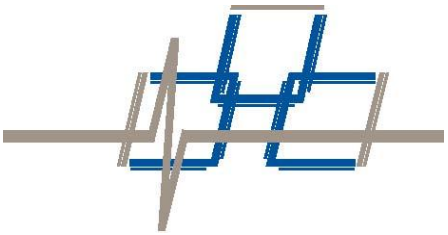
Fiber SenSys
PERIMETER SECURITY

Electrical Power Substation Perimeter Security

Application Note



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
www.fibersensys.com

Fiber SenSys

Contents

Introduction

The security of electrical substations impacts the reliability of the electrical grid in a city or town. Increasing frequency of attacks on electrical substations and the on-going threat of the terrorist / saboteur makes continual evaluation of substation security programs a necessity. Most substations appear impenetrable, but with close inspection, it is relatively easy to identify areas of the facilities where unauthorized access with intent to damage, vandalize or otherwise intrude upon the property may occur. Attacks could leave populations without power and unauthorized access endangers the lives of the intruders, employees and inhabitants of the nearby community.

The recent publicity over the increasing threat of international terrorism has added focus to perimeter security and safety, while the inherent high value of electric utility assets are also driving the need for perimeter security standards.

CIGRE, the International Council on Large Electric Systems, conducted an international study of power substation security in 2002, according to a report by Pro Vigil.com (**http://tinyurl.com/es-712**). From a sampling of 40 respondents, 35 reported that they had at least one unauthorized intrusion annually. 11 of the respondents reported that their power substations had 11 or more intrusions

annually, and 10% of the overall respondents reported 20 or more intrusions. The surveyed organizations reported that 32% of their annual intrusions involved theft and 27% of intrusions involved vandalism, graffiti and cutting/climbing security fences. Additional industry perspectives from power substation remote surveillance installations are typically higher than those found by CIGRE – possibly because of the increase in power substation copper theft and other security breach reports.

For safety and security reasons, electric utility operations areas have a need for high security 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 substation security requirements from an integrated, systems approach, manufacturers are teaming up to offer complementary technologies in response to common utility industry problems.

A systems approach to power substation 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.) Substation Threat Deterrence Measures

2.) Substation Threat Detection & Assessment Technologies

3.) Substation 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 power substation and perimeter security that employ the latest in complementary intrusion detection technologies. Fiber SenSys (FSI) is a full solution, perimeter security manufacturer, offering everything needed to secure electrical utility facilities according to the highest commercial and military standards, including priority level one (PL-1) configurations.

Fiber SenSys

Substation Overview

Unauthorized access to electrical substations endangers the lives of the intruders, employees and inhabitants of the nearby community. 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 substations 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 power substation security directors. This press article from May 2012 is example of a common copper theft scenario: **http://tinyurl.com/es-7-12-b.** Power transformers are vulnerable targets for intruders attempting to disable or vandalize a substation. The puncturing of a transformer case could cause it to leak toxic PCBs or other chemicals or, more dramatically could cause it to overheat and explode. These types of intrusions also create utility industry liability as a result of accidents or physical harm to the intruders.

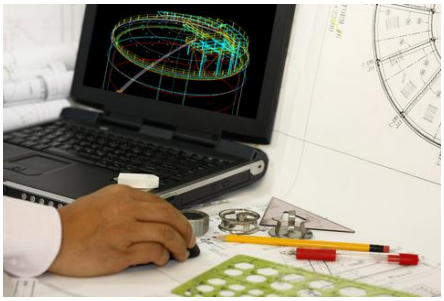
The recent growth in the market price of copper has created an increase of copper wire theft at power substations. The U.S. Dept. of Energy estimates that copper theft is now a $1 billion problem with copper prices billowing from 80 cents to over $3.50/pound. More significantly, the damage done by removing $200 of wire easily costs tens of thousands of dollars to repair. Copper theft has become a major concern for the electrical power industry.

Best practices for protecting substations 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 electric substations, 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 Substation Security Planning

a.) Threat Deterrence Measures

Threat deterrence at substation 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 substation facility experiences unacceptable intrusion rates, then a revisit of existing threat deterrence efforts and an evaluation of desired deterrence measures are required.

b.) Threat Detection/Assessment Technologies

Electric substations 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 substation security requires higher than normal barbed wire toped 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 include modern communications capability, such that head end / annunciation technologies seamlessly integrate 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, and Fiber SenSys, Inc. sensors have received Priority Level One (PL-1) certification for the military and for nuclear power plants. 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 include Alarm Processing Units (APU's) that offer reliability for perimeter intrusion detection solutions. Systems installed on a fence (or operating from remote facilities) in a zone configuration are 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 identifying the zone of intrusion along the perimeter. Through various system design alternatives, fences are protected from 500 meters up to 5,000 meters per zone. The specifications of each alarm processor unit should be carefully understood during the design phase of a project.

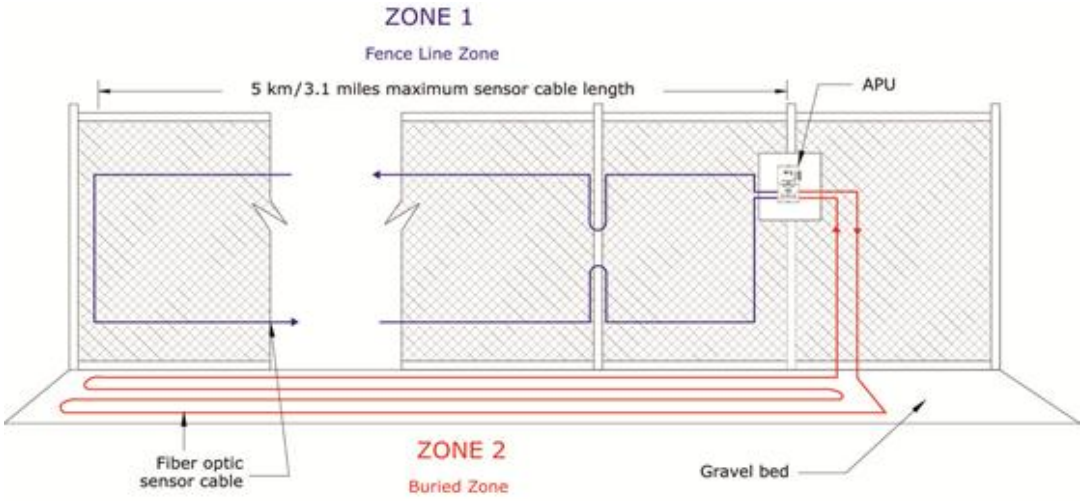


Figure 1: Field mounted FD300 series APU head-end with dual -zone configuration, fence mounted sensor cable & buried zone

Intended for fence line or buried applications, each of the perimeter 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 can be located away from the sensor cable assembly, or installed in a NEMA enclosure directly on to the fence.

FD348R (left) and FD508 (right) rack-mounted APU's, with capacity of up to 8 independent zones

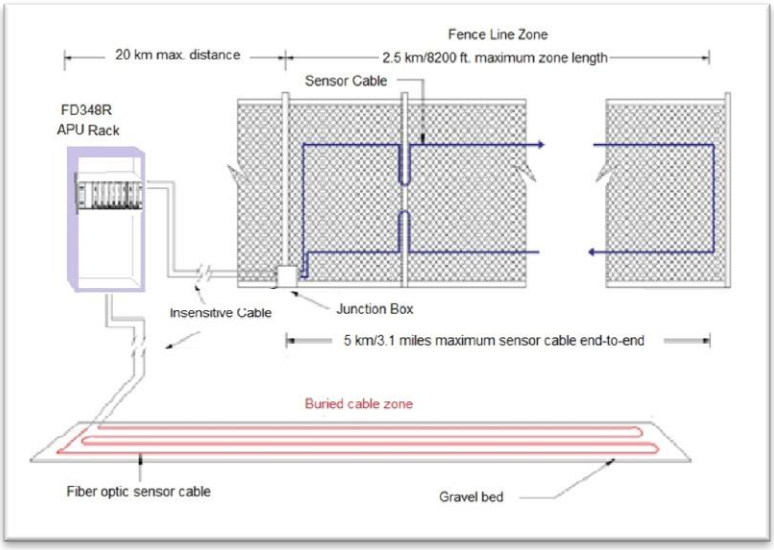


Figure 2: rack-mounted FD348R APU and fence / buried installation

High-end APU perimeter systems such as the FD525 APU 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.

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.

Figure 3: Bi-static volumetric intrusion detection

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.

Microwave protection units combine “fuzzy” digital logic technology that provides enhanced detection reliability by analyzing the received microwave signals. The microwave detection sensor offers bi-state operation, in either X-band or K-band frequencies. K-band operation offers optimal performance at military bases or commercial airports with high levels of background (RF) radiation with enhanced immunity to RF interference (RFI) that X-band cannot.

Fiber SenSys Digital Microwave units support Fuzzy logic. It is a form of probabilistic 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, it ensures the highest level of confidence in a generated alarm.

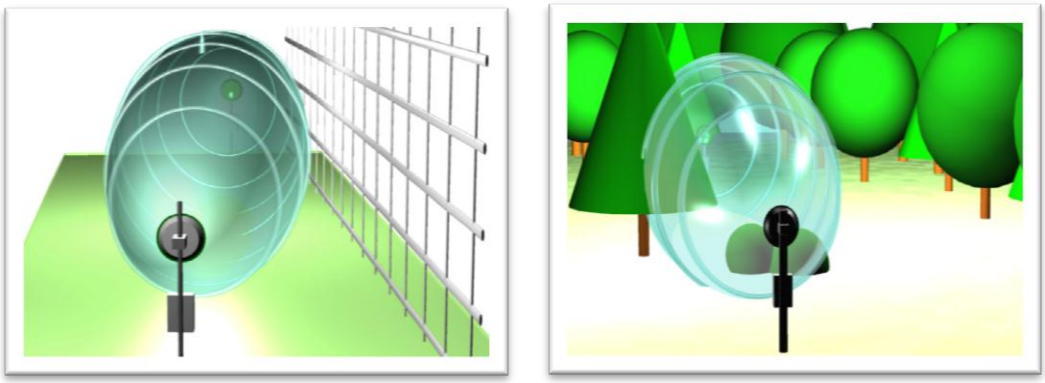


Figure 4: Avoid areas that will interfere with proper operation of Bi-static detection zones.

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

Gates pose a unique problem to fence line fiber-optic 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.

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.

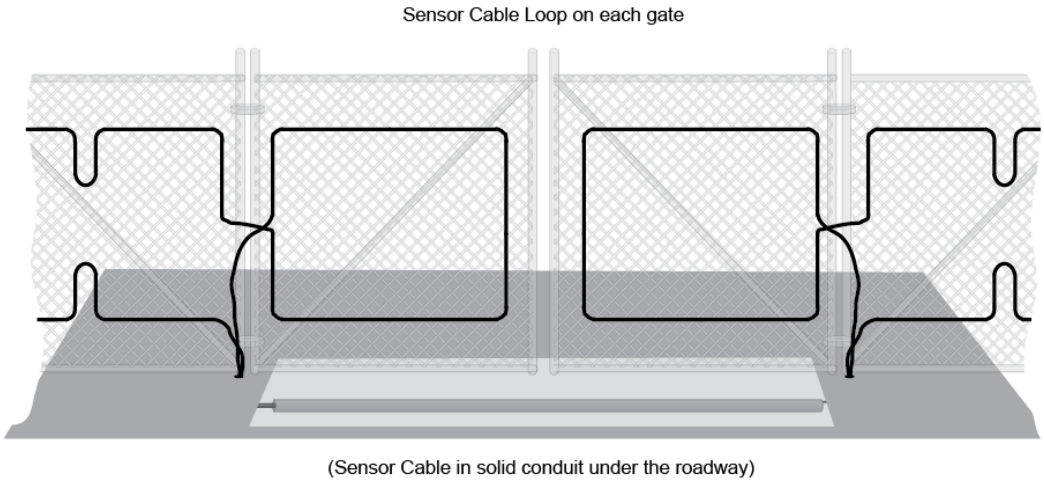


Figure 5: Sensor cable deployed on swinging gates

Sliding Gates

Although sensor cable cannot be mounted practically on the sliding gate itself, it can be mounted on the support rail (Figure 6) 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.

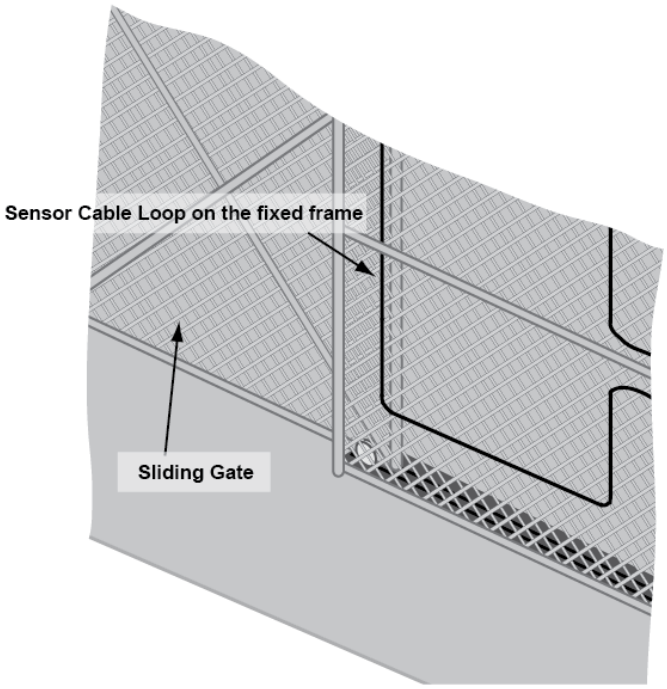
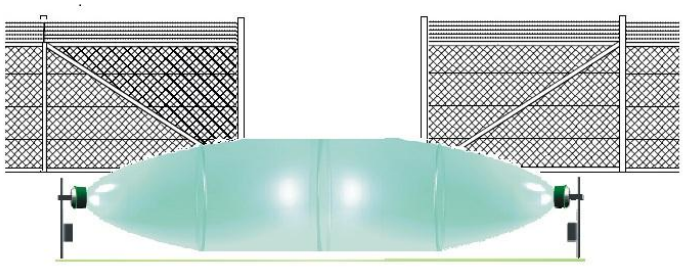


Figure 6: Sensor cable deployment on a sliding gate

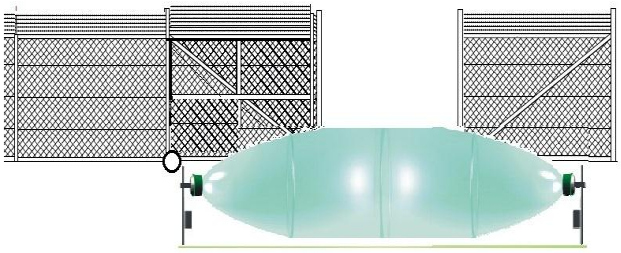
Gates Not Requiring Protection

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 PVC conduit (as shown in figure 5). This creates a gate bypass that is insensitive to vibration from the roadway.

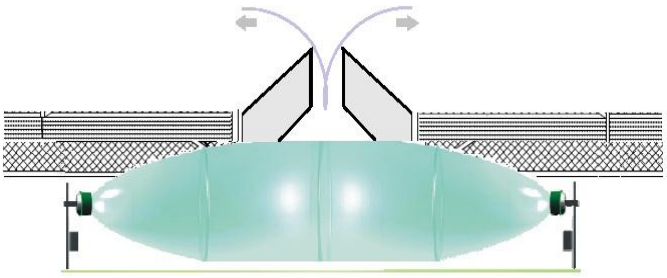
Microwave Protection for Gates



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.

Hinged gate solutions benefit from area lighting and camera coverage for threat assessment. Swinging gate access points should take measures to restrict the gate from disturbing or interrupting the protective microwave barrier. The advantage increased security and access control of ingress & egress to perimeter, disadvantage is increased cost.

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. LDxx units are used both internally and externally for any CCTV requirement, and they are impact resistant and fully weather proof (IP67) with an attractive design. 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).

Fiber SenSys

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 electrical substation facilities. By integrating a variety of technologies into an overall security solution, 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 addition to the technology guidelines discussed in this document, security regulations for the electricity sector have been published by The North American Electric Reliability Corporation (NERC) 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.

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 Aloclek Drive, #120
Hillsboro, Oregon 97124, USA
Tel: +1(503)692-4430 • Toll free (US) +1(888)736-7971
www.fibersensys.com

High Performance – High Reliability – High Security