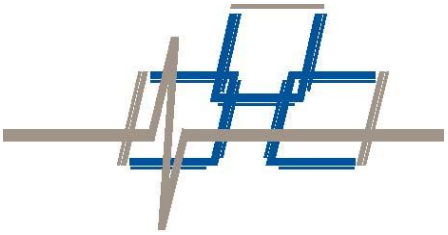
HIGH PERFORMANCE
HIGH RELIABILITY
HIGH SECURITY

Fiber SenSys
PERIMETER SECURITY

Airport Perimeter Security Solutions
(International)

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

Contents

Introduction

In the United States, the Transportation Security Administration (TSA) was created in the wake of the terrorist attacks of September 11, 2001 to strengthen the security of the nation's transportation systems. The Aviation and Transportation Security Act, passed by the 107th Congress on November 19, 2001, established a series of challenging and critically important milestones toward achieving a secure air travel system. Two of the many guidelines created under this law are requirements for improved access control and perimeter security measures.

The document has been created to support security industry end users, systems integrators and systems designers in light of several timely and relevant marketplace factors. The persistent threat of terrorist attacks and new global security directives are contributing to an increase in spending on airport security systems throughout the world, as recently reported by Frost & Sullivan http://www.frost.com/prod/servlet/press-release.pag?docid=258315033 . Frost & Sullivan estimates that global airport security expenditures were approximately $19 billion in their 2011 Global Airport Security Market Assessment. That number is predicted to grow at double digit rates for the next 7 years and will reach an estimated $45 billion by 2018. High threat potential from terrorist attacks,

coupled with global legislation will continue to pressure airport security managers to boost their investment in security, and technology companies will continue to support these trends with efficient integrated solutions and improved industry partnerships.

Increased efforts to protect critical airport infrastructure following 9/11 have led to increased budget allocations to combat security threats and protect airport perimeters. Accordingly, a proactive approach is being adopted to install integrated security solutions that will be interoperable with new emerging technologies, as well as legacy security systems. Hence, large system integrators are marking a foray into the security market and forging partnerships with smaller niche companies to offer airport operators greater benefits.

With the United States, Western Europe and Asia Pacific nations as well as countries in South America exhibiting tremendous growth in the number of airline passengers, airports will require strong, proactive security solutions. The perimeter still remains a vulnerable target for terrorists, which, as history has shown, are highly adaptable in their techniques to breach security. As a result, increased funding allocation is expected for new technology and protection initiatives, especially in countries witnessing the largest influx of airline passengers.

Commercial or military aircraft operations areas represent high security zones requiring dependable security. Even before the increasing threat of international terrorism brought added focus to airport security, the inherent high value of airport assets and the safety requirements of air operations made security a high priority. As a result, access control and perimeter security technology solutions based on changing national and international airport security standards have evolved to address the latest design requirements.

An airport facility is saturated with electromagnetic energy; an abundance of radar and radio emissions over wide frequency ranges make security detection systems that utilize electrical or electromagnetic sensors unreliable and highly subject to electromagnetic interference (EMI). Fiber-optic sensors are immune to the effects of EMI, RFI and lightning, and are ideal for protecting airports. Innovative applications of fiber-optic mat sensors are also available where the use of fences is not practical (such

as parking and taxiway areas). In modern designs, security system efficiency is increased through zone redundancy, such as a dual-zone fence and mat-sensor combined solution.

A March 2012 security assessment of the Philadelphia Airport which, at the time, did not employ a perimeter security system identified that: "the (unprotected) perimeter is the weakest point in security at U.S. airports today."[1] The Fiber SenSys, Inc. (FSI) airport intrusion detection system eliminates all of the perimeter security risks identified in this report and provides integrated technology architecture.

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

According to industry consultants, there are five key elements to an effective perimeter security system:

1. Redundant, complementary, minimally invasive and diverse sensor elements
2. Automatic detection: flexible alarm processing units to address unique needs required by specific locations for remote, local and zone based solutions
3. Intrusion-deterrent lighting solutions that include an automated security response
4. Command & Control: Integration software with annunciation capabilities
5. Cameras for visual verification and alarm response

[1] Reference: U.S. House of Representatives Press Release 3/1/12 - **http://tinyurl.com/PS6-12**

Getting Started

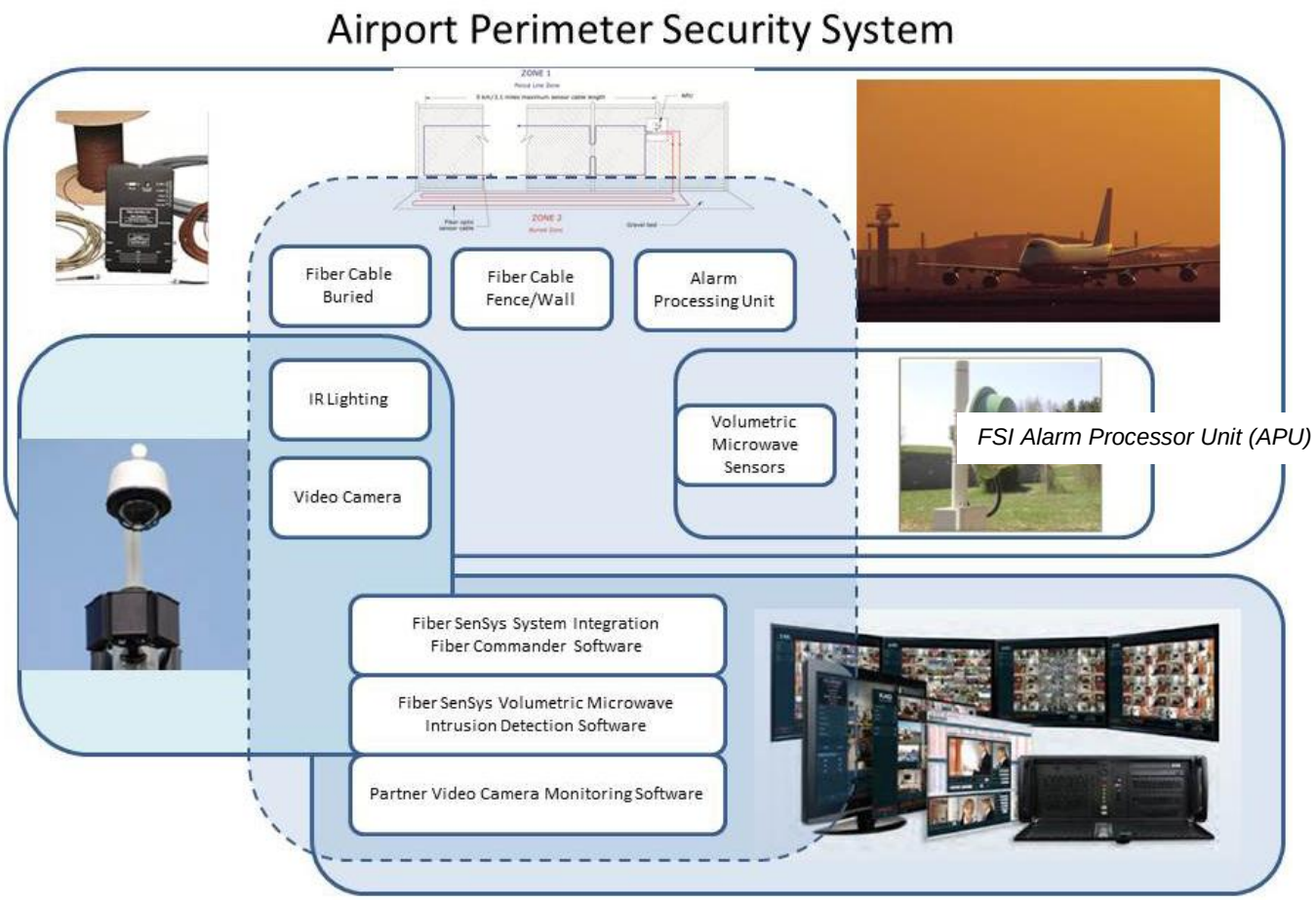
Typical perimeter security projects include provisions for several phases of work culminating in a successful perimeter security installation. Design and support teams are frequently engaged in the project to guide and train end users and systems integrators, and if requested, will visit the area to be secured. Getting started begins with a detailed site drawing showing building and perimeter layouts with dimensional lengths. It is best to establish preliminary 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. These can include open fields, fences, runways, fuel storage areas, buildings, information technology considerations and command & control requirements.

During the walk-through, supporting personnel and industry technicians observe and note details not contained in the drawing such as hills, dips and other topography considerations. They will also 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 quantities.

FSI Alarm Processor Unit (APU)

Another consideration during the initial design phase is the overall budget requirements. In the absence of strict budget enforcement by government procurement initiatives, small and medium-sized commercial airports offer feasible growth opportunities to security vendors to provide cost-efficient security structures. Moreover, to sustain market growth, companies will need to evaluate airport operations on a regional level to determine the countries that are facing the highest threat from terrorism or sabotage at the airport perimeter.

Currently, a greater number of airports are switching to digital networks, rendering it essential to network all security solutions to the main command, control and communications (C3) center. Furthermore, as layered technology security solutions are offered, integrated network systems which feature open architecture structures will become crucial for existing airport operators.



FSI Alarm Processor Unit (APU)

Also included as a preliminary project analysis is a review and discussion of desired alarm response and monitoring procedures. For example, the threat of trespass into a fenced area may be countered by a sensor buried in gravel located inside or outside the fence; the alarm annunciation capability may include an audible alarm or activation of flood lights. Incident response criteria built into integrated solutions can also include local guard and patrol services that can be notified through an auto-dialer or through SMS (Short Messaging Service) enabled by the alarm output technology. Alternatively, alarm relay outputs and integration with the head end system may be used to trigger incident response, enhanced lighting and video assessment.

Fence mounted sensors are well suited to deter and detect conditions of cutting, climbing or the use of ladders, and wall-delineated perimeter areas can also be protected in the same 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. Mat sensors have been used in major transportation centers in the U.S. and can easily be applied to airport security areas. Most importantly, all choices of perimeter security technologies are outfitted with modern communications capability, such that head end / annunciation technologies can seamlessly integrate with the security sensors.

Perimeter Sensors

Fiber Optic Intrusion Detection

Fiber optic-based airport security systems have been deployed globally for more than 2 decades and serve as the foundation for modern perimeter security solutions. Fiber optic technology is widely accepted in both commercial and military air base applications. The U.S. Air Force has approved the use of fiber optic intrusion detection technology to protect some of the nation's highest security facilities where installed systems consistently deliver the highest performance. Those systems that have achieved U.S. *priority level one* (PL-1) certification are rated for protection of the most valuable assets[2]. In addition to reliably detecting multiple intrusion attempts and tampering, fiber-optic immunity to EMI, RFI and lightning has demonstrated superior perimeter security value. Fiber optic sensor systems continue to operate smoothly and unimpeded after the effects of disruptive weather-related events.

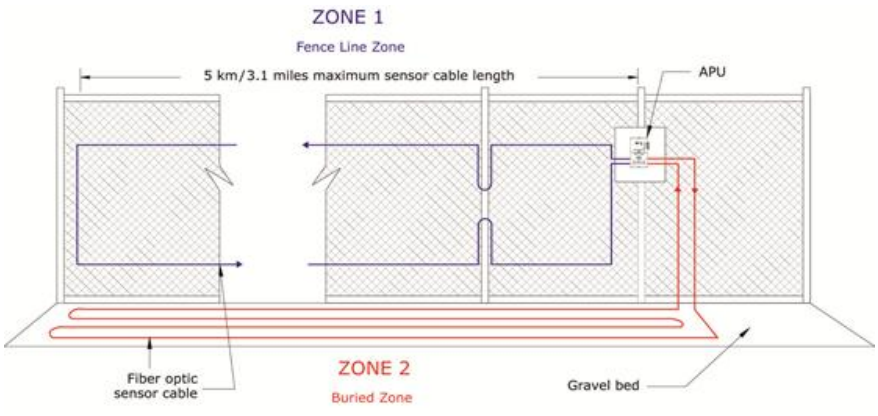


Figure 1: Outdoor configuration with closed loop fence and buried zones.

[2] The Fiber SenSys FD525, FD332 and FD342 APU's have been certified for priority level one (PL-1) installations.

The Fiber Defender™ Alarm Processing Units (APU's) from Fiber SenSys, Inc. (FSI) offer high reliability for perimeter intrusion detection solutions. Consisting of the either the FD3xx or FD5xx series APUs, these all-fiber-optic intrusion detection systems 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. The Fiber Defender APU identifies intrusion attempts along a perimeter in a zone configuration. When one zone is breached, the system instantly identifies the zone of each intrusion attempt, while continuing to monitor the other zones. Fiber Defender system installations protects aircraft and aviation equipment along the fence perimeter with zone lengths up to 5,000 meters.

With the FD34x and FD5xx series sensors, an insensitive lead-in cable provides design flexibility for connecting the APU to remotely-deployed zone(s)[3]. There is a significant design advantage and cost savings associated with the use of insensitive lead-in cable equating to reduced power requirements in the field. In an airport environment, perimeter fences can be protected without the requirement to provide power in the field, removing many environmental and logistical design challenges.

FD525 Alarm Processor Unit

Intended for fence line or buried applications, the Fiber Defender FD3xx series APU includes a cable design that divides a perimeter into a maximum of either 1 or 2 zones per APU. In the case of the FD525, each APU can support up to 25 independent zones. Each of the independent zones is sensitive to vibrations from intrusion attempts, and 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. The APU provides independent tuning of each zone for optimal system effectiveness. Additional tuning and calibration of the APU is provided by the FSI SpectraView™ software and the FD525 software suite.

[3] Insensitive lead-in capability: FD525 – up to 5KM; FD34x series – up to 20 KM

For increased security, the trunk and lead-in cables of an APU can be buried and the sensing element can be installed in PL-1 configurations. The unique capabilities of the Fiber Defender APU provide the highest security in the market: detection of simultaneous events on all zones, sensing in high security configurations (PL-1), and single-point failure mitigation. An insensitive lead-in cable up to 5 km (FD5xx) or 20 km (FD34x) in length connects the APU to the remotely-deployed sensor assembly.

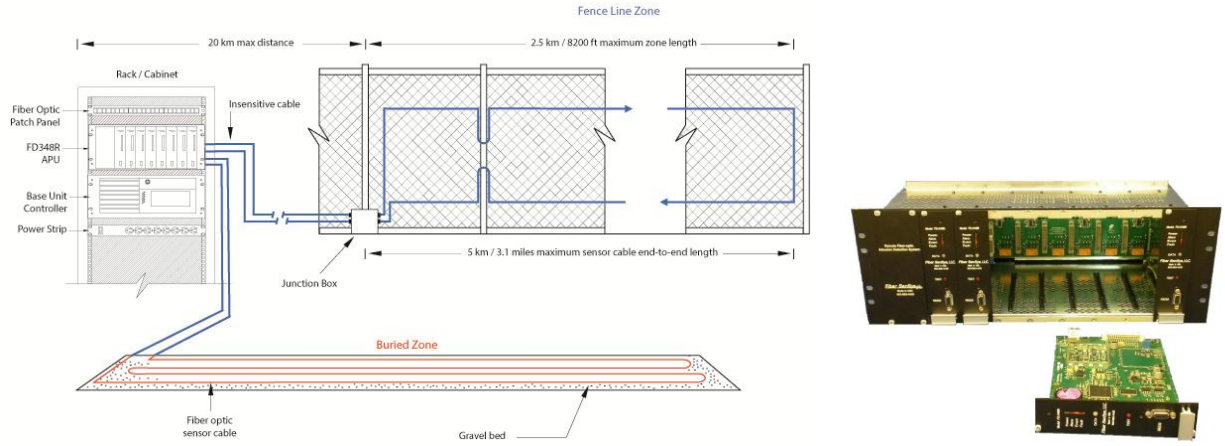


Figure 2: Indoor head-end, rack-mounted APU, shown with 3 APU cards, with area coverage of up to 8 independent zones when fully configured, into closed loop fence and buried zones.

The rack-mounted Fiber Defender model FD348R APU is uniquely suited to remotely monitor and protect multiple zones from a single, indoor server rack, with up to 8 FD348R APU's and up to 8 independent zones. The FD348R multi-zone protection typically includes a combination of buried zone and fence or wall zones. Each of the FD348R's are calibrated independently and set for optimal detection sensitivity levels. As with the other Fiber Defender APU's, the FD348R has individual zone sensitivity settings to ensure screening out of sensor signals from nuisance events, such as wind, while focusing on events caused by genuine intruders.

Remote Communication Capability

The IP/XML option configures the Fiber SenSys APU's with an RJ-45 connector, in order to provide TCP/IP connectivity with your business network and with industry-standard head end and annunciation equipment. This option enables the APU to send and receive commands while receiving detection information live, with real-time alarm data to remote monitoring stations. Additional support for complementary technologies is enabled through the *FSI Device SDK*, a software development kit used to assist other manufacturers with FSI APU communications.

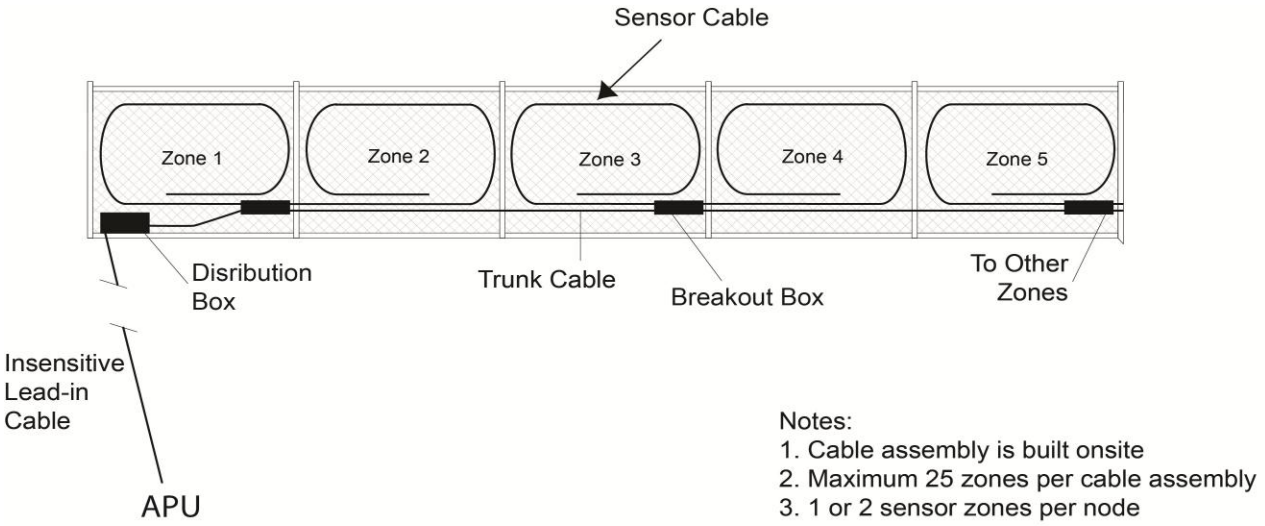


Figure 3: FD525 APU remote head-end configuration supports up to 25 distinct zones.

The FD525 APU's rugged cable assembly consists of up to 25 individual sensor elements branching off an insensitive trunk cable. Sensor node placement along the trunk cable defines each zone location. The APU protects perimeter lengths of up to 5 km for fence applications. An insensitive lead-in cable up to five km in length connects the APU to the remotely-deployed sensor assembly.

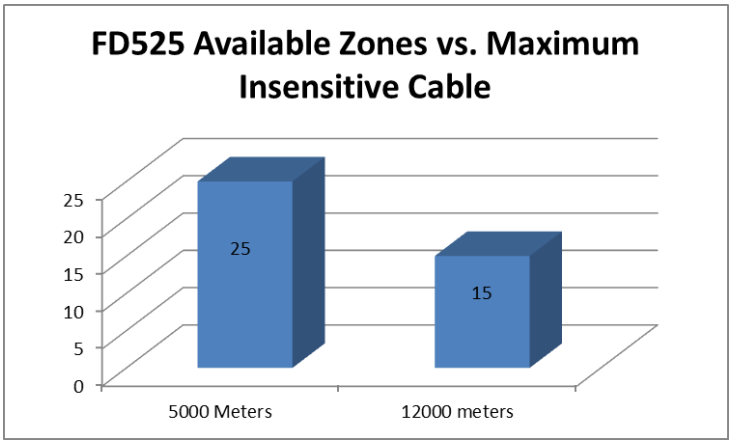
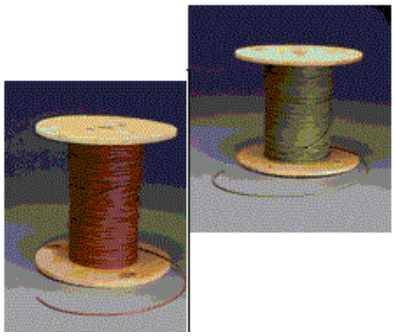


Figure 4: FD525 APU zone configurations depend on insensitive cable length.

Fiber Optic Sensor Cable

Used together with a Fiber Defender™ Alarm Processing Unit, the sensor cable forms a complete fiber-cable intrusion detection system. Immune to the effects of EMI, magnetic fields, radio frequency transmissions and lightning, the fiber optic sensor cable is a proprietary multi-mode cable designed to optimize the effects that vibration and pressure have on the conductance of light. Rugged, durable construction ensures the cable survives exposure to the harsh elements and weather conditions associated with outdoor deployment.

Two versions of sensor cable are available. The SC-3 is a 3 millimeter diameter cable for fence line and indoor applications, and SC-4, (4 millimeter diameter) for buried applications. The SC-3 sensor cable requires insertion in flexible conduit prior to deployment for fence line applications. Each sensor cable has uniform sensitivity throughout the entire length.



SC-3 and SC-4 cable

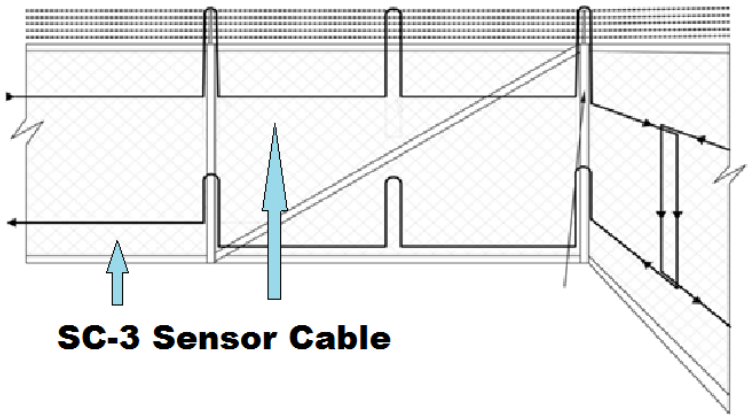


Figure 5: The SC-3 sensor cable installation in a high-security fence, corner zone.

Fiber Lead-in Cables

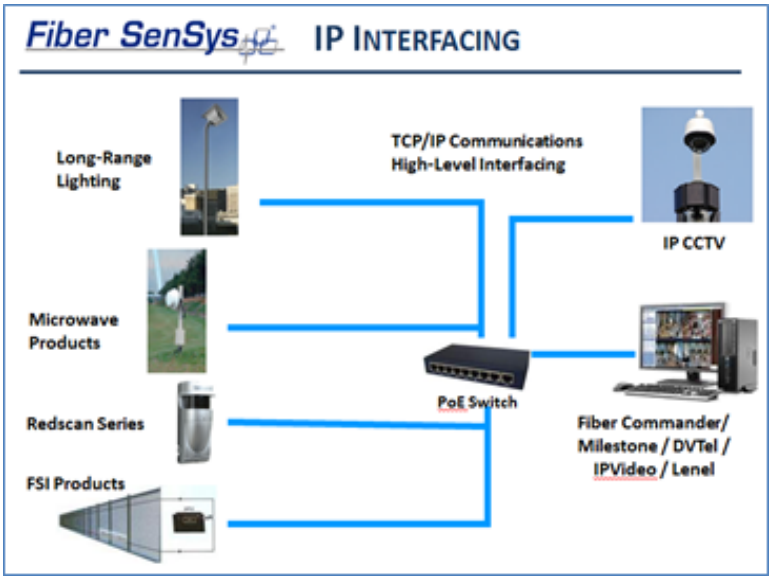
Relatively impervious to the effects of vibration, motion and pressure, insensitive fiber optic cable provides a method to extend the distance between the deployed sensor cable and the FD300 series Alarm Processing Unit (APU) up to 20 kilometers (12.4 miles).

Insensitive cable is available in two versions, depending upon the application: IC-3, a 3 millimeter diameter cable for above-ground applications, and IC-4 (4 millimeter diameter), for buried applications. The IC-3 insensitive cable requires insertion into protective PVC conduit prior to deployment for above-ground applications. The IC-4 insensitive cable can be buried directly without the use of conduit.

The insensitive cable consists of a standard 9 µm/125 µm single-mode optical fiber protected by a UV-resistant rugged jacket which enables it to survive in harsh, outdoor conditions. The IC-4 insensitive cable has an additional layer of outdoor jacket materials for direct burial.

Integrated Security Management

Proven and certified perimeter security fiber-optic sensor technologies have been integrated at the manufacturer level and are combined to create a more robust perimeter technology solution. FSI has expanded its scope to include complementary products in partnership with industry manufacturers that enhance its fiber-optic sensor offerings, enabled by a Device SDK.



The related components include PC command & control software with internet protocol (IP) interface capability, alarm processing units (APU), optical lead-in cable, either single mode or multi-mode sensor cable.

Fiber SenSys provides everything for a completely integrated perimeter security system.

- **Single integration point** – a seamless platform and architecture integrates the most common perimeter security sensors used in airport applications.
- **Real-time intrusion detection**, immediate response – event-driven alarms and automation alerts operators for an effectively measured intervention response.
- **Simplified, effective, solutions** – event verification avoids unnecessary and time consuming threat responses, simplified interface reduces operator training and reuse of existing video surveillance equipment.

Considering the unique environment specific to airports, Fiber Defender systems are suitable for protecting areas where aircraft, refueling vehicles or flammable fuel containers are stored, provided that no electrical components (the APU, power leads, etc.) are routed through the area. Please refer to the Fiber SenSys *Protecting Hazardous Material Application Note* (available at www.fibersensys.com) for deploying a system in a manner that ensures that flammable and hazardous areas are protected against intrusion, while meeting intrinsically safe apparatus requirements.

Fiber SenSys 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, barrier & obstruction mediating
- Long-range lighting – deters intruders & supports camera image resolution
- Camera & Video Systems - supports new or existing video/camera infrastructure

Command & Control

Airport security systems can also include Fiber Commander® Software from FSI, a comprehensive and intelligent head end, for the integration, monitoring and control of industry-leading fiber optic sensors from FSI and complementary technology from industry partners. No other system gives you total perimeter security with the lowest nuisance alarm rate, highest probability of detection, and lowest overall cost of ownership.

Fiber Commander® offers powerful, easy-to-use, IT facilitated, integrated perimeter security management. It is compatible with the popular Microsoft Windows operating system environments. Now supporting Adam I/O, and the Milestone POE, where power over Ethernet is facilitated, Fiber SenSys is able to bring in relay contacts and network communications from third party sensors. Additionally, relay outputs can be controlled to turn on lights, open or close gates and perform other device management tasks through Fiber Commander Software.

Fiber Commander® is a complete, end-to-end solution targeting commercial & military airport perimeter security applications. The software provides real-time monitoring, command, and control automation in a single unified system.

Figure 6: Fiber Commander® provides direct interface to Fiber Defender APUs.

Fiber Commander® detects intrusions early and provides alarm notifications to operators, facilitating the dispatch of security forces immediately to the precise location where intrusion attempts are detected. When combined with the advanced technology of the Fiber Defender (APU), the graphical computer display highlights the precise zone locations of perimeter intrusion attempts.

Input & Output Relay Mapping

As a complement to the FSI head end integrated solution, the Adam 6060 is a networked relay module that contains relay outputs and digital inputs. A customer can use Fiber Commander to monitor remote devices connected to Adam 6060 units. Fiber Commander can be configured such that when an alarm event occurs, Fiber Commander will activate a relay on the Adam 6060. The relay will remain active until the event is acknowledged through a response or dispatch.

Unmanned mode allows Fiber Commander to operate without the need for an operator to acknowledge alarms. Unmanned mode works in conjunction with Adam 6060s and Fiber Commander's Input to output features to automate onsite lighting and cameras to simplify alarm response procedures.

Sixnet® SLX-5MS-4ST Managed Switches

For more complex installation requirements, the optional Sixnet® SLX-5MS-4ST managed switch architecture allows a customer to build a redundant fiber optic network. In this scenario, a communications ring topology is enabled as Fiber Commander monitors each switch and generates an alert when a connection has gone down.

The SLX-5MS and SLX-8MS are 5 and 8 port managed industrial Ethernet switches designed to be rugged, reliable and secure. Combining compact DIN-rail packaging and protected circuitry with powerful software, our managed switches keep industrial networks up and running even in the toughest conditions.

Industrial Switch Product Highlights include:

- 5 or 8 fast Ethernet (10/100) ports including up to 4 fiber (100Mb) ports
- Managed with advanced features and security
- Slim 5 or 8 port DIN-rail packaging
- High performance and value
- Industrial-hardened design

Camera & Video Systems

The Fiber Commander® head end solution also provides a crucial link for industry leading partners in open source security video management solutions. Fiber SenSys systems are now fully compatible with most IP cameras, encoders and digital recording systems through the Commander™ SDK. Milestone® compatibility makes it easy to create high-level integration and form complete integrated solutions using other edge devices.

Fiber Commander (and its optional integrated components) is positioned as the value leader among security monitoring, annunciators and control systems. It provides the features needed for a head end solution that is priced thousands of dollars less than the competition. Fiber Commander is feature rich and simpler to use and install than other security systems that cost thousands of dollars more.

Access Control System Integration

FSI airport security systems also support access control solutions from leading industry partners, such as Lenel. OnGuard® Access is an advanced access control application that includes a feature-rich alarm monitoring module. IP-enabled controllers allow the application to extend easily to all parts of the enterprise with the appropriate degree of security at the door. OnGuard® Access offers built-in support for all card technologies including MIFARE and iCLASS smart cards, as well as biometrics and wireless access control devices.

Multiple Buildings on One Campus

Long-Range Lighting Systems

Fiber SenSys integrated airport technology systems can also support cameras & lighting as a vital part of a perimeter security system. Illuminating the camera field of view with an Infrared (IR) and white lighting (WL) system 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 LIRxx 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.

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 LIR series can provide huge energy and maintenance savings. Impact resistant and fully weather proof (IP67) with an attractive design, LIR units can be 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 D/N camera into night mode. The LIR Series is suitable for all low light installations up to 820 feet (250m).

Fiber SenSys LIRxx Security Lighting

Summary

Fiber optic-based airport security systems have been deployed globally for over a decade and serve as the foundation for modern perimeter security solutions. Fiber optic technology is widely accepted in both commercial and military air base applications. New technology is revolutionizing airport security by enhancing labor-intensive and expensive security measures as identified by Frost & Sullivan, a leading industry research firm.

Security companies that provide a total security solution are becoming important industry partners with the integration of security system elements at the manufacturer level. Along with enhanced security technology, human interaction is still required, “to evaluate and implement the appropriate (threat) response". Cohesive, single-point control over individual security system elements such as fiber-optic cable, video cameras and lighting helps to identify and, in some cases, eliminate or scatter intrusion threats. Technology that can be easily integrated offers “bolt-on” scalability to existing systems, while providing cost savings to new initial builds. With this strategy in place, airport security managers can begin with a basic initial security investment that can be enhanced at a later date.

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

Appendix A: Fiber SenSys APU Selection Table

	FD525R	RLM525	FD525	OM525	FD348R	RK348	FD342	FD341	FD332	FD331
Calibration SW Included	●		●							
Store Data Internal					●		●	●	●	●
Parameters	●		●		●		●	●	●	●
TCP/IP Compatible	●		●		●		FDIP	FDIP	FDIP	FDIP
USB /IO	●		●							
RS232 /IO					●		●	●	●	●
Form C Relay / Zone		●		●	●		●	●	●	●
Dedicated Fault Relay		●		●	●			●		●
Two Year warranty	●		●		●	●	●	●	●	●
Upgrade Firmware	●		●		●		●	●	●	●
Max Zones	25	25	25	25	1	8*	2	1	2	1
Insensitive Lead-in	12k **	●	12K **	●	20K		20K	20K		
Wind Software	●		●		●		●	●	●	●
Temperature	0 to 40° C	-40 to 70 °C			0 to 40°C	0 to 40° C	-40 to 70 °C			
Minimum Power	12w @ 12VAC	2W	8w @ 12VDC	3W	3W	25w @ 12VAC	3W @ 12VDC			
PL-1 Rated			●				●	●	●	●
NS TISSI Compliant					●					

Accessories	
SC-3 / SC-4	Fiber Optic sensor cable / Conduit Clad Cable
EZ300	Conduit kit
BB100	Breakout Box
Hyperion	Handheld APU Calibration Device
SLX-5MS-4ST	Sixnet® SLX-5MS-4ST managed switch
Adam-6060	Relay Switch module
EZ--370	Cable mounting, Metal Wire Twist Tool

All APUs comply with CE, RoHS * With 8 cards installed ** Refer to Figure 4