

**Architectural and Engineering Specification for a
Fiber Optic System for Perimeter Intrusion, Pipeline TPI, and
Conduit TPI Detection**

FiberPatrol® FP1150

This document is intended to provide performance specifications and operational requirements for the FiberPatrol FP1150 system for perimeter intrusion, pipeline TPI, and conduit TPI detection. It is written in a generic format. These specifications may be copied verbatim to form a generic procurement specification.

Senstar and the Senstar logo are registered trademarks of Senstar Corporation. FiberPatrol and Silver Network are trademarks of Senstar Corporation. The information in this document is subject to change without notice. Senstar reserves the right to make changes to product design or manufacturing methods, as engineering progresses, or as other circumstances warrant.

Copyright © 2023. Senstar Corporation. All rights reserved.

PART 1	GENERAL	4
1.1	System Summary.....	4
1.2	Submittals	4
1.3	Qualifications	5
1.4	Spares.....	5
1.5	Warranty	6
1.6	References.....	6
PART 2	PRODUCTS.....	7
2.1	Precision-Locating Fiber Optic Detection System.....	7
2.2	Manufacturers	7
2.3	Regulatory Requirements.....	7
2.4	Mechanical Requirements.....	7
2.5	Environmental Requirements	8
2.6	Reliability and Redundancy Requirements	9
2.7	Electrical Requirements	9
2.8	Detection Capabilities – Classification Algorithms.....	10
2.9	Detection Capabilities – Fence Detection.....	10
2.10	Detection Capabilities – Wall-Top Detection.....	12
2.11	Detection Capabilities – Buried Cable Perimeter Intrusion Detection.....	13
2.12	Detection Capabilities – Pipeline TPI Detection.....	15
2.13	Detection Capabilities – Data Conduit TPI Detection.....	17
2.14	Mixing of Installation Types.....	19
2.15	Cable cut response.....	19
2.16	Installation and Configuration Capabilities.....	20
2.17	System-level Cybersecurity Provisions.....	20
2.18	TCP/IP-Based Integration Interface.....	20
2.19	Access Control.....	21
PART 3	EXECUTION	22
3.1	Site Assessment.....	22
3.2	System Installation	22
3.3	System Calibration	22
3.4	Training	22

PART 1 GENERAL

1.1 System Summary

The contractor shall install a precision locating fiber optic sensor.

When the sensor cable is fence-mounted for perimeter intrusion detection the system shall detect and locate intruders that attempt to cut, climb, or lift the fence fabric.

When the sensor cable is installed on wall-tops for perimeter intrusion detection the system shall detect any impingement on the sensor cable by an intruder or by a climbing aid such as a rope or ladder.

When the sensor cable is buried for perimeter intrusion detection the system shall detect the footsteps of an intruder walking over or near the sensor cable.

When the sensor cable is buried along a pipeline right-of-way the system shall detect third-party interference events that threaten the integrity of the pipeline such as hot tapping or nearby manual digging, machine digging, or presence of heavy equipment.

When the sensor cable is installed inside or near a telecommunications conduit or when the system's sensing fibers are integral to a telecommunications cable, the system shall detect third-party interference events that threaten the integrity of the telecommunications cables such as fiber tapping or nearby manual digging, machine digging, or presence of heavy equipment.

The detection sensors shall consist of fiber optic cables. Fibers within the cable shall connect to a signal processing module that detects and locates attempted intrusions by analyzing the changes in reflected 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.

To provide optimum performance and situational awareness the system shall provide an extensive set of classification algorithms, including at least fence-cut, fence-climb, footstep, manual digging, machine digging, vehicle engine, and vehicle motion.

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' 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 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 repair or make equivalent parts available for a minimum of 10 years from the date of purchase, based on a site's original equipment ship date.

1.6 References

- A. Abbreviations and acronyms: The following acronyms and abbreviations are used in this document:
 - 1. PIDS: Perimeter Intrusion Detection System
 - 2. MTBF: Mean Time Between Failures
 - 3. MTTR: Mean Time To Replace
 - 4. OTDR: Optical Time-Domain Reflectometer
 - 5. PD: Probability of Detection
 - 6. TPI: Third-Party Interference
- 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 Precision-Locating Fiber Optic Detection System

- A. The contractor shall supply a precision locating fiber optic detection system capable of perimeter intrusion detection, pipeline TPI detection, and data conduit TPI detection.
- B. 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® FP1150 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 regulatory requirements:
 - 1. FCC 47 CFR Part 15, Subpart B requirements for Class A devices
 - 2. CE
 - 3. REACH (Registration, Evaluation, Authorization & Restriction of Chemicals)
 - 4. Safety (IEC 62368-1:2018)

2.4 Mechanical Requirements

- A. Sensor cable:
 - 1. 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.
 - 2. The sensor cable shall have a minimum bend radius no greater than 15 cm (6.0 in).
 - 3. When used in fence-mounted perimeter intrusion detection applications, the sensor cable shall be affixed to the facility's fence through the use of UV-resistant plastic or metal cable ties.
 - 4. When used in fence-mounted perimeter intrusion detection applications, the sensor cable shall not require a cable conduit to be installed along the fence perimeter to protect the cable.
 - 5. The sensor cable shall be able to include additional, unused fibers for use by other equipment (such as for data or video communications).

6. The sensor cable shall not require conductive elements.
 7. The sensor cable shall be intrinsically safe within explosive atmospheres.
 8. It shall be possible to use sensor cable with fire ratings such as LSZH, fire-retardant, and fire resistant.
 9. The sensor cable shall be completely immune to all forms of electromagnetic energy from radio communications, radar, electrical power transmission equipment and lightning.
 10. The system shall be capable of being used with standard commercially-available fiber optic cable that meets the necessary attenuation and single-event loss requirements.
- B. Sensor unit equipment:
1. The system shall not require any active devices or processor modules to be installed outdoors.
 2. All active components shall be rack-mountable in an indoor equipment room environment
 3. The indoor system components shall be designed for a 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.

2.5 Environmental Requirements

- A. The sensor cables shall be able to operate 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: 0 to 50°C (32 to 122°F)
 - b. Storage: -20 to 70°C (-4 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 Redundancy Requirements

- A. Sensor cables: The sensor cables shall have 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. System mass storage will be implemented with a minimum of two field-replaceable solid-state drives in a RAID1 configuration that are installed inside the sensor unit.
 - 3. The sensor unit shall incorporate two redundant field-replaceable power supplies.
 - 4. The sensor unit shall incorporate dual Gigabit Ethernet interfaces.
 - 5. The sensor unit shall be capable of performing continuous self-diagnostic tests of the internal circuitry, software operation, and cable continuity and be capable of reporting any faults detected.
 - 6. The sensor unit software shall be field-upgradeable.

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 200W
- 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 system shall not require any outdoor power or grounding connections.

2.8 Detection Capabilities – Classification Algorithms

- A. To provide optimum Probability of Detection vs. Nuisance Alarm Rate performance and situational awareness the system shall incorporate classification algorithms:
 - 1. for fence applications, separate fence-climb and fence-cut detection algorithms shall be provided to enable the detection of stealthy fence cutting attempts without compromising NAR performance
 - 2. for buried applications – footstep, manual digging, machine digging, vehicle engine, and vehicle motion classification algorithms shall be provided

2.9 **Detection Capabilities – Fence Detection**

- A. The sensor shall consist of fiber optic cable that is attached to the fence along the full length to be protected.
- B. The system shall provide two independent sensing channels.
- C. The system shall be able to detect and locate intrusions over a cable distance of up to 80 km (49.7 mi) when the two sensing channels are used independently.
- D. The system shall be able to detect and locate intrusions over a cable distance of up to 40 km (24.8 mi) when the system is deployed in the cut-immune configuration.
- E. The sensor unit shall have the following detection capabilities:
 - 1. Process the signal from the sensor cable to detect intruders attempting to breach the perimeter fence by cutting, climbing, or lifting the fence fabric
 - 2. Locate the position of a detected intrusion within 4 m (13 ft) or less at least 95% of the time.
 - 3. Detect multiple simultaneous intrusions, when each intrusion attempt is separated by a sensor cable distance greater than 30 m (100 ft) when deployed in the cut-immune configuration or 15 m (50 ft) when deployed in the non-cut immune configuration.
 - 4. Support up to 1440 virtual detection zones.
 - 5. Be capable of being calibrated to equalize the effective sensitivity on different types and conditions of metal fencing.
 - 6. Utilize adaptive algorithms in the detection process to optimally discriminate between actual intrusions and environmental activity.
 - 7. Provide separate detection settings for fence climb and fence cut.
- F. Intrusion detection performance:
 - 1. The probability of detection (Pd) of an intruder cutting the fence, lifting the fence fabric, or climbing unaided over the fence, shall be 95% with a 95% confidence factor when the system is installed in accordance with the manufacturer's directions on a high-quality fence.
 - 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 zone per year, averaged over the total number of zones in 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:

- .1 Temperature changes
 - .2 Motion of nearby objects or vegetation that are not striking the fence
 - .3 Motion of surface or ground water
 - .4 Sunrise/sunset
 - .5 Acoustic or magnetic effects
 - .6 Snow
 - .7 Fog
 - .8 Seismic vibration caused by nearby vehicular traffic
 - .9 Seismic vibration caused by nearby rail traffic when the fence is further than 5 m (16 ft) from the rails.
 - b. The system shall utilize advanced processing and an environmental compensation algorithm to minimize the probability of nuisance alarms from the following sources:
 - .1 Wind
 - .2 Rain and hail
 - .3 Sandstorms
- G. Time to detection:
- 1. The system shall be capable of generating an alarm within one second from the onset of an attempted breach that involves aggressive contact with the fence (such as one attempted by quickclimbing).
 - 2. Other detected intrusion attempts shall be reported no later than one second after the breach is completed.
- H. Fence compatibility:
- 1. The system shall support installation on the following types of metal fencing:
 - a. Chain-link
 - b. Expanded metal mesh
 - c. Welded mesh
 - d. Concertina and/or razor wire
 - e. Vinyl-coated chain-link
 - f. Palisade-style fences
 - 2. The system shall perform as specified in single-pass installations on high-

quality chain-link fences of up to 4.3 m (14 ft) in height

3. It shall be possible to use multiple passes of sensor cable to obtain the specified detection performance for fences of any height.
4. The manufacturer shall provide installation guidelines regarding the type and height of fences that can be protected with one, two, and multiple passes of sensor cable.
5. Gate compatibility: The sensor cable shall be capable of being installed on swinging gates.

2.10 Detection Capabilities – Wall-Top Detection

- A. The sensor shall consist of fiber optic cable that is attached to the top corner of the wall along the full length to be protected.
- B. The system shall provide two independent sensing channels.
- C. The system shall be able to detect and locate intrusions over a cable distance of up to 80 km (49.7 mi) when the two sensing channels are used independently.
- D. The system shall be able to detect and locate intrusions over a cable distance of up to 40 km (24.8 mi) when the system is deployed in the cut-immune configuration.
- E. The sensor unit shall have the following detection capabilities:
 1. Process the signal from the sensor cable to detect any impingement on the sensor cable by an intruder or by a climbing aid such as a rope or ladder.
 2. Locate the position of a detected intrusion within 4.0 m (13 ft) or less at least 95% of the time.
 3. Detect multiple simultaneous intrusions, when each intrusion attempt is separated by a sensor cable distance greater than 45 m (150 ft) when deployed in the cut-immune configuration or 30 m (100 ft) when deployed in the non-cut immune configuration.
 4. Support up to 1440 virtual detection zones.
 5. Utilize adaptive algorithms in the detection process to optimally discriminate between actual intrusions and environmental activity.
- F. Intrusion detection performance:
 1. 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 zone per year, averaged over the total number of zones in the system.
 2. Nuisance (environmental) alarms:

- a. The system when calibrated according to manufacturer's guidelines shall not suffer nuisance alarms from any of the following sources:
 - .1 Temperature changes
 - .2 Motion of nearby objects or vegetation that are not striking the cable
 - .3 Motion of surface or ground water
 - .4 Sunrise/sunset
 - .5 Acoustic or magnetic effects
 - .6 Snow
 - .7 Fog
 - .8 Seismic vibration caused by nearby vehicular traffic
 - .9 Seismic vibration caused by nearby rail traffic when the wall is further than 5 m (16 ft) from the rails.
 - b. The system shall utilize advanced processing and an environmental compensation algorithm to minimize the probability of nuisance alarms from the following sources:
 - .1 Wind
 - .2 Rain and hail
 - .3 Sandstorms
- G. Time to detection:
- 1. The system shall be capable of generating an alarm within one second from the onset of an attempted breach that involves aggressive contact with the sensor cable (such as one attempted by quick climbing).
 - 2. Other detected intrusion attempts shall be reported no later than one second after the breach is completed.

2.11 Detection Capabilities – Buried Cable Perimeter Intrusion Detection

- A. The sensor shall consist of fiber optic cable that is buried along the full length to be protected.
- B. The system shall provide two independent sensing channels.
- C. The system shall be able to detect and locate intrusions over a cable distance of up to 80 km (49.7 mi) when the two sensing channels are used independently.
- D. The system shall be able to detect and locate intrusions over a cable distance of up to 40 km (24.8 mi) when the system is deployed in the cut-immune configuration.

- E. The sensor unit shall have the following detection capabilities:
1. Process the signal from the sensor cable to detect the footsteps of an intruder and nearby manual or machine digging.
 2. Locate the position of a detected intrusion within 4.0 m (13 ft) or less at least 95% of the time.
 3. Detect multiple simultaneous intrusions, when each intrusion attempt is separated by a sensor cable distance greater than 30 m (100 ft) when deployed in the cut-immune configuration or 15 m (50 ft) when deployed in the non-cut immune configuration.
 4. Support up to 1440 virtual detection zones.
 5. Be capable of being calibrated to equalize the effective sensitivity for different burial conditions.
 6. Utilize adaptive algorithms in the detection process to optimally discriminate between actual intrusions and environmental activity.
- F. Intrusion detection performance:
1. The typical detection range for different intrusion types shall be as given in the table below. It shall be recognized that actual performance will depend on specific site conditions and can increase or decrease considerably from these typical values.

INTRUSION TYPE	TYPICAL DISTANCE FROM CABLE FOR DETECTION
Human normal walking	1 to 5 m (3 to 16 ft)
Human running	5 to 10 m (16 to 33 ft)
Human crawling slowly	1 m (3 ft)
Light vehicle moving	3 to 10 m (10 to 33 ft)
Heavy vehicle moving	10 to 20 m (33 to 66 ft)
Heavy vehicle engine running	5 to 10 m (16 to 33 ft)
Manual digging (pickaxe)	10 to 20 m (33 to 66 ft)
Tunnel digging	20 m (66 ft)

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 zone per year, averaged over the total number of zones in 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:
 - .1 Temperature changes
 - .2 Sunrise/sunset
 - .3 Acoustic or magnetic effects
 - .4 Snow
 - .5 Fog
 - b. The system shall utilize advanced processing and an environmental compensation algorithm to minimize the probability of nuisance alarms from the following sources:
 - .1 Wind
 - .2 Rain and hail
 - .3 Sandstorms
 - .4 Motion of nearby objects or vegetation
 - .5 Motion of surface or ground water
 - .6 Seismic vibration caused by nearby vehicular traffic
- G. Time to detection:
 1. Detected intrusion attempts shall be reported no later than one second after the breach is completed.

2.12 Detection Capabilities – Pipeline TPI Detection

- A. The sensor shall consist of fiber optic cable that is buried along the full length of pipeline right-of-way to be protected.
- B. The system shall provide two independent sensing channels.
- C. The system shall be able to detect and locate Third-Party Interference (TPI) events over a cable distance of up to 100 km (62.1 mi) when the two sensing channels are used independently.
- D. The system shall be able to detect and locate TPI events over a cable distance of up to 50 km (31 mi) when the system is deployed in the linear cut-immune configuration.
- E. The sensor unit shall have the following detection capabilities:

1. Process the signal from the sensor cable to detect TPI events
2. Locate the position of a detected TPI event within 4.0 m (13 ft) or less at least 95% of the time.
3. Detect multiple TPI events, when each TPI event is separated by a sensor cable distance greater than 30 m (100 ft) when deployed in the cut-immune configuration or 15 m (50 ft) when deployed in the non-cut immune configuration.
4. Support up to 1440 virtual detection zones.
5. Be capable of being calibrated to equalize the effective sensitivity for different burial conditions.
6. Utilize adaptive algorithms in the detection process to optimally discriminate between actual TPI events and environmental activity.

F. Intrusion detection performance:

1. The typical detection range for different TPI events shall be as given in the table below. It shall be recognized that actual performance will depend on specific site conditions and can increase or decrease considerably from these typical values.

TPI EVENT	TYPICAL DISTANCE FROM CABLE FOR DETECTION – FIRST 40 KM OF EACH SENSOR CHANNEL*
Hot taping	0 m
Light vehicle moving	3 to 5 m (10 to 16 ft)
Heavy vehicle moving	10 to 20 m (33 to 66 ft)
Heavy vehicle engine running	5 to 10 m (16 to 33 ft)
Manual digging (pickaxe)	10 to 20 m (33 to 66 ft)
Machine digging (backhoe)	10 to 30 m (33 to 100 ft)

* At the maximum sensor length of 50 km the typical lateral detection distances are halved

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 zone per year, averaged over the total number of zones in 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:

- .1 Temperature changes
 - .2 Sunrise/sunset
 - .3 Acoustic or magnetic effects
 - .4 Snow
 - .5 Fog
 - b. The system shall utilize advanced processing and an environmental compensation algorithm to minimize the probability of nuisance alarms from the following sources:
 - .1 Wind
 - .2 Rain and hail
 - .3 Sandstorms
 - .4 Motion of nearby objects or vegetation
 - .5 Motion of surface or ground water
 - .6 Seismic vibration caused by nearby vehicular traffic
 - c. The system shall provide a means to detect and reject alarms from vehicle traffic moving parallel to the sensor cable.
- G. Time to detection:
 - 1. Detected TPI events shall be reported no later than one second after the detection conditions have been met.

2.13 Detection Capabilities – Data Conduit TPI Detection

- A. The sensor shall consist of fiber optic cable installed along the full length of the data conduit to be protected.
- B. The system shall provide two independent sensing channels.
- C. The system shall be able to detect and locate Third-Party Interference (TPI) events over a cable distance of up to 100 km (62.1 mi) when the two sensing channels are used independently.
- D. The system shall be able to detect and locate TPI events over a cable distance of up to 50 km (31 mi) when the system is deployed in the linear cut-immune configuration.
- E. The sensor unit shall have the following detection capabilities:
 - 1. Process the signal from the sensor cable to detect TPI events

2. Locate the position of a detected TPI event within 4.0 m (13 ft) or less at least 95% of the time.
3. Detect multiple TPI events, when each TPI event is separated by a sensor cable distance greater than 30 m (100 ft) when deployed in the cut-immune configuration or 15 m (50 ft) when deployed in the non-cut immune configuration.
4. Support up to 1440 virtual detection zones.
5. Utilize adaptive algorithms in the detection process to optimally discriminate between actual TPI events and environmental activity.

F. Intrusion detection performance:

1. The typical detection range for different TPI events shall be as given in the table below. It shall be recognized that actual performance will depend on specific site conditions and can increase or decrease considerably from these typical values.

TPI EVENT	TYPICAL DISTANCE FROM CABLE FOR DETECTION – FIRST 40 KM OF EACH SENSOR CHANNEL*
Direct manipulation of the data communications cable	0 m
Light vehicle moving	3 to 5 m (10 to 16 ft)
Heavy vehicle moving	10 to 20 m (33 to 66 ft)
Heavy vehicle engine running	5 to 10 m (16 to 33 ft)
Manual digging (pickaxe)	10 to 20 m (33 to 66 ft)
Machine digging (backhoe)	10 to 30 m (33 to 100 ft)

* At the maximum sensor length of 50 km the typical lateral detection distances are halved

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 zone per year, averaged over the total number of zones in 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 followingsources:
 - .1 Temperature changes
 - .2 Sunrise/sunset

- .3 Acoustic or magnetic effects
 - .4 Snow
 - .5 Fog
 - b. The system shall utilize advanced processing and an environmental compensation algorithm to minimize the probability of nuisance alarms from the following sources:
 - .1 Wind
 - .2 Rain and hail
 - .3 Sandstorms
 - .4 Motion of nearby objects or vegetation
 - .5 Motion of surface or ground water
 - .6 Seismic vibration caused by nearby vehicular traffic
 - c. The system shall provide a means to detect and reject alarms from vehicle traffic moving parallel to the sensor cable.
- G. Time to detection:
 - 1. Detected TPI events shall be reported no later than one second after the detection conditions have been met.

2.14 Mixing of Installation Types

- A. The system shall support a mix of installation types on a single sensor channel including fence-mounting, wall-top mounting, burial for perimeter intrusion detection, burial for pipeline TPI detection, and data conduit protection.
- B. Between different installation types a 30 m (100 ft) spool of sensor cable shall be installed to act as timing buffer.

2.15 Cable cut response

- A. The system shall support a closed-loop cut-immune configuration that enables the system's detection and locating capabilities to remain fully operational in the event of a sensor cable cut.
- B. The system shall be capable of detecting and locating a sensor cable cut.
- C. The cut location shall be determined and reported with an absolute accuracy of equal to or less than 30 m (100 ft).

- D. In the event of a sensor cable cut, the system shall retain detection and locating capabilities in the portion(s) of the sensor cable that remain connected to the system sensor unit.

2.16 Installation and Configuration Capabilities

- A. The system shall have the following characteristics, as a minimum:
 - 1. The sensor cable shall be capable of being attached directly to a fence without needing to be in a conduit.
 - 2. The sensor cable shall be capable of being attached to the fence with standard UV-resistant cable ties (plastic or metal).
- B. The system shall support the following configuration and calibration features:
 - 1. A Windows®-based graphical user interface (GUI)
 - 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.
 - 3. It shall be possible to access the configuration GUI remotely using Windows® Remote Desktop Connection.

2.17 System-level Cybersecurity Provisions

- A. The system shall incorporate a documented list of cybersecurity provisions including having been cyber-penetration testing.

2.18 TCP/IP-Based Integration Interface

- A. The system shall provide a TCP/IP-based integration interface for communicating alarm and status data to and from security management systems.
- B. The integration interface shall incorporate cybersecurity provisions including the use of TLS 1.2 for authentication and encryption, and an IP authorized connection list (Allow list).
- C. The system supplier shall make available a complete Software Development Kit (SDK) to facilitate integration with third party systems such as video management systems, security management systems, or physical security information management systems.
- D. The SDK shall consist of complete written documentation, sample code, and a software simulator that eliminates the need to have actual hardware to test the integration.

2.19 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 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. Examples of such conditions include loose fence fabric, loose gates, or objects such as signs or tree branches hitting the fence.

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.