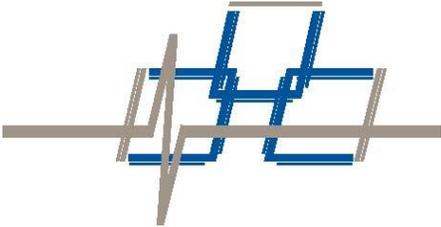


# Nuclear Energy Perimeter Security

## Application Note



©Copyright 2013, Fiber SenSys® all rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from Fiber SenSys®, Inc., 2925 NW Aloclek Drive, Suite 120, Hillsboro, Oregon 97124, USA.

This application note is provided by Fiber SenSys Inc. While reasonable efforts have been taken in the preparation of this material to ensure its accuracy, Fiber SenSys Inc. makes no express or implied warranties of any kind with regard to the documentation provided herein. Fiber SenSys Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Fiber SenSys Inc. to notify any person or organization of such revision or changes.

Fiber Defender™, Microwave Defender™ and Fiber Commander™ are trademarks of Fiber SenSys Inc.

Fiber SenSys® is a registered trademark of Fiber SenSys Inc.

Windows® is a registered trademark of Microsoft Corporation.

Fiber SenSys Inc.  
2925 NW Aloclek Dr.  
Suite 120  
Hillsboro, OR 97124  
USA

Tel: 1-503-692-4430  
Fax: 1-503-692-4410  
[info@fibersensys.com](mailto:info@fibersensys.com)  
[www.fibersensys.com](http://www.fibersensys.com)

## Contents

<i>Introduction</i> .....	4
<i>Nuclear Facility Overview</i> .....	7
<i>Design &amp; Installation Considerations</i> .....	9
<i>Considerations for Nuclear Facility Security Planning</i> .....	9
<i>Fiber-Optic Intrusion Detection</i> .....	10
<i>Volumetric Microwave Detection</i> .....	13
<i>Protecting Gates</i> .....	15
Single or Double Swinging Gates .....	16
Sliding Gates .....	16
Gates Not Requiring Protection .....	17
<i>Security Lighting</i> .....	19
<i>Integrated Solutions</i> .....	20
<i>Summary</i> .....	21



## Introduction

The nuclear energy industry is one of the nation's safest industries. It is protected by multiple back-up safety systems, robust physical defenses and plant security forces with rigorous training. Since the Sept. 11, 2001 terrorist attacks, the industry has continued to improve its safety systems to prepare for emerging threats, such the impact of a wide-bodied commercial airliner and computer-based cyber-attacks. Each U.S. nuclear power plant is equipped with extensive security measures to protect the facility from intruders and to protect the public from the possibility of exposure to radioactive releases caused by acts of sabotage. The [U.S. Nuclear Regulatory Commission \(NRC\)](#) calls nuclear power plants "among the best-protected private sector facilities in the nation."

Protection of critical energy facilities is a key national security concern. The dangers resulting from theft, vandalism or terrorist activity associated with nuclear facilities is significant, and these facilities are required to maintain the highest levels of security.

The nuclear energy industry is one of the few industries whose security programs are regulated by the U.S. federal government. According to the Nuclear Energy Institute ([www.nei.org/](http://www.nei.org/)), the U.S. Nuclear Regulatory Commission (NRC) (<http://www.nrc.gov/>) holds nuclear power plants to the highest security standards of any American industry. After the terrorist attacks of Sept. 11, 2001, the NRC ordered substantial security enhancements at all nuclear power plants. A rule issued in 2009 contains requirements similar to those previously imposed by order, as well as new requirements that evolved from experience in implementing the orders and in preparing to license new reactors.



To formally protect nuclear power and energy facilities, the U.S. Nuclear Regulatory Commission has published document number 10CFR73.55 (Code of Federal Regulations – Energy) and NRC (Nuclear Regulatory Commission) as the basis for a security protection system.

The NRC coordinates closely with other federal organizations. The agency coordinates with the Domestic Nuclear Detection Office, the National Counterterrorism Center and the U.S. Department of Homeland Security's Infrastructure Protection Office. The NRC also has agreements in place with the Federal Aviation Administration and the North American Aerospace Defense Command.

Security measures at the 104 U.S. operating nuclear plants include:

- physical barriers and illuminated detection zones
- approximately 8,000 well-trained and well-equipped armed security officers at 65 sites who are on duty shifts all day, every day
- surveillance and patrols of the perimeter fence
- perimeter intrusion detection aids (including several types of detection fields, closed-circuit television systems and alarm/alert devices)
- bullet-resisting barriers to critical areas
- a dedicated contingency response force.

With the increasing demand for clean alternative energy sources, many power utilities are shifting their attention to harnessing abundant and non-intrusive nuclear energy. Ever since emitted radiation was detected from Japan's Fukushima Daiichi failed reactor facility in March of 2011, global calls to abandon nuclear plants have risen in the U.S. and other western countries. Nuclear power contributes 20 percent of the U.S. power supply and for the present, alternative sources are falling well short of meeting energy demands. Fossil-fueled power plants pollute the air and coal companies strip the trees and soil from mountain-tops, natural gas hydraulic fracturing methods violates subterranean water supplies and economic disruption of oil dependence and carbon footprints are well known.

For safety and security reasons, Nuclear Facility operations areas have a need for high security protection zones requiring dependable security. As a result, access control and perimeter security technology solutions have evolved, as industry manufacturers integrate the latest technologies into overall security offerings. To address nuclear facility security requirements from an integrated, systems approach, manufacturers are teaming up to offer complementary technologies in response to common utility industry problems.

An integrated systems approach to nuclear facility security delivers the highest level of cost savings. Though the approach often requires an upfront investment in security procedure development and security infrastructure, the savings realized over time are profound.

**A layered, systems security approach should consider:**

- 1.) Threat Deterrence Measures
- 2.) Threat Detection & Assessment Technologies
- 3.) Intrusion Response Plan

The emergence of advanced microprocessors, enhanced fiber optic sensor detection, IP- network device convergence, digital signal processing capabilities and X-band and K-band microwave technologies all combine to provide a wide range of integrated intrusion detection technologies for long range perimeter detection. The most reliable solutions for perimeter security applications are frequently built on fiber-optic intrusion detection systems complemented with microwave sensors, with enhanced device communications capability.

The purpose of this application note is to outline the most reliable and complete solutions for nuclear power facilities and perimeter security that employ the latest in complementary intrusion detection technologies. Fiber SenSys, Inc. (FSI) is a full solution, perimeter security systems manufacturer, offering everything needed to secure nuclear facilities according to the highest commercial and military standards, including priority level one (PL-1) configurations.

## Nuclear Facility Overview

Unauthorized access to nuclear generation facilities endangers the lives of the intruders, employees and inhabitants of entire regions. The North American Electric Reliability Corporation (NERC) has been designated by the U.S. Department of Energy to coordinate critical infrastructure protection activities within the electricity sector. NERC has issued a number of advisory security standards for electrical utilities, including guidelines pertaining to physical security of their facilities.

According to NERC, each facility should implement physical security measures at their critical facilities to safeguard personnel and prevent unauthorized access to critical assets, control systems, equipment, and information that may be resident in the substation. Each entity should implement substation security solutions in a way that is consistent with the criticality of the substation and sufficient to provide appropriate situational awareness of activity at these substations so that the entity can initiate an appropriate and timely response.

Security concerns are not only centered on terrorism. Increasingly, safety issues are also paramount in the minds of facility security directors. This Reuters article from August 2012 provides one example of a growing threat to Nuclear Weapons Storage facilities:

<http://www.reuters.com/article/2012/08/02/us-usa-security-nuclear-idUSBRE8711LG20120802>

This article discusses the successful efforts of anti-nuclear extremists to shut down operations at Oak Ridge Tennessee. They were able to infiltrate the facility, wander freely at will and generally demonstrate that even these highly secure nuclear facilities are vulnerable targets for intruders attempting to disable or vandalize a facility. These types of intrusions also create utility industry liability as a result of accidents or physical harm to the intruders. Not to mention the operational costs associated with shutting a facility of this strategic significance down for a period of three days.

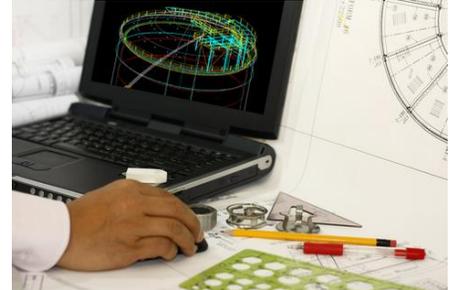
Best practices for protecting nuclear facilities combine multiple layers of detection technologies. Perimeter fencing is at the core of any basic security system and minimally impedes the attempts of unauthorized intruders. Fiber optic cable intrusion detection systems offer an excellent first-line of defense, when attached to a fence, a wall, or when buried around the perimeter. Mono-static and bi-static microwave detections systems offer a second layer for increased system reliability. Additional security technology layers include video camera monitoring and DVR recording systems for intrusion detection and events are recorded and used as evidence for later incarceration. Finally, efficiently designed automated lighting offers an excellent deterrent to intrusion attempts by would-be intruders. When any of the aforementioned sensors are triggered, relays automatically turn on lights, audible alarms or other deterrents and hopefully deter intruders before they gain access. These detection technologies offer the foundation for modern perimeter detection systems and greatly enhance the security of a chain link fence topped with barbed wire.

This application note identifies the type and frequency of security threats facing critical nuclear facilities, and outlines a layered approach to power substation security. It also includes an overview of the most effective security measures. A layered, integrated system approach to power substation security delivers the greatest overall value. With this approach, incremental solutions are installed and updated later as funding becomes available. With integrated security, the savings are significant and overall system costs are reduced.



## Design & Installation Considerations

Typical perimeter security projects include provisions for several phases of work resulting in a successful perimeter security installation. Design and support teams are engaged during all phases of a project to guide and train end users and systems integrators, and will visit the area to be secured. Getting started begins with a detailed site drawing showing building and perimeter



layouts with dimensional lengths. It is important to establish security goals and objectives prior to conducting a site walk-through with consideration for the unique areas to be secured and the location of control room equipment. Open fields, fences, runways, fuel storage areas, buildings, information technology considerations and command & control requirements are all considered during the design phase of a project.

During the walk-through, supporting personnel observe and note details not contained in the drawing such as hills, dips and other topography issues. Note any objects that would facilitate intruder bypass of the intrusion detection system, such as tall grass, trees or other vaulting aids. Analysis of the data obtained during the threat assessment and the site evaluation is used to determine the number of zones, zone layouts, intrusion detection sensor types and equipment needs.

## Considerations for Nuclear Facility Security Planning

### a.) Threat Deterrence Measures

Threat deterrence at nuclear facility includes physical deterrents like high fencing, crash-proof vehicle gates and smart locks along with the implementation of both policies and technologies that control authorized access. When a nuclear facility experiences intrusion attempts, then an evaluation of desired deterrence measures are required.

### b.) Threat Detection/Assessment Technologies

Nuclear facilities no longer have to rely only on perimeter control as the first and last defense against unauthorized intrusion. Motion detection, sound detection, lighting and video surveillance represent the current technologies that effectively and economically detect and assess threats to substations.

## c.) Intrusion Response Plan

Complete security strategies include an intrusion response procedure. Questions to consider include who in the organization determines when and if to involve the local authorities? How do natural disaster and malicious acts response plans differ? What is the procedure for getting a substation back online in the event of a catastrophic intrusion? Response plans must cover these questions to effectively protect the facility.

## Fiber-Optic Intrusion Detection

The critical importance of nuclear power facility security requires higher than normal barbed wire topped fences, secondary perimeter fencing, concrete footings around the base of the fences and solid walls. Fence mounted sensors detect and deter intruders and are tuned to conditions of cutting, climbing or the utilization of ladders, and wall-delineated perimeter areas are protected in a similar manner. Buried sensor cable, installed in serpentine patterns and rated for weather exposure (and protected from insect and rodent interference) is another common security methodology. Most importantly, all choices of perimeter security technologies are outfitted with modern communications capability, such that head-end / annunciation technologies seamlessly integrates with the security sensors.

Fiber optic-based security systems have been deployed globally for decades as the foundation for modern perimeter security solutions. The U.S. military has approved the use of fiber optic detection technology to protect the nation's highest security facilities with PL-1 compliance. In addition to reliably detecting multiple intrusion attempts and tampering, fiber-optic systems are immune to EMI, RFI and lightning representing superior security value.



Fiber-optic cable detection systems are self-contained with Alarm Processing Units (APU's) that offer reliability for perimeter intrusion detection solutions. Fiber-optic intrusion detection systems are installed on a fence or in remote monitoring facilities capable of detecting intrusion attempts along the perimeter.

With these systems deployed, end users will know instantly when an intruder, or a coordinated group of intruders, is attempting to breach the perimeter. When a zone is breached, the system instantly identifies the zone of each intrusion attempt, while continuing to monitor the other zones. Fiber optic cable systems

protect installations and equipment by pinpointing the location of intrusions anywhere along the perimeter, and protects up to 5,000 meters per zone.

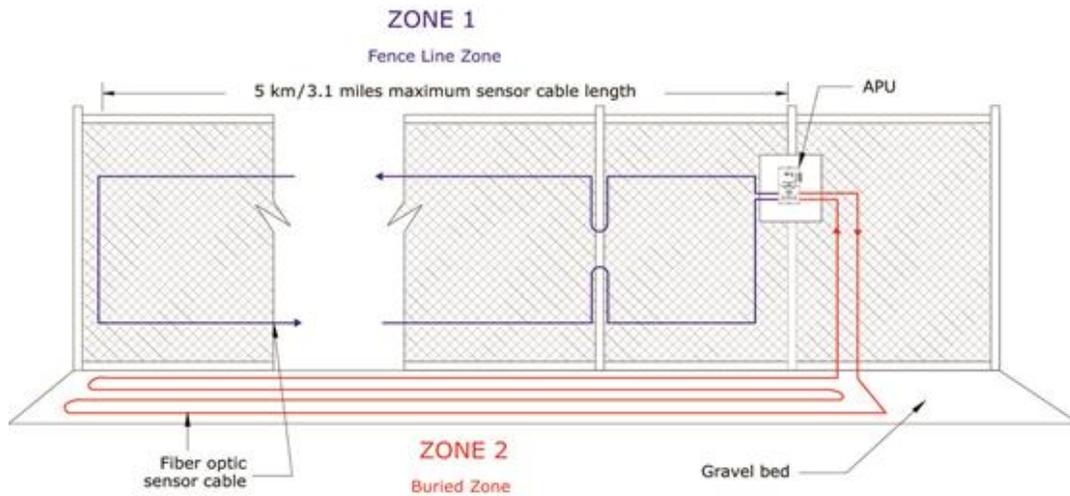


Figure 1: Field mounted APU head-end with dual -zone configuration, fence mounted sensor cable & buried zone.

Intended for fence line or buried applications, most fiber optic APU designs divide a perimeter into a maximum of either 1 or 2 zones per APU. Each of the zones is sensitive to vibrations from intrusion attempts. The APU interrogates each zone continuously and analyzes the optical return signals from each zone to determine whether or not an intrusion is taking place. Depending on the model of the APU, the sensor electronics are located up to 20 km away from the sensor cable assembly.

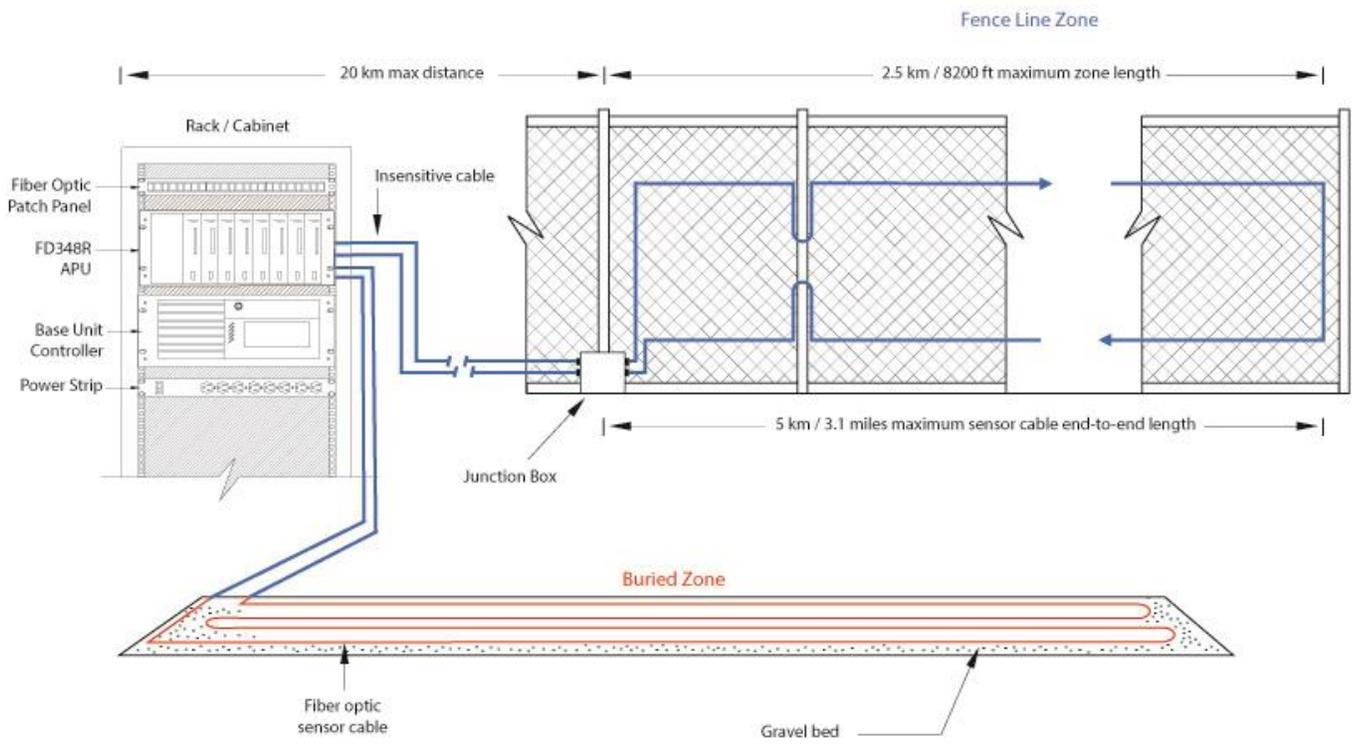


Figure 2: Rack-mounted APUs located in remote facility, with full capacity of up to 8 independent zones.

High-end APU head-end systems support up to 25 independent zones. The APU interrogates each zone continuously and analyzes the optical return signals from each zone to determine whether or not an intrusion is taking place. Best practices for high-security installations include looping the cable with outgoing cable top and return on the bottom of the fence.

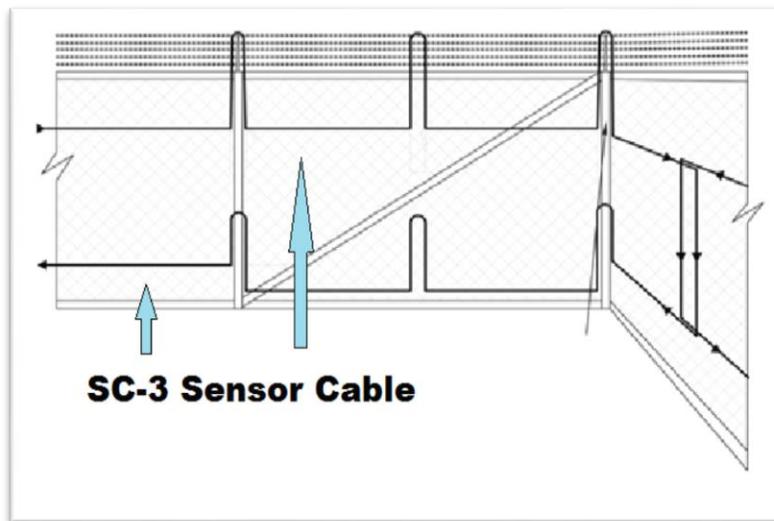


Figure 3: Double fiber cable installation, with dual-zone cross over in a high-security fence corner.

## Volumetric Microwave Detection

Microwave security systems are based on volumetric sensor designs. The microwave sensor provides a semi-conical intrusion detection area, referred to as a barrier curtain, and is described by volume of the area protected. Microwave security systems tend to be self-contained solutions that stand alone and offer a relatively clean integration to existing facility and perimeter security systems. When designing a microwave system, highly conductive materials such as fences and overhead wires may impact the microwave sensors.

The two most prevalent volumetric microwave security system designs are classified as Mono-static and Bi-static system designs. Mono-static designs require a single transceiver unit that includes both transmitter (Tx) and receiver (Rx) elements. Mono-static units typically offer a short barrier curtain, less than 50 m, where security is enhanced with a wide the area of coverage.

Bi-static microwave detection systems require two units, a transmitter (Tx) and a receiver (Rx) to protect an area. Bi-static systems provide long-range “invisible fence” coverage where the volumetric barrier is a focused, narrow beam, curtain for open area intrusion detection. The bi-static designs provide asset protection at distances ranging from 50 m to 500 m.



Figure 4: Volumetric microwave barrier curtain models range from 50 m to 500 meters.

Advanced Digital Microprocessor based designs use “fuzzy” logic to create behavior models based on received signals. It is a form of logic and uses proprietary algorithms based on multi-variable equations. It employs statistical approximations rather than fixed variables with exact values. Traditional logical methods utilize binary number sets consisting of ones & zeros, true or false. Fuzzy logic variables have values that range in degree, between 0 and 1. For this reason Fuzzy logic has been employed for the minimization of false positives, where alarm conditions occur with varying range of certainty between completely true and completely false. Put simply, fuzzy logic ensures the highest level of confidence in a generated alarm.

Some digital microwave designs also provide multi-frequency crystal designs with anti-masking capability to prevent tampering. The advanced units are immune to temperature changes with automatic environmental adjustments.

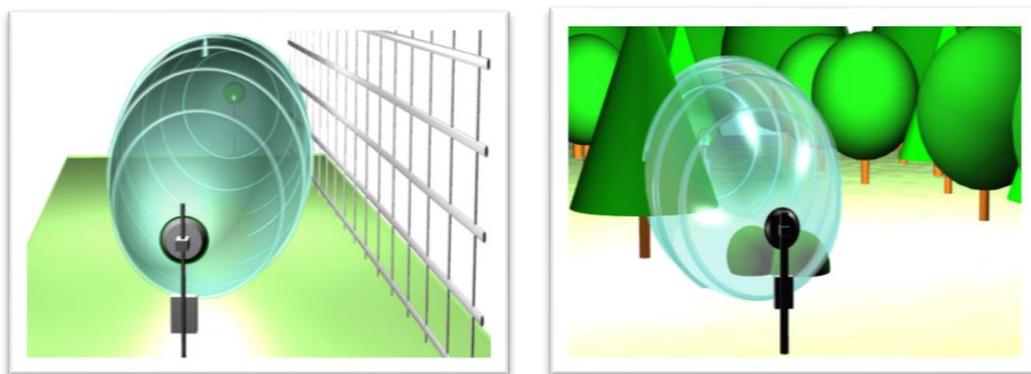


Figure 5: Avoid areas that will interfere with proper operation of Bi-static detection zones.

When metallic mesh or link fences are present, precautions are suggested:

- ensure that the fence has been properly fixed and does not move excessively

- microwave beam should not be parallel to fence, should be at an angle to it
- moving fences behind the equipment may also cause barrier distortions
- microwave barrier curtain requires a minimum of 5 meter clearance for metallic fence corridors

## Protecting Gates



Figure 6: Gate Protection with Fiber-Optic Sensor

Gates pose a unique complexity 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 can be a source 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. Isolating the gate from the fence 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.

## Single or Double Swinging Gates

For swinging gates, 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 flexible conduit and routed correctly. The sensor cable is then routed below the gate and buried in hardened PVC or metal conduit 0.3 meters (1 foot) below the roadway surface to make it insensitive to vibrations from the roadway. The cable may also be routed above the gate if a barbed wire top guard extends over the swinging gate section.

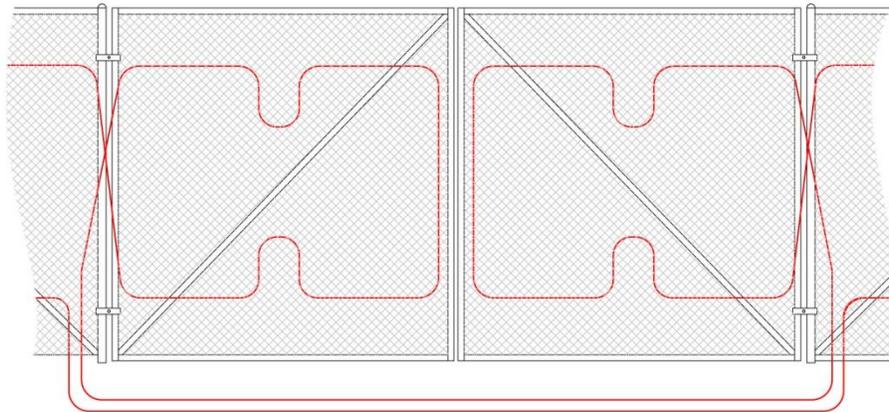


Figure 16: Sensor cable deployed on swinging gates

## Sliding Gates

Although sensor cable cannot be mounted practically on the sliding gate itself, it can be mounted on the support rail (figure 17) to detect movement of the gate. In many cases, the support rail conducts physical disturbances from the gate to the sensor.

As with the swinging gate application, the sensor cable is routed below the gate within underground rated rigid conduit 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) below the surface.

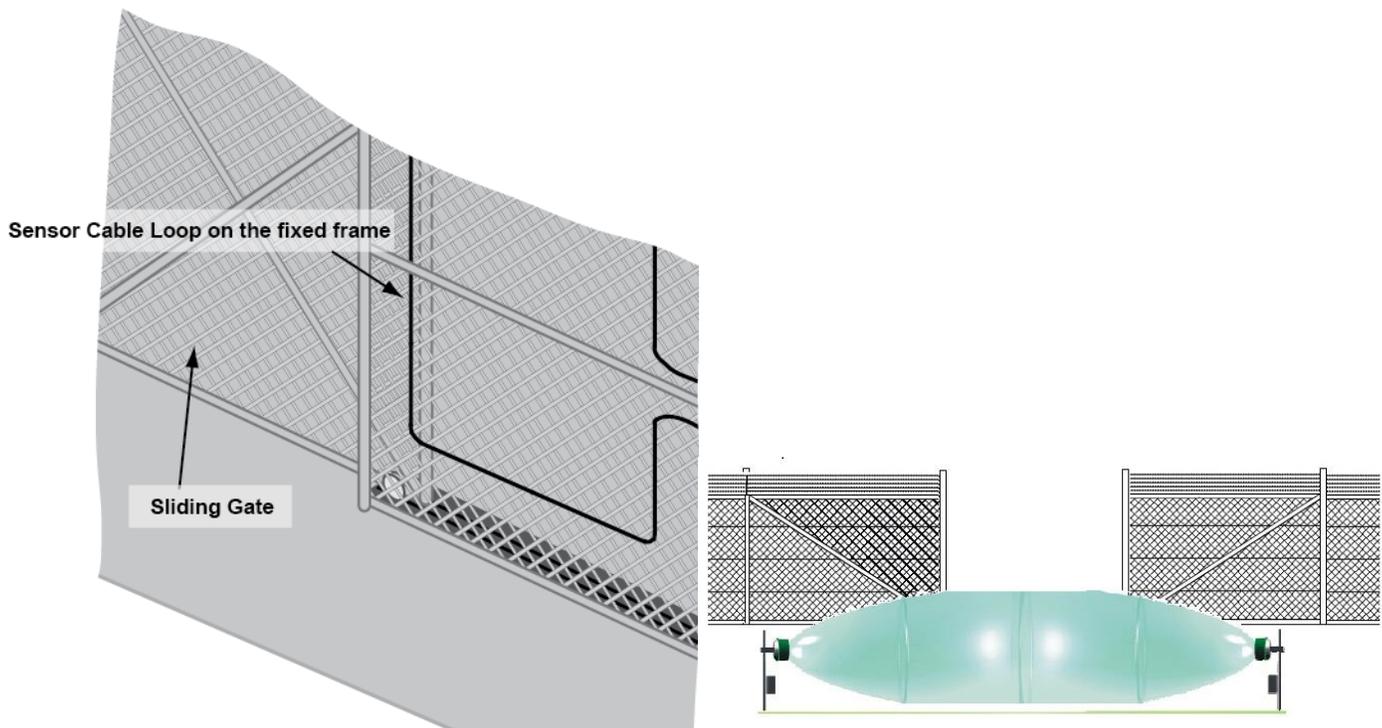


Figure 17: Sensor cable deployment on a sliding gate

## Gates Not Requiring Protection

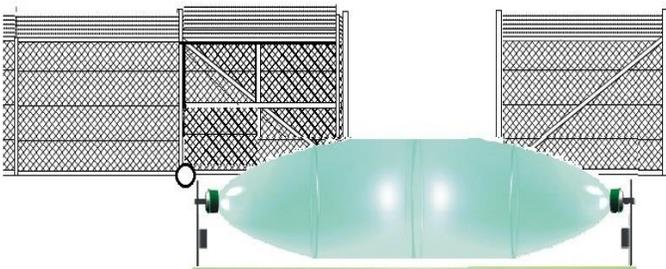
For gates that do not require protection, it is recommended that the cable be routed and buried 0.3 meters (1 foot) or more below the roadway in rigid conduit. This creates a gate bypass that is insensitive to vibration from the roadway.

A perimeter is only as secure as the fence that protects it, the material condition and integrity of the fence itself is critical to the success of preventing intrusion. Both fiber cable and microwave intrusion detection systems are intended to complement the fence and gate access points. Bi-state microwave barrier curtains offer an effective intrusion detection solution at gate entry points. Volumetric microwave detection systems can provide an alternative to swing gates or sliding gates, and sensors protect gate areas with a system that contains fewer moving parts and can operate reliably longer and with less maintenance. Volumetric sensors are easy to install, especially for existing facilities where protection is desired without a re-design of the fence system. Precautions are necessary in microwave installations to prevent

interference of the sensitive barrier curtain due to conductive electrical materials, copper wire, transformers and other materials within the perimeter.

Open gate access points benefit from microwave intrusion detection solutions in lower security applications. Open gate solutions in particular, benefit from additional Camera coverage of the area for pre response threat assessment. Installations should ensure that the barrier curtain does not intersect fences that may be impacted by the wind or other obstructions that would prevent proper operation of the microwave units. The advantage lower cost, disadvantage is detection capability only with no physical restriction to entry attempts, people & animals can freely ingress the perimeter area. This is easily resolved with a locking, sliding gate or a swing gate that restricts free access to perimeter areas.

Single and dual hinged gates offer increased security levels through access control measures in addition to both fiber cable and microwave intrusion detection at gate access points. Three system zones are required for dual technology applications in dual hinged gate solutions. One zone for each gate mounted cable and a third zone for the microwave sensor.



## Security Lighting

Perimeter security lighting is a crucial part of a security system. Illuminating the camera field of view with an Infrared (IR) or white lighting systems significantly improves the performance of the camera. Since IR lighting is invisible to the human eye, it adds an element for covert camera detection. White light is useful for guard responses and to deter intruders from entering the site. Additionally, Fiber SenSys' lighting is the most energy efficient method to illuminate airports and other large outdoor areas.

Fiber SenSys Model LDxx lighting systems are now fully integrated to provide intrusion deterrence with long-range LED and IR solutions for zone-based automatic lighting to illuminate areas with initial potential intrusion attempts. Lighting scatters the culprits before a crime is committed and saving money by reducing the need and priority to dispatch a security force.



*Fiber SenSys LDxx Security Lighting Units*

FSI lighting solutions include:

- Lighting up to 820 feet (250m) for urban unit, safety and critical infrastructure security
- Elimination of poor lighting - critical for improving HD CCTV images in low-light areas
- APU and IP enabled lighting as a part of the integrated solution

The inherent low power consumption of solid state LED arrays result in ultra-low running costs over the life of the lamp. With an average LED life well in excess of 10 years, the LDxx series provide huge energy and maintenance savings. Impact resistant and fully weather proof (IP67) with an attractive design, LDxx units are used both internally and externally for any CCTV requirement. Fiber SenSys illuminators are supplied with a U-bracket and require 12-24V AC/DC input power. Integrated control features on the illuminator include telemetry input, power and photocell sensitivity adjust, and photocell following contact to switch a day/night camera into night mode. The LDxx Series is suitable for all low light installations up to 820 feet (250m).

## Integrated Solutions

Modern security systems derive the greatest value from flexibility and scalability, integrating a variety of technologies, not based a single technology. Smart manufactures have expanded system scope to include complementary products through partnerships with other industry manufacturers, resulting in enhanced systems with multiple sensor technologies and modern communications capability.

In response to increasing need for integrated communications, and considering industry trends toward more and more security devices operating over an IP network infrastructure, organizations today are looking to integrate various electronic systems. The integration of indoor security, perimeter security, camera systems and video



management systems (VMS) combined into one centrally monitored and controlled solution is a documented industry trend. Such integration has many benefits for the end-user including the simplification of common operating methods and lowering of the system costs.

Security monitoring and control systems that provide comprehensive and intelligent integration of industry-leading technologies are an important part of any design. A head end system that ensures low nuisance alarm rates, the highest probability of detection, and the lowest overall total cost of ownership represents a value leader among security monitoring and control systems. PC-based command & control with internet protocol (IP) communications capability provides an efficient platform for integrating the components of a system, which include fiber-optic cable alarm processing units and volumetric microwave sensors. When an alarm occurs, it is automatically displayed on the relevant site map, making the job of responding to the alarm much more efficient.

### Integrated security solutions provide:

- Command & Control - graphic monitoring, controls and alert notifications
- Automatic alarm processing units – with alarm priority color coding
- Cable Sensors - continuous tamper/fault detection, with nuisance reduction
- Insensitive Cable - remote operation & obstruction mediating
- Long-range lighting – deters intruders & supports camera image resolution
- Camera & Video Systems - supports new or existing video/camera infrastructure

## Summary

Integrated perimeter intrusion detection systems are a key part of securing nuclear facilities. By integrating a variety of technologies into an overall security solution, manufacturers have expanded system scope to include complementary products through partnerships with other industry manufacturers, resulting in enhanced systems with multiple sensor technologies and modern communications capability.

Several of the technology guidelines discussed in this document are outlined in Regulatory Guide 5.44 for Perimeter Intrusion Alarm Systems as published by the United States Nuclear Regulatory Commission Systems to coordinate critical infrastructure protection activities within the Nuclear sector. This regulatory Guide establishes a number of advisory security standards including guidelines pertaining to physical security of facilities.

Any organization that has facilities, employees or information to protect will benefit from an intrusion detection system. Too often, end-users and systems integrators believe that one type of detector or sensor will cover an entire perimeter when, in fact, a better and more cost effective method might be available by combining technologies.

Integrated security systems are complex and the expertise required to facilitate a successful installation comes from years of experience. Since 1991, Fiber SenSys has been assisting designers, consultants, systems integrators and end users worldwide with their perimeter security requirements.



**Please contact us at:**  
**Fiber SenSys, Inc.**  
2925 NW Alcolek Drive, #120  
Hillsboro, Oregon 97124, USA  
Tel: +1(503)692-4430 • Toll free (US) +1(888)736-7971  
[www.fibersensys.com](http://www.fibersensys.com)

**Fiber SenSys<sup>®</sup>**  
High Performance – High Reliability – High Security