Reject Factor"			
Units	**Low Limit**	**High Limit**	**Default Value**
"MilesPerHour"	"20"	"80"	"50"
Syntax			
<ConfigurationSettingName="Wind Reject Factor" Units="MilesPerHour” MinimumValue="20" MaximumValue="80" CurrentValue="50"/>			

Wind Processing
"Wind Processing"
Units
"None"
Syntax
<ConfigurationOptionBlock Name="Wind Processing" Units="No ne" <ConfigurationOption Option="Enabled" Selected="true"/> <ConfigurationOption Option=”Disabled” Selected="false"/>

Fiber Security Network (FSN) Option

The FD-348R is fully compatible with the Fiber Security Network (FSN) through the RK348. The embedded capability means the APU can be integrated into the network as a component without the need for an FCA-282 or other intermediate device.

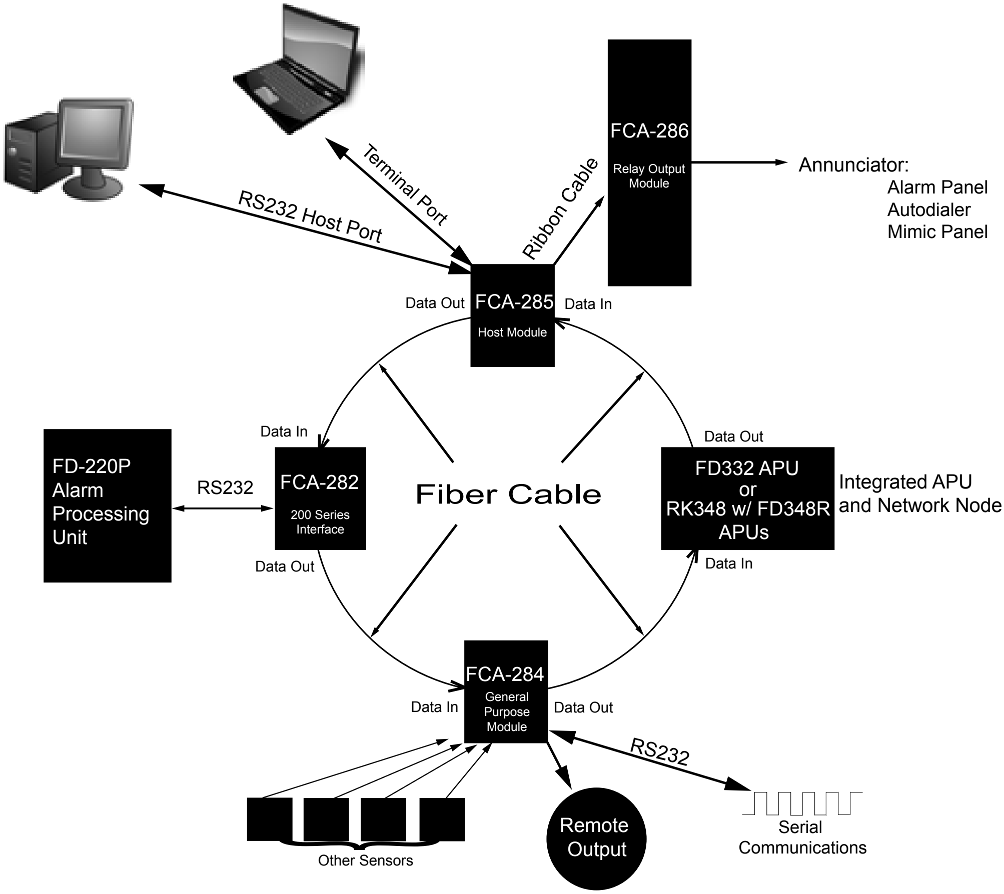


Figure 7-28: The Fiber Security Network (FSN)

The RK348 rack enclosure will arrive from the factory with two ST-type FSN connectors located on the lower rear panel of the unit (figure 7-29).

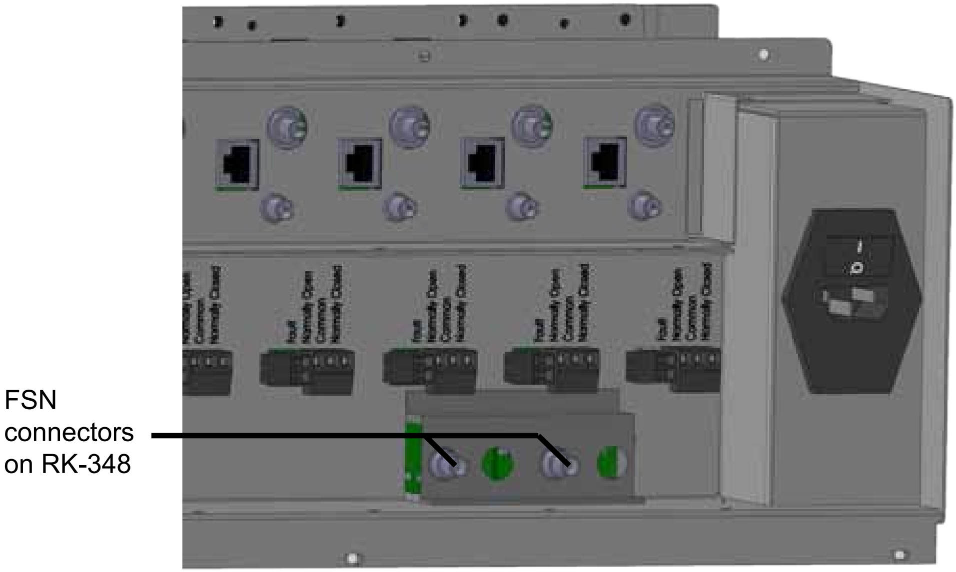


Figure 7-29: The Fiber Security Network (FSN) connectors

The dark grey connector is used for connecting data from the network to the APU. The light grey connector is used to connect data from the APU to the FSN network.

FSN Addressing Schemes

When connected to the FSN, the FD-348R APU is assigned a unique network address ("Unit 003", for example).

NOTE:
The FD-348R only has one channel which is channel "A"

For instance, if an alarm report is received from the APU, the message reads:

"Alarm Unit 003a"

This message indicates an alarm is received from Unit 003, Processor 1.

Alternately, a status report received from the device would read:

"Sensor Open 003"

This message indicates the sensor is in fault.

For more information on using the Fiber Security Network, contact Fiber SenSys or refer to the Fiber Security Network manual.

A

Connecting Conduit Sections

The flexible, protective conduit used to protect the sensor cable in fence line applications is available from Fiber SenSys in 100 meter (328 foot) sections. Creating multiple zones or protecting large areas in fence line applications usually requires more than one section of protective conduit. Thus, these separate conduit sections must be joined together as the sensor cable is pulled through.

Connecting Split Conduit (EZ-300SS)

Split conduit (Fiber SenSys part number EZ-300SS) is joined together using an *expansion joint*. Each expansion joint consists of 45.7 cm (18 inch) UV-resistant split conduit and has an inside diameter that matches the outside diameter of the sensor cable conduit. These expansion joints are available from Fiber SenSys.

To join 2 sections of split conduit together using an expansion joint:

1. Insert the first section of conduit into one end of the expansion joint. Ensure the split in the conduit is lined up with the split in the expansion joint

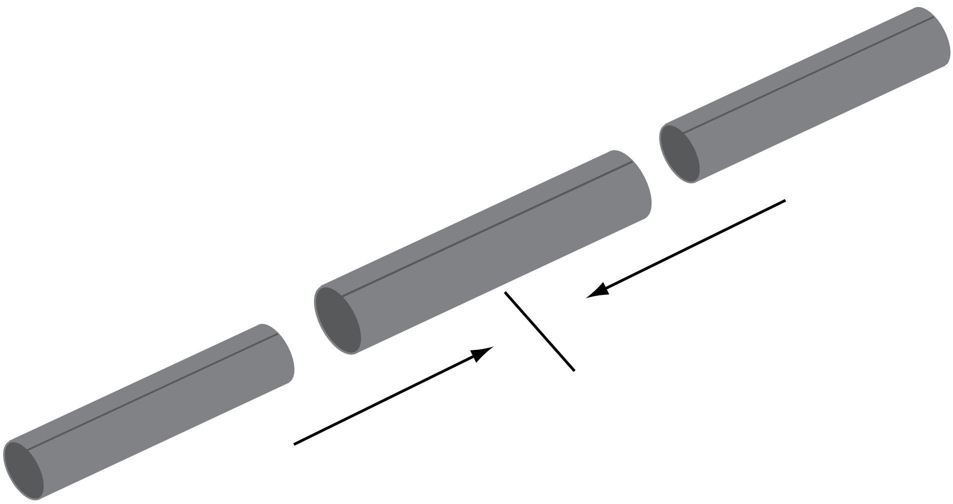


Figure A-1: Connecting split conduit sections together

2. Insert the conduit into the expansion joint far enough that it is secure. It should not be easy to pull the conduit back out

3. Repeat the process for the other second section of conduit

Connecting Non-Split Conduit (EZ-300NSS)

Non-split conduit (Fiber SenSys part number EZ-300NSS) is joined together using a barrel coupler. These barrel couplers are available from Fiber SenSys.

A barrel coupler consists of the following components:

- 2 end caps
- 2 metal lock rings
- 2 rubber washers
- 2 rubber grommets

Barrel couplers come from Fiber SenSys fully assembled and should not be disassembled.

To join 2 sections of non-split conduit together using a barrel coupler:

1. Unscrew both barrel coupler end caps several turns but do not remove them

2. Hold the first conduit section in hand and pull the pull cord out about 6 inches

NOTE:
Use care to ensure the pull cord is not lost while performing this step.

3. Slide the pull cord through the barrel coupler and tie it to the pull cord of the second conduit section

4. Using care to avoid pinching the pull cord as it rests inside the barrel coupler, push the first conduit section firmly into the barrel coupler until it comes to a stop in the center

5. Push the second conduit section into the barrel coupler using the same caution

6. Tighten both end caps to secure the conduit sections

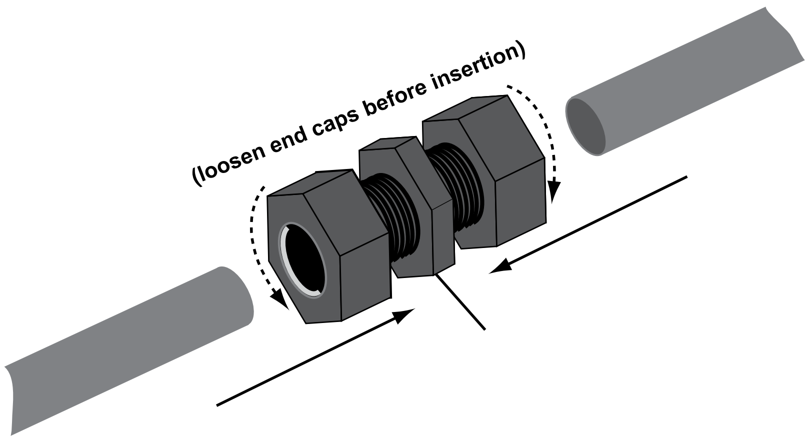


Figure A-2: Connecting non-split conduit sections together

B

TERMINATING OPTICAL FIBER

Fiber optic cable must be terminated in order to connect one sensor cable to another or to connect sensor cable to the APU. Terminating cable circumvents the need for permanently fusion splicing fiber segments together. Any cable connecting to the APU must be terminated with ST-type connectors.

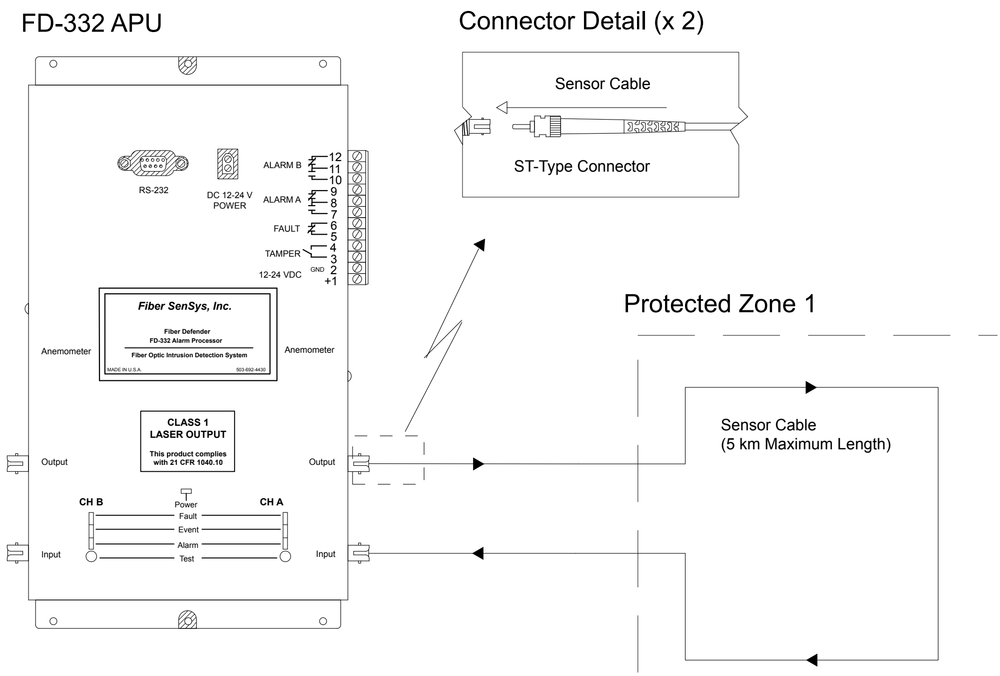


Figure B-1: Connecting fiber with ST couplers

Following termination, fiber optic cable segments can be joined together using a *feed through coupler* (also sometimes referred to as a "mating sleeve").

Whenever two fiber optic cable segments are joined together, the connected ends should always be enclosed in a protective capsule to keep the connection point clean and dry. Fiber SenSys offers the ENKT-661 Encapsulation Kit (Figure B-2) for this purpose. This encapsulation kit contains sealing gel, eliminating the need to mix and pour sealing compound as required by most other encapsulation kits. In addition, the sealing gel does not harden, allowing users to remove the connection joint at a later point in time.

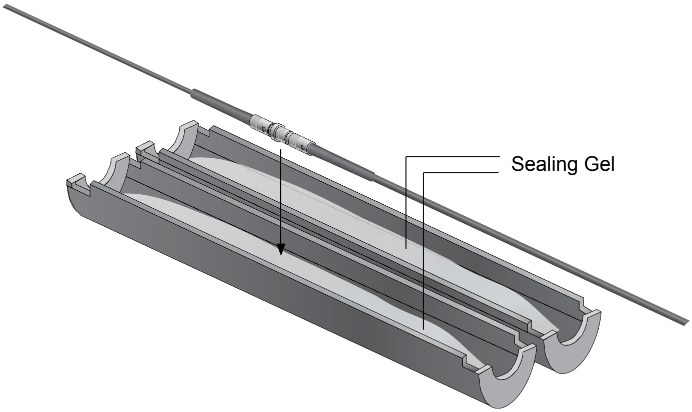


Figure B-2: ST Connectors in an ENKT-661 Encapsulation Kit

To use the ENKT-661 Encapsulation Kit:

1. Remove the capsule from the box
2. Gently lay the cable connection joint in the sealing gel in one of the capsule “clamshell” halves (Figure B-2). The joint does not have to be pressed down into the sealing gel
3. Close both clamshell halves, ensuring the cable is not pinched during the process

Use a section of UV-resistant PVC pipe to surround and couple the encapsulated joint to the rest of the conduit (for a fence line application). For a buried application, the capsule can be placed directly in the ground and buried directly with the sensor cable.

Alternatively, users may also secure the encapsulated joint in an enclosure or protective junction box.

ST-Type Connectors

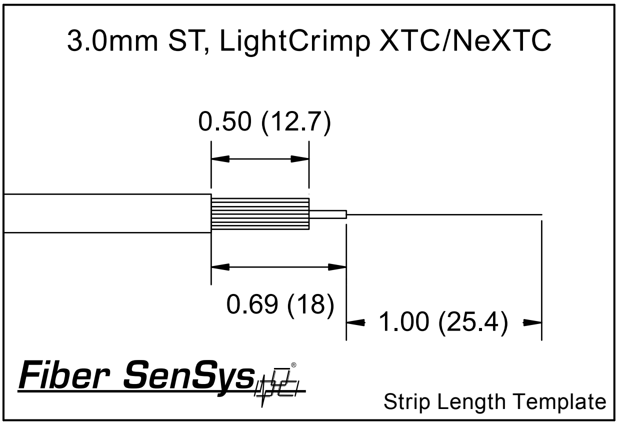
The FD-348R APU is terminated with standard ST-type connectors, requiring any cable connected to it to be terminated with ST connectors as well.

Fiber optic cable can be terminated with either crimp-on or epoxy-based ST connectors. Fiber SenSys offers a crimp-on type ST connector kit (Fiber SenSys part number CK-600). The advantage of the crimp-on type connector is it does not require an AC power supply to be on hand, as do oven-cured, epoxy-based connectors.

Generally, the procedure for terminating a fiber optic cable with crimp-on type connectors involves 7 steps:

1. Slide the strain relief and crimp sleeve over the end of the cable

2. Remove the outer jacket and trim the cable in accordance with the dimensions of the template (Figure B-3 shows sample template only)



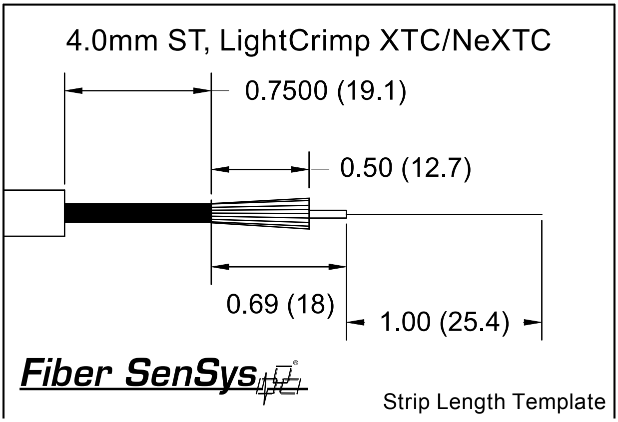


Figure B-3: Sample fiber templates

3. Insert the bare fiber of the trimmed end into the ferrule of the ST connector body, using care to prevent breaking off the unprotected fiber

4. Using a crimp tool, crimp the connector body onto the end of the fiber

5. Cleave the end of the fiber protruding from the ceramic tip of the ST connector so that the fiber is now flush with the edge of the ceramic tip

6. Polish the cleaved fiber in the ceramic tip

7. Inspect the end of the fiber and verify the core and cladding are properly polished, with no pits or jagged, sheared edges. Verify the core of the fiber properly conducts light

For detailed instructions on terminating fiber with crimp-on type ST connectors, refer to the instructions that come with the kit.

C

Product Specifications

Specifications	
Number of Channels	1 per APU 8 per RK-348
Input Power Requirements	
Voltage	120-240 VAC, 25 Watts, 50-60Hz for RK-348
Power	2.5 Watts per FD-348R APU
Communications	
Options	RS232 serial communications (standard) Fiber Security Network (FSN) compatible -- or -- IP / XML (shielded ethernet cable required for CE compliance)
Fault and Alarm Relays	
Contact Ratings	28 to 14 AWG 100 mA, 24 VDC non - inductive
Relay Defaults	Fault relay - Normally Closed (NC) Alarm relay - Normally Open or Normally Closed (NO / NC)
Environmental	
Temperature	0°C to 55°C (32°F to 131°F)
Humidity	0 to 95% non - condensing
Dimensions	
Rack-mount chassis (RK-348)	17.78 cm x 48.26 cm x 34.93 cm (7.0 in x 19.0 in x 13.75 in), H x W x D
Standards and Certifications	
RoHS, CE, FCC Part 15 Class B	

Programming / Calibration	
RS232 using laptop PC or Hand-held Calibrator	
Optical Cables	
Sensitivity	Uniform over the entire length
Maximum Insensitive Lead Length	20 km (12.4 miles) to protected zone
Maximum Sensor Cable Length	5 km (3.1 miles / 16,400 feet)
Maximum Pull Tensile Strength	300 N (60 lb)
Minimum Bend Radius	5 cm (2 inches)
IC - 3 Insensitive Lead Cable Specification	Fiber Coating Type: Acrylate Secondary Buffer Type: Hard elastomeric with aramid strength member (Kevlar®) Outer Jacket: Flame retardant polyurethane (gray) Outer Diameter: 3.6 mm
IC - 3D Duplex Insensitive Lead Cable Specification	Fiber Coating Type: Acrylate Fiber Buffer Type: Hard elastomeric with aramid strength member (Kevlar®) Fiber Jacket: Flame retardant polyurethane (gray) Outer Jacket: Polyurethane with additional aramid strength member Outer Diameter: 6.5 mm
IC - 4 Insensitive Lead Cable Specification	Fiber Coating Type: Acrylate Secondary Coating Type: Hard elastomeric with aramid strength member (Kevlar®) Outer Jacket: Exterior grade polyurethane jacket rated for direct burial (blue) Outer Diameter: 4 mm

D

WARRANTY INFORMATION

The Fiber SenSys product warranty is as follows:

A. Fiber SenSys warrants the Fiber Defender Model FD-348R to be free from electrical and mechanical defects in materials and workmanship for a period of two years from the date of shipment. This warranty does not apply to defects in the product caused by abuse, misuse, accident, casualty, alteration, negligent use of current or voltages other than those specified by Fiber SenSys, application, or installation not in accordance with published instruction manuals or repair not authorized by Fiber SenSys. This warranty is made in lieu of any other warranty either expressed or implied.

B. All returns will be tested to verify customer claims of non-compliance with the warranty described herein. If non-compliance is verified and is not due to customer abuse or the other exceptions described previously, Fiber SenSys will, at its option, repair or replace the FD-348R returned to it, freight prepaid. Contact Fiber SenSys and obtain an RMA number prior to returning a product. Fiber SenSys will pay for ground return freight charges only. The customer must pay for any other return shipping options.

C. Fiber SenSys liability is limited to the repair or replacement of the product only, and not the costs of installation, removal or damage to user’s property or other liabilities. If Fiber SenSys is unable to repair or replace a non-conforming product, it may offer a refund of the amount paid to Fiber SenSys for such product in full satisfaction of its warranty obligation. Maximum liability to Fiber SenSys is the cost of the product.

INDEX

A

B

C

D

E

F

S

T