Architectural and Engineering Specification for a Fiber Optic Buried Intrusion Detection System

FiberPatrol™ FP6100X

This document is intended to provide performance specifications and operational requirements for the FiberPatrol FP6100X fiber optic buried intrusion detection system. It is written in a generic format. These specifications may be copied verbatim to form a generic procurement specification.

Part 1 General....4
1.1 System Summary....4
1.2 Submittals....4
1.3 Qualifications....4
1.4 Spares....4
1.5 Warranty....4
1.6 References....5
Part 2 Products....6
2.1 Intrusion Detection System....6
2.2 Manufacturers....6
2.3 Regulatory Requirements....6
2.4 Mechanical Requirements....6
2.5 Environmental Requirements....7
2.6 Reliability and Maintenance Requirements....7
2.7 Electrical Requirements....7
2.8 Detection Capabilities....8
2.9 Cable cut response....10
2.10 Installation and Configuration Capabilities....10
2.11 Networking Capabilities....10
2.12 Event Management....11
2.13 Access Control....12
Part 3 Execution....13
3.1 Site Assessment....13
3.2 System Installation....13
3.1 System Calibration....13
3.2 Training....13

PART 1 GENERAL

1.1 System Summary

The contractor shall install a ranging fiber optic intrusion detection system. When the sensor cable is buried, the system shall provide covert detection of intruders, vehicles, and tunneling. When the sensor cable is attached to a fence, the system shall detect any attempt to cut, climb, lift, or dismantle the fence.

The detection sensors shall consist of fiber optic cables. The cables shall connect to a signal processing module that detects and locates attempted intrusions by analyzing the changes in reflected optical energy that occur as a result of minute vibrations in the sensor cables.

If a sensor cable is cut, the system shall retain detection and locating capabilities in the portion(s) of the sensor cable that remain connected to the sensor unit. When using a single sensor unit, it shall be possible to install the system in a cut-immune configuration such that the system remains fully operational after a single cable cut.

The system shall be capable of being integrated into the facility's Security Management System.

1.2 Submittals

A. Contractor submittals to the facility owner shall include the following as a minimum:

1. Site conditions report as per article 3.1
2. Configuration and calibration settings for the system after installation and calibration are complete as per article 3.3
3. All manufacturer-supplied software required for the calibration and operation of the system
4. Documentation providing system operation and maintenance procedures.

1.3 Qualifications

A. The manufacturer of the system shall have a minimum of five (5) years of experience in the last 10 years of the manufacture and successful implementation of similar systems.

1.4 Spares

A. The contractor shall deliver to the facility owner spare system components.

B. For each system component, spares consisting of at least one unit or 10% of the number that comprise the system, whichever is greater, shall be provided.

1.5 Warranty

A. The product shall be under warranty for a minimum of three years from the date of purchase.

B. The supplier shall make available replacement components, parts or assemblies for a minimum of 10 years from the date of purchase.

1.6 References

A. Abbreviations and acronyms: The following acronyms and abbreviations are used in this document:

1. MTBF: Mean Time Between Failures
2. MTTR: Mean Time To Replace
3. Pd: Probability of Detection
4. NAR: Nuisance Alarm Rate.

B. Reference Standards: The following regulatory and industry standards are referenced in this document:

1. Federal Communications Commission: FCC CFR Part 15, Subpart B requirements for Class A devices.
2. Conformité Européenne (CE).

PART 2 PRODUCTS

2.1 Intrusion Detection System

A. The contractor shall supply a ranging fiber optic intrusion detection system.

B. When the sensor cable is buried, the system shall provide covert detection of intruders, vehicles, and tunneling.

C. When the sensor cable is attached to a fence, the system shall detect any attempt to cut, climb, lift, or dismantle the fence.

D. The system shall support a cut-immune deployment configuration that enables the system's detection and locating capabilities to remain fully operational in the event of a sensor cable cut.

2.2 Manufacturers

A. The FiberPatrol™ FP6100X system from Senstar Corporation (www.senstar.com) meets the requirements stated in this document.

2.3 Regulatory Requirements

A. The system shall comply with the following regulations:

1. FCC 47 CFR Part 15, Subpart B requirements for Class A devices
2. CE

2.4 Mechanical Requirements

A. Sensor cable:

1. The sensor cable shall incorporate single-mode optical fibers.
2. The system shall require only a single fiber to provide standard non-redundant functionality.
3. The sensor cable shall have the option to be encased in an armor jacket, for use in areas that have a high potential of physical damage to the cable.
4. The sensor cable shall have a minimum bend radius no greater than 15 cm (6.0 inches).
5. The system shall not require that the sensor cable be installed in a conduit.
6. The sensor cable shall be able to include additional, unused fibers for use by other equipment (such as for data or video communications).
7. The system shall be capable of being used with pre-existing cable providing the optical fibers of the pre-existing cable meet attenuation and reflective event guidelines as set down by the system manufacturer.

B. Sensor unit equipment:

1. The system shall not require any electronic devices, communications cabling, or grounding points to be installed outdoors.

2. All electronic components shall be rack-mountable in an indoor, equipment room environment.
3. The indoor system components shall be designed for standard 19-inch wide rack.
4. The system shall provide the option for a slide-out monitor and keyboard that enables local console access to the system.
5. The system shall include a fiber optic patch panel for interfacing the sensor cable to the processor and controller modules.

2.5 Environmental Requirements

A. The sensor cables shall withstand operation in temperatures from –40°C to 70°C (–40°F to 158°F) and a relative humidity of 0 to 100% (condensing) without performance degradation.

B. The sensor unit components shall be designed for indoor use and meet the following requirements:

1. Temperature:
   a. Operating: 10°C to 35°C (50°F to 95°F)
   b. Storage: –20°C to 70°C (–4°F to 158°F)
2. Humidity:
   a. Operating: 20% to 80% (relative, non-condensing)
   b. Shipping and storage: 5% to 85% (relative, non-condensing)

2.6 Reliability and Maintenance Requirements

A. Sensor cables: The sensor cables shall provide a nominal service life of 20 years, excluding damage caused by non-environmental forces.

B. Sensor unit:

1. The sensor unit modules shall have a predicted mean time between failures (MTBF) of greater than 87,000 hours.
2. The sensor unit shall be capable of performing internal self-diagnostic tests of the internal circuitry, cable continuity, and detection processing.
3. The sensor unit software shall be field-upgradeable, either locally via a USB connection or over the network.

2.7 Electrical Requirements

A. Each sensor unit shall meet the following electrical requirements:

1. Input power: 100 to 240 VAC, 50/60 Hz
2. Power consumption: Less than 450W

B. Backup power: The sensor unit shall be capable of being powered from a third-party uninterruptable power supply (UPS) or standby generator.

C. The sensor cable shall include no conductive elements.

D. The sensor cable shall be intrinsically safe within explosive atmospheres.

E. The sensor cable shall be completely immune to all forms of electromagnetic energy from radio communications, radar, electrical power transmission equipment and lightning.

F. The system shall not require any outdoor power or grounding connections.

2.8 Detection Capabilities

A. The system shall provide two independent sensing channels.

B. When the two sensing channels are used independently the system shall be able to detect and locate intrusions over the following cable distances:

1. Up to 80 km (49.7 mi) for fiber attenuation (installed) of 0.25 dB/km or less @ 1550 nm.
2. Up to 72 km (45 mi) for fiber attenuation (installed) of 0.28 dB/km or less at 1550 nm.

C. When the two sensing channels are deployed in the cut-immune configuration the system shall be able to detect and locate intrusions over the following cable distances:

1. Up to 40 km (24.85 mi) for fiber attenuation (installed) of 0.25 dB/km or less @ 1550 nm.
2. Up to 36 km (22.37 mi) for fiber attenuation (installed) of 0.28 dB/km or less at 1550 nm.

D. The sensor unit shall have the following detection capabilities:

1. Process the signal from a buried sensor cable to detect the following intrusion types at the given typical distances from the sensor cable:
    a. Hand and machine digging and tunneling at distances up to 20 m (66 ft) from the sensor cable in any direction
    b. Person walking normally at from 1 to 5 m (3 to 16 ft)
    c. Person running at from 5 to 10 m (16 to 33 ft)
    d. Person crawling slowly at 1 m (3 ft)
    e. Light vehicle moving at from 3 to 10 m (10 to 33 ft)
    f. Heavy vehicle moving at from 10 to 20 m (33 to 66 ft)
    g. Heavy vehicle engine running at from 5 to 10 m (16 to 33 fit)
    h. Manual digging (pickaxe, etc.) at from 10 to 20 m (33 to 66 ft)

2. Process the signal from a fence-mounted sensor cable to detect intruders attempting to breach the perimeter fence by cutting, climbing, lifting, or dismantling the fence.
3. Locate the position of a detected intrusion within 5 m (16 feet) or less at least 95% of the time for detectable intrusions in an otherwise acoustically quiet environment.
4. Detect multiple simultaneous intrusions, when each intrusion attempt is separated by a sensor cable distance greater than 45 m (150 feet).
5. Support up to 1,140 virtual detection zones.
6. Be capable of detecting and locating a sensor cable cut to within 30 m (100 feet).
7. Utilize adaptive algorithms in the detection process to optimally discriminate between actual intrusions and environmental activity.

E. Intrusion detection performance:

1. The probability of detection (Pd) for a typical intrusion attempt shall be 95% with a 95% confidence factor, when the system is installed in accordance with the manufacturer's directions.
2. False alarm rate: The maximum rate for alarms generated by the internal electronic processes of the processors (cables excluded) shall be less than one per km per month typical, averaged over the total length of the system.
3. Nuisance (environmental) alarms:
    a. The system when calibrated according to manufacturer's guidelines shall not suffer nuisance alarms from any of the following sources:
        i. Temperature changes
        ii. Sunrise/sunset
        iii. Acoustic or magnetic effects
        iv. Snow
        v. Fog
        vi. Wind
        vii. Rain and hail
        viii. Sandstorms
    b. The system shall utilize advanced processing and ambient compensation to minimize the probability of nuisance alarms from the following sources:
        i. Motion of nearby objects or vegetation
        ii. Motion of surface or ground water
        iii. Seismic vibration caused by nearby vehicular traffic

iv. Seismic vibration caused by nearby rail traffic

4. Once an intrusion event is detected, the system shall be capable of reporting the alarm to the Security Management System within one second.

2.9 Cable cut response

A. The system shall be capable of detecting and locating a sensor cable cut.

B. The cut location shall be determined and reported with an absolute accuracy of equal to or less than 30 meters (100 feet).

C. In the event of a sensor cable cut, the system shall retain detection and location ability in the portion(s) of the sensor cable that remain connected to the system sensor unit.

2.10 Installation and Configuration Capabilities

A. The system shall have the following characteristics, as a minimum:

1. The sensor cable shall be capable of being buried directly without needing to be put in a conduit.

2. It shall be possible to disable detection along sections of the cable where intrusion detection is not required (i.e., lead-in sections).

B. The system shall support a cut-immune deployment configuration in which both sides of the sensor cable continue to detect interference events after a cut occurs.

C. The system shall support the following configuration and calibration features:

1. A Windows-based graphical user interface (GUI), accessible locally or via Windows Remote Desktop.

2. Configuration and calibration settings shall be capable of being stored in a computer file for record keeping purposes and available for reuse when configuring additional or replacement processors.

2.11 Networking Capabilities

A. Network manager tools: The system's network management software shall provide the following tools to facilitate system commissioning and trouble-shooting:

1. System status tool that provides a visual display of the status of all processors in the system

2. System event log tool that provides a searchable log of system events.

B. The processors shall support dual Gigabit Ethernet on RJ-45 connectors.

C. Network management:

1. The system shall include network management software to manage the communications over the sensor network. The network management software shall be capable of running on a standard Windows PC as well as on the sensor unit itself and be accessible via Windows Remote Desktop.

2. The system's network management software shall provide a TCP/IP-based interface for communicating alarm, status, and configuration data to and from security management systems. The system supplier shall furnish complete documentation of this interface to facilitate integration with security management systems.

2.12 Event Management

A. The system shall provide a local PC-based operator interface with graphical alarm annunciation at the sensor unit.

B. The system shall provide access to the following information and functionality when in a local or networked configuration:

1. A user-configurable image depicting the protected site with a schematic perimeter overlay.
2. Hardware monitoring and control
3. Event detection and alarm generation (including flashing notification message, location marker, and audible alert)
4. Basic alarm management
5. Event and alarm logging
6. Detection zone definition and configuration
7. Adjustment of detection parameters

C. The system shall support the following alarm management functions:

1. Maintain complete information on all alarms for 24 hours or until the alarm is cleared.
2. Alarms shall be cleared by local or remote operator or automatically in 24 hours after alarm generation.
3. Until cleared, the alarm information shall be compiled in a scrollable multi-column table.
4. The maintained information shall include:
    a. Unique alarm ID number
    b. Time label
    c. Event duration
    d. Event status
    e. Event strength
    f. Event location.
5. The Operator shall be able to:
    a. Select any of the alarms from the list.

b. Enter text notes regarding the cause of the alarm and the mitigation measures.

c. Clear the alarm.

6. Operator notes as well as the alarm clearing event shall be recorded in the event log.

7. Alarm location Format:

a. The primary format of the alarm location shall be the linear position along the sensor cable.

b. It shall be possible to express the alarm location in either meters or feet.

c. Secondary location formats shall be derived from the primary measure using appropriate calibration tables.

d. Secondary location formats shall require corresponding mapping of the perimeter fence line.

e. It shall be possible to provide secondary alarm location formats including:

i. Software-defined zone numbers

ii. Latitude and longitude (GPS) coordinates

8. Event logging:

a. The system shall maintain and display an event log, including alarms, system notifications, and user actions.

b. The logs shall be periodically saved to the hard drive.

c. A new set of log files shall be generated every 24 hours at midnight.

2.13 Access Control

A. The system shall require the entry of a valid password at start-up and shutdown.

B. The system shall divide user access into to three security levels:

1. Operator level for routine operation

2. Supervisor level for advanced system monitoring, configuration, and troubleshooting

3. Installer level for advanced configuration and troubleshooting.

PART 3 EXECUTION

3.1 Site Assessment

A. Before installation begins, the installation contractor shall provide a report to the facility's owner documenting any site conditions that may prevent the system from operating satisfactorily.

3.2 System Installation

A. The system shall be installed in accordance with the manufacturer's recommended procedures as defined in the manufacturer's documentation for the system.

3.3 System Calibration

A. The installation contractor shall calibrate the system in accordance with the manufacturer's recommended procedures as defined in the manufacturer's Product Guide.

B. The installation contractor shall submit to the owner the calibration and configuration settings for the system.

3.4 Training

A. The installation contractor or vendor shall train the owner's maintenance personnel in the calibration and system maintenance procedures as given in the manufacturer's product documentation.