SANDIA REPORT

SAND94-0020 • UC-706
Unlimited Release
Printed March 1994

An Evaluation of Fiber Optic Intrusion Detection Systems in Interior Applications

Jose T. Vigil

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-94AL85000

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A03
Microfiche copy: A01

Distribution
Category UC-706

SAND94-0020
Unlimited Release
Printed March 1994

AN EVALUATION OF FIBER OPTIC INTRUSION DETECTION SYSTEMS IN INTERIOR APPLICATIONS

Jose T. Vigil
Intrusion Detection Technology Department
Sandia National Laboratories
Albuquerque, New Mexico 87185

ABSTRACT

This report discusses the testing and evaluation of four commercially available fiber optic intrusion detection systems. The systems were tested under carpet-type matting and in a vaulted ceiling application. This report will focus on nuisance alarm data and intrusion detection results. Tests were conducted in a mobile office building and in a bunker.

Acknowledgments

The author would like to acknowledge the assistance of Tim P. Malone, Project Leader of the Interior Sensor Group, for providing input and data and for reviewing this report.

Contents

Figures

Tables

1 Introduction

This report discusses the testing of four commercially available fiber optic intrusion detection systems. The report focuses on intrusion detection results and nuisance alarm data, and is part of an ongoing evaluation of interior intrusion detection systems. The following paragraphs discuss the basic operation and techniques of fiber optic sensors. The chapters that follow will describe the systems tested, the test procedures, and results.

Interior intrusion detection systems are designed to detect an unauthorized intrusion into a building or a room within a fixed-site facility. Fiber optic sensor technology is one method of intrusion detection. In recent years, fiber optic sensor technology has been growing in both interior and exterior security applications. In interior applications, the sensor can be used under carpet, on walls, or on top of suspended ceiling tiles. The sensor is basically a standard commercially available fiber optic cable that is sensitive to pressure, vibration, or movement. The fiber optic sensing cable is connected to an alarm processing unit that determines if an alarm has occurred. In simple terms, a laser is used to inject light into the fiber. The light travels the length of the cable and is received by a detector that converts the light signal into an electrical signal.

1.1 Fiber Optic Sensor Basic Operation

Two types of techniques are being implemented in the detection systems being evaluated. One type uses what is called a speckle pattern technique. When light is sent through the sensing cable, it appears at the end of the cable as a speckle pattern of light and dark patches. The patterns of light and dark patches are caused by the many different modes or paths light can travel in a multi-mode fiber optic cable. When the cable is stationary, the pattern is also stationary. However, when pressure is applied to the cable, it changes the way light is distributed through the cable. This change redistributes the speckle patterns of light and dark patches. These speckle patterns are converted to usable electrical signals through the use of a photo-diode. The alarm processing unit (APU) uses this information to determine if an alarm has occurred.

The second technique uses interferometry to determine the changes in the sensing cable. This technique uses wavelength-division multiplexing (WDM), which is a method capable of sending multiple signals at different wavelengths through the same fiber. A beam splitter is used to send two signals at different wavelengths in opposite directions. A photo-diode is then used to add the algebraic sum of the two beams. When pressure is applied to a fiber, it changes the index of refraction, thus changing the velocity of light. The APU uses this information to determine if an alarm has occurred. Interferometric sensing techniques can only be accomplished with single mode fiber optic cable.

2 Fiber Optic Sensor Technologies Evaluated

The systems being evaluated are:

1. **Fiber SenSys M106E/M105E**
   Fiber SenSys, Inc., Beaverton, Oregon

2. **FOIDS Model 1000**
   Mason & Hanger National, Inc., Huntsville, Alabama

3. **Sabrefonic & Sabreline System**
   Pilkington Security Systems, United Kingdom
   marketed in the U.S. by Stellar Security Products,
   Santa Clara, California

A detailed description of these systems will follow.

2.1 Fiber SenSys, Inc., Model M105E/M106E

2.1.1 System Description

The Fiber SenSys M106E is a single channel fiber optic detection (FOD) system designed for use in both interior and exterior applications. The M106E is specifically installed remotely from the structure or perimeter being protected. The M105E is designed to be installed at the location of the structure or perimeter being protected. Both FOD systems share the same basic operating principles. The "E" at the end of the model number refers to the APU mounted in an enclosure. The system incorporates a combination of interferometric sensing techniques and the speckle pattern techniques (the exact technique is proprietary information).

The Fiber SenSys processor is housed in a fiberglass polyester NEMA Type 4X enclosure. It has quick release latches with knockout padlock provisions. The overall dimension is 16.55-inches-high x 14.55-inches-wide x 8.55-inches-deep. A transient surge protector and an anti-tamper device are also mounted in the enclosure.

The system requires a hand-held calibrator with a security key. The calibrator is a weather-resistant programming unit with an alphanumeric keyboard and a 2-line LCD display. It is used to adjust the alarm settings, troubleshoot the system, and read information describing the system. The security key provides interface between the calibrator and the APU helping to prevent unauthorized access to the system.

The sensing cable is available in lengths of up to 6,560 feet. The insensitive cables (M106E only) are approximately 10 dB less sensitive than the sensing cable. The maximum length of the combined sensitive and insensitive cable is 6,560 feet. Figure 1 shows a picture of the Fiber SenSys unit in a NEMA enclosure with the calibrator attached.

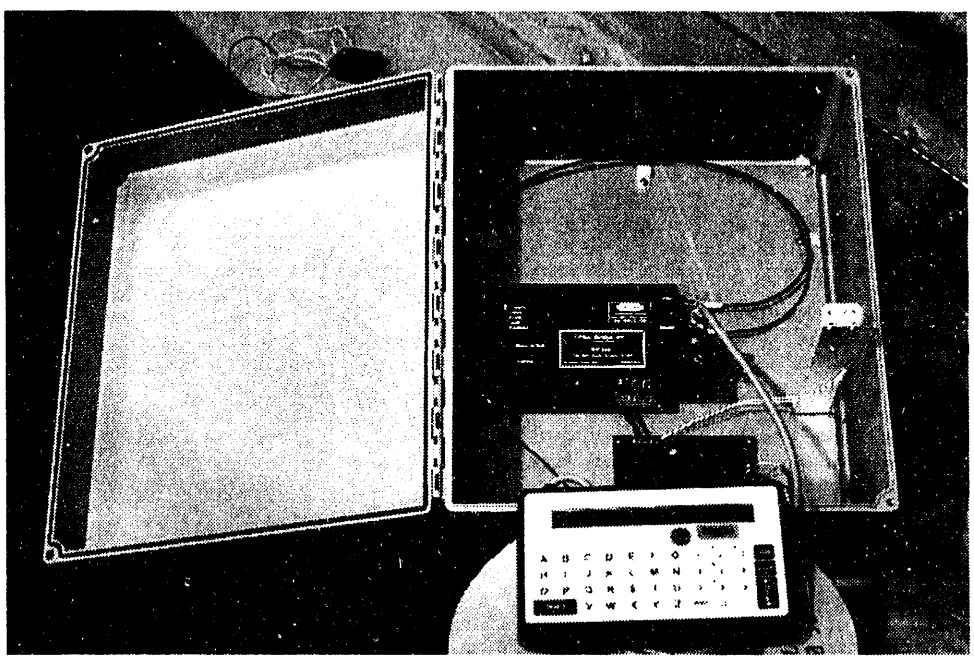

Figure 1. Fiber SenSys, Inc. Model M105E (M106E similar)

2.1.2 Operating Characteristics

The Fiber SenSys system has seven alarm processing parameters that are used to discriminate natural phenomena from an intruder. In order to get a better idea about how the system works, a discussion of the entire alarm process will follow. Each parameter will be italicized. Refer to figure 2 for a block diagram of the process.

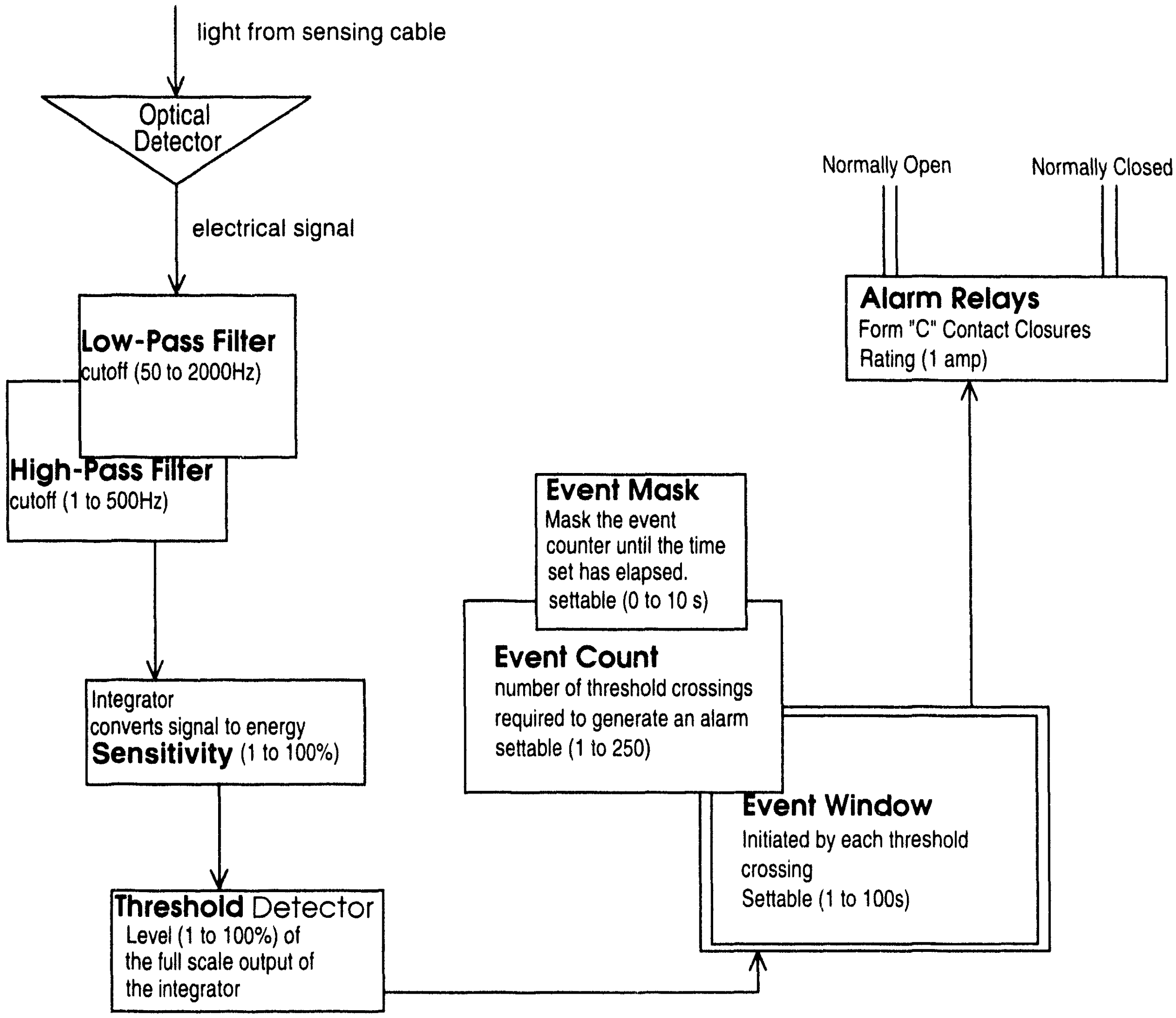

Figure 2. Block Diagram of Alarm Process

Alarm Process

First, light from the fiber strikes the detector which generates an electrical current proportional to the amount of optical interference. The current is converted to a voltage and then amplified. At this time, it passes through two programmable frequency filters that are used to eliminate unwanted frequencies. The *low-frequency cut-off* may be set in increments of 1 Hz from 1 to 500 Hz. The *high-frequency cut-off* may also be set in increments of 1 Hz from 50 to 2 KHz. Not all setting values are available above 200 Hz.

The processor chooses the closest value available and displays that value in the upper line of the display.

After filtering, the signal is rectified to create a DC voltage with an average amplitude proportional to the transmitted power absorbed by the fiber. At this point, the voltage is digitized and then integrated. The *Sensitivity* parameter changes the characteristics of the integrator by changing the rate of the integration. The Sensitivity setting may be set in increments of 1 from values of 1 to 100 percent. When 100 percent is chosen, the integrator is set at its longest time period. This is the most sensitive setting for this parameter. The *Threshold* parameter would correspond to the accumulated voltage (transmitted power). The threshold may be set from 1 to 100 percent of the full scale output of the integration circuit. When the signal reaches this point, it qualifies as an event.

When an event occurs, a timer is initiated (*event window*) that is selectable from 1 to 100 seconds. If another event occurs before this window of time elapses, the event counter is incremented by 1 and the timer is restarted. If an event does not occur, the *event counter* is set to zero along with the event window timer. The *event counter* is selectable from 1 to 250 events. The *Event Mask Time* is also initiated by an event. Once an event occurs, the event is counted, but the counter will not increment until after the event mask time has elapsed and another event has occurred. Therefore, the event counter is masked from seeing any other events for a selectable time period of 0 to 9.99 seconds in increments of 33 milliseconds.

Other Parameters

Alarm Relay Time - The alarm will remain active until the time set for the alarm relay output has elapsed. It can be set from 1 to 1800 seconds.

Date code - The date can be recorded when the processor is set up or updated (YYMMDD).

Comment Field - The user may store any 30 character message with the alarm processor parameters selected.

Allow Disable? (Y/N) - The front panel switch on the M105/M106 has a position for disabling the unit. Entering "N" will not allow the switch to disable the unit.

Lock Unit? - If "Y" is entered, no alarm parameters may be changed without entering the password.

Version and Status Information

When the unit requests a password, the installer is able to access information about the alarm processor by entering the word "Version" or "Status." "Version" displays the model number, serial number, and firmware version and date. "Status" displays the optical power level, DC voltage level, laser current, and hours operated.

2.1.3 System Cost

The following table is a price schedule for the Fiber SenSys intrusion detection system:

Description	Unit Price
• M105E mounted in a NEMA enclosure with surge suppressor and tamper switch closure	$2,675.00
• M106E mounted in a NEMA enclosure with surge suppressor and tamper switch closure	$2,950.00
• Hand-held Calibrator	$1,350.00

Insensitive lead-in - transmit	Feet	Price
(used with M106)	0-100 ft.	$250.00
	100-499 ft.	$2.50/ft.
	500-999 ft.	$2.10/ft.
	1000-1499 ft.	$1.90/ft.
	1500-2499 ft.	$1.75/ft.
	2500-3200 ft.	$1.60/ft.

Insensitive lead-in - receive	Feet	Price
(used with M106)	0-100 ft.	$200.00
	100-499 ft.	$2.00/ft.
	500-999 ft.	$1.70/ft.
	1000-1499 ft.	$1.30/ft.
	1500-2499 ft.	$1.10/ft.
	2500-3200 ft.	$0.95/ft.

Sensing Cable	Feet	Price
	0-100 ft.	$150.00
	100-499 ft.	$1.50/ft.
	500-999 ft.	$1.15/ft.
	1000-1499 ft.	$1.00/ft.
	1500-2499 ft.	$0.90/ft.
	2500-3200 ft.	$0.85/ft.

2.2 Sabrefonic System

2.2.1 System Description

The Sabrefonic system is a single channel FOD system designed for various types of fence such as chain link, welded mesh or palisade, and other building fabrics. This system incorporates the use of the speckle pattern technique as its means for detection. It is designed to detect frequencies that occur during climbing or cutting of a fence. The electronics (the processing electronics printed circuit board, input terminal block, and tamper switches) are installed in a waterproof polyester glass fiber reinforced enclosure.

Sensitivity and threshold parameters are set by adjusting voltage levels using a digital voltmeter. An analog output of the processing electronics PCB is also available so that the performance of the system can be monitored during setup. A digital multimeter or a chart recorder must be used to take advantage of this feature. The sensing cable is made out of a multi-mode 62.5/125 micron duplex fiber optic cable in a 4.8 mm loose PVC outer sheath. The optic signal is transmitted down one of the fibers in the duplex cable and returns on the other. An enclosure at the end of the cable contains a fusion splice that connects the two fibers. The cable assembly does not loop back to the processor. Figure 3 shows a picture of the Sabrefonic unit inside an enclosure.

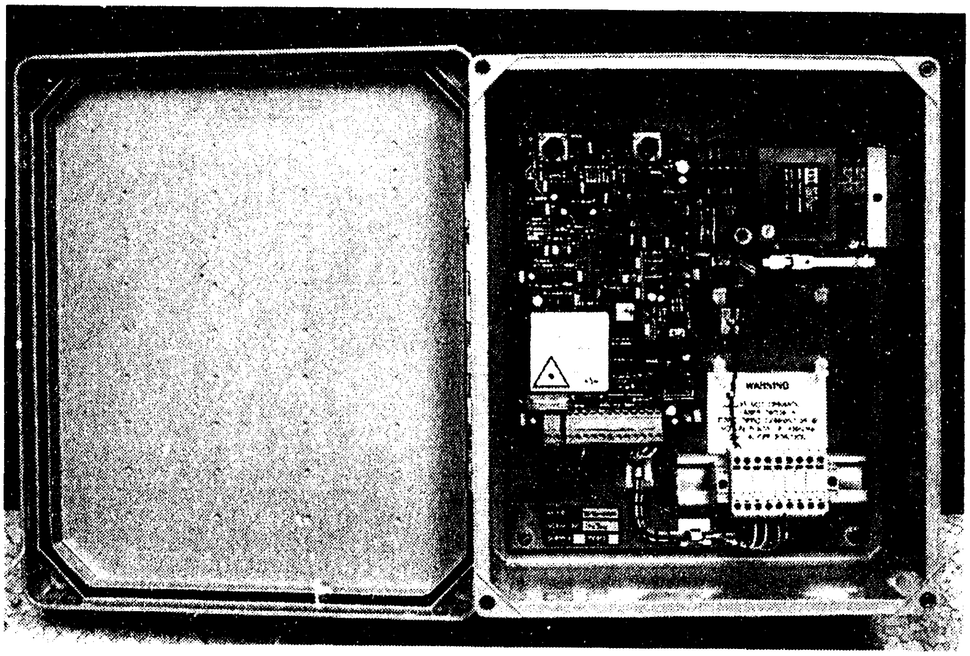

Figure 3. Sabrefonic System

2.2.2 Operating Characteristics

The Sabrefonic system can be powered by a 12 volt dc source or by 120 volt ac (transformer included). The system requires a voltage between 11 and 13.8 volts for operation. All switches, LEDs, and setup controls (potentiometers) are located on the PCB. A red LED indicates that the laser diode is operational. A green LED indicates that the fiber optic path is complete.

Threshold

Threshold can be set in an automatic mode or a manual mode. The automatic threshold setting automatically adjusts the alarm threshold to compensate for background noise. The manufacturer recommends using the automatic mode. The automatic threshold under normal conditions is set at negative one volt. If the background noise increases, the threshold voltage increases.

Sensitivity

The sensitivity is set by adjusting a potentiometer and using a digital multimeter connected across TP5 and TP6. Initial recommended setting is -0.5 volts. Final setting is accomplished after detection testing. The manufacturer recommends adjusting the sensitivity in .1 volt steps. Decreasing the voltage increases the sensitivity and vice-versa.

Alarm Delay

The Sabrefonic has an automatic alarm reset adjustment. This is set by using a 4 switch dual-in-line package, with settings of 1.5 seconds, 3 seconds, 6 seconds, and 12 seconds. A total delay of 22.5 seconds can be set.

Event Counter

The event counter is used to count the number of times the system has detected an intrusion. The counter is capable of counting events from 1 to 15.

Event Counter Time

A time period selector is available to select the required time period for the selected number of events to occur. Any combination of the following times can be selected: 1.2 seconds, 4.8 seconds, 19.2 seconds, and 38.4 seconds.

2.2.3 System Cost

The following is a price schedule for the Sabrefonic intrusion detection system:

Description	Price
• Processor PCB on baseplate with terminal strip	$1,365.00
• Processor PCB mounted in NEMA 4 enclosure with tamper switch, and 115 VAC/12 VDC converter/transformer	$1,955.00
• Fiber optic sensing cable	$1.46/ft.
• Event counter	$285.00
• Pre-terminated sensor cables with connectors (SMA)	$189.00

2.3 Sabreline System

2.3.1 System Description

The Sabreline is a single channel FOD system designed for exterior buried applications such as under grass, sand, gravel, roads, or roofs. This system also uses the speckle pattern technique as its means for detection. The Sabreline is designed for detecting low frequencies associated with walking on the ground. The electronics (the processing electronics printed circuit board, manual threshold adjust control, input terminal block, and tamper switches) are installed in a waterproof polyester glass fiber reinforced enclosure.

Sensitivity and threshold parameters are set by adjusting voltage levels using a digital voltmeter. An analog output of the processing electronics PCB is also available so that the performance of the system can be monitored during setup. A digital multimeter or a chart recorder must be used to take advantage of this feature. The sensing cable is made out of a multi-mode 100/140 micron tight buffered fiber optic cable that can be supplied, pre-terminated, at any length of up to 3,300 feet. The system can be powered by a 12 volt dc source or by 120 volts ac (transformer included). Figure 4 shows a picture of the Sabreline inside an enclosure.

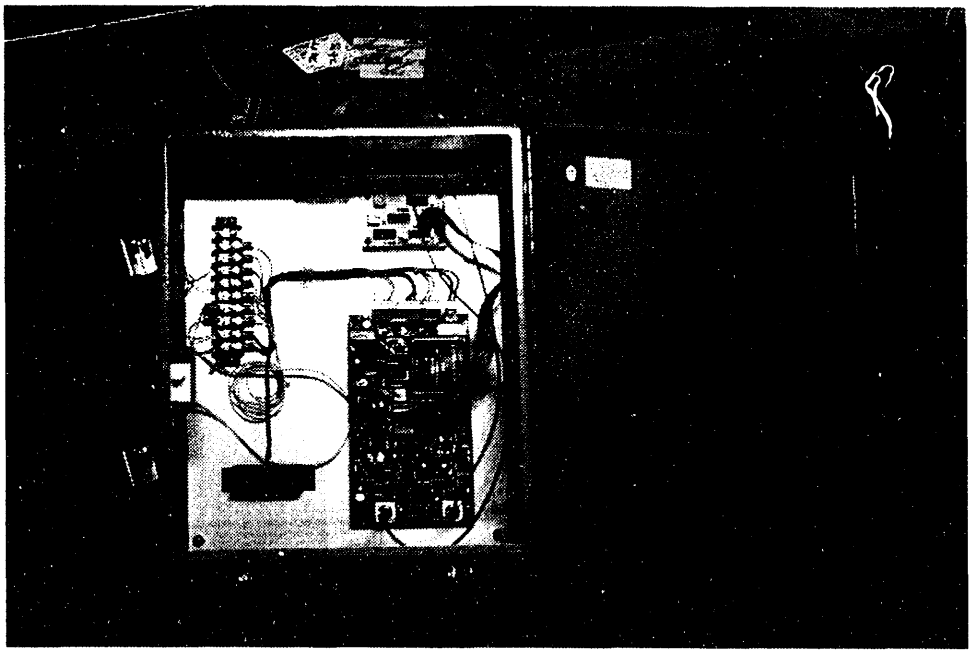

Figure 4. Sabreline System

2.3.2 Operating Characteristics

The system requires nominal 12 volts DC for operation. All switches, LEDs, on/off switch, and voltage level controls are located on the PCB. A red LED indicates that the laser diode is operational. A green LED indicates that the fiber optic path is complete. The power of the laser needs to be adjusted for various lengths of fiber. This is accomplished by placing a voltmeter between TP5 and TP2 and turning RV2 clockwise until the meter reads a specified voltage. For fiber less than 900 feet, the voltage must be set at 900 mv; for fibers 900 feet to 2,400 feet, the voltage must be set at 800 mv; and for fibers greater than 2,400 feet, the voltage must be set at 700 mv.

Threshold

The manual threshold mode is the preferred method for the Sabreline system. In this mode the alarm threshold does not automatically compensate for background noise. The manual threshold sets the threshold at a negative one volt. Switch 5 (SW5) must be set at MT for manual threshold adjustments.

Sensitivity

Sensitivity is set by adjusting potentiometer (RV1), while measuring the voltage across test points 5 and 6. For initial set up, the voltage should be adjusted to 500 mv. The sensitivity should be tested at this setting. When the system alarms, the green LED extinguishes. If the system is not sensitive enough, decreasing the voltage will increase the sensitivity.

Alarm Delay

The Sabreline has an automatic alarm reset setting. The delay can be set by using a 4 switch dual-in-line package, with switch settings of 1.5 seconds, 3 seconds, 6 seconds, and 12 seconds. A total delay of 22.5 seconds can be set.

Event Counter

The event counter is used to count the number of times the system has detected an intrusion. The counter is capable of counting events from 1 to 15.

Event Counter Time

A time period selector is available to select the required time period for the selected number of events to occur. Any combination of the following times can be selected: 1.2 seconds, 4.8 seconds, 19.2 seconds, and 38.4 seconds.

2.3.3 System Cost

The following is a price schedule for the Sabreline intrusion detection system:

Description	Price
• Processor PCB on base plate with sensitivity control and terminal strip (without NEMA enclosure)	$1,375.00
• Processor with tamper switch, water proof NEMA 4 enclosure (for underground installations), sensitivity control, terminal strip and 115 to 12 VDC converter	$1,825.00
• Processor with tamper switch, NEMA 4 enclosure (for post-mounted installations), and 115 to 12 VDC converter	$1,675.00
• Fiber optic sensing cable	$.84/ft.
• Event counter	$285.00
• Pre-terminated sensor cables with connectors (SMA)	$160.00

2.4 Mason & Hanger National, Inc. FOIDS Model 1000

2.4.1 System Description

The Fiber Optic Intelligent Detection System (FOIDS) 1000 is a single channel FOD system designed for both interior and exterior applications. The system uses interferometric techniques as its means for detection. The FOIDS 1000 is designed to detect frequencies between 10 and 1000 hertz when set in the "A" mode. The "B" mode by-passes the filter. Besides the A/B frequency mode select, there is only one setup parameter adjustment for sensitivity.

The system consists of a power/audio module and a laser module. It is designed to be a stand-alone or rack-mounted unit when eight laser modules are used in conjunction with the power module. The sensing cable is single-mode fiber optic cable. The transmitter laser operates at a wavelength of 1300 nm. The FOIDS 1000 is one of three units manufactured by Mason & Hanger. They also manufacture a Model 500 and a Model 3000. The Model 500 is advertised with the following features: small and lightweight, user adjustable sensitivity control, event pulse counter, false alarm reject (time window), enhanced audio feature, headphone/speaker/line out for audio monitoring, universal dry contacts, enhanced alarm discrimination, cut-loop detector with separate output strip, and ac/dc power operation. The Model 500 would have been the preferred system to test because of the additional settings available. However, the prototype was in the final stages at the time of the evaluation. Currently, the Model 500 is procurable. The Model 3000 is advertised with the following features: automatic sensor and system self-checking, enhanced zone sensitivity and alarm parameter control, enhanced acoustics, multiple alarm discrimination features, custom-designed graphics, supports unlimited number of zones, fully compatible with other security and identification systems, keyboard or mouse use, and password controlled. Figure 5 shows a picture of the FOIDS 1000 with the power/audio module and three laser modules.

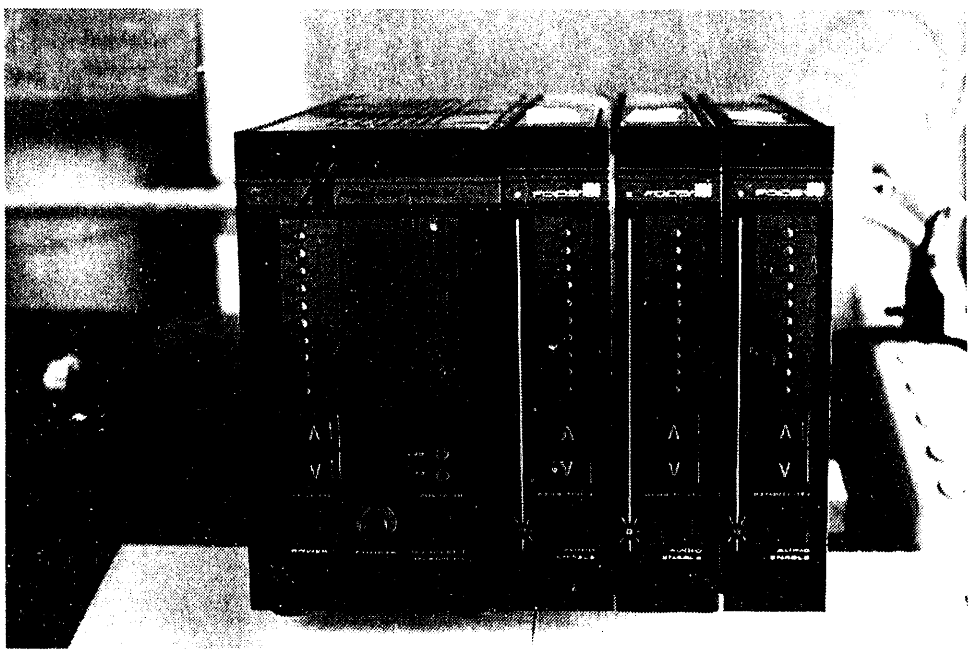

Figure 5. FOIDS Model 1000

2.4.2 Operating Characteristics

Power/Audio Module

The Power/Audio Module has the following indicators and controls (refer to figure 6):

1. *Volume Indicator Lights* - gives visual indication of relative volume of sound for external speakers or head phones.
2. *Volume Controls* - adjusts sound level for comfortable listening.
3. *12 volt Positive and 12 volt Negative Lights* - green light indicates voltage is normal. Flashing red light indicates voltage is low.
4. *Power Switch and Light* - power to laser module.
5. *External Speaker Jack* - accepts 1/4 inch monaural speaker or headphone jack.

6. *Sonalert Override* - when depressed gives a 20 second pause in the alarm being generated by a particular sensor.
7. *DC-AC Switch* - allows switching between power source.
8. *110 V AC Power Receptacle* - connection for 110 volt power cord.
9. *12 V DC Power Receptacle* - connection for 12 volt DC source.
10. *Power Feed to Laser Module* - power connection to laser module.
11. *Fuse* - .5 amp/250 volt.

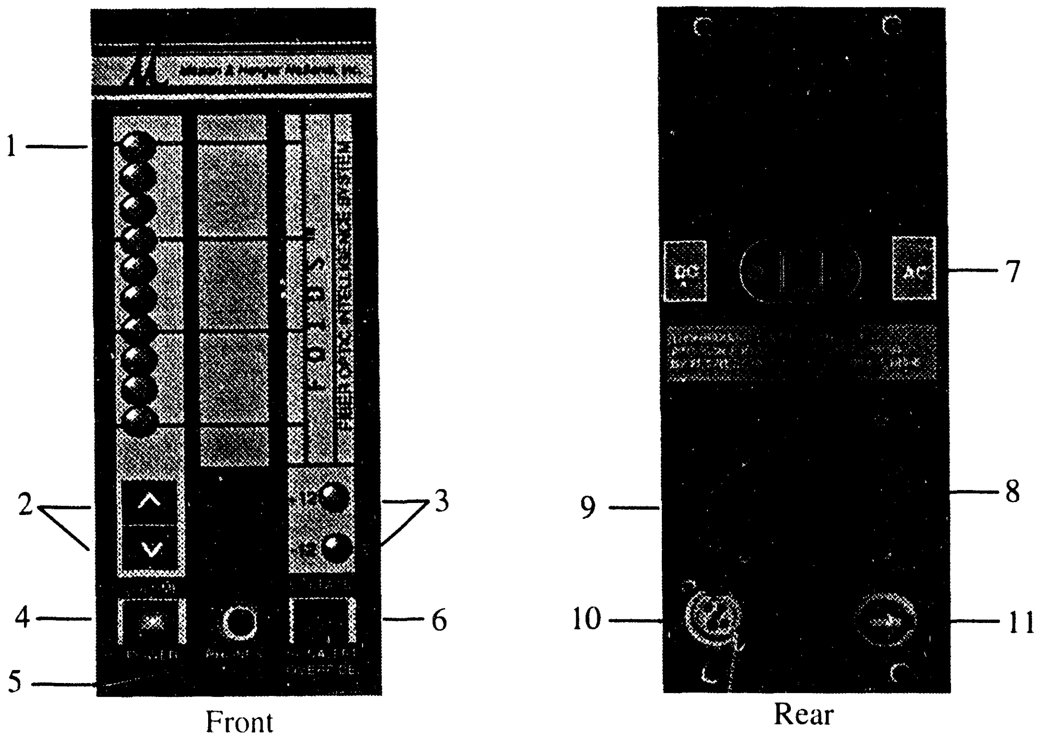

Figure 6. FOIDS 1000 Power and Audio Module

Laser Module

The Laser Module has the following indicators and controls (refer to figure 7):

1. *Laser Control Light* - visual indicator of relative sensor activity.
2. *Sensitivity Control* - increases or decreases relative sensitivity (10 being the most sensitive and 1 being the least sensitive).
3. *Laser on Light* - visual indicator that laser is operating.
4. *Audio Enable* - switches from sonalert to sound monitoring; external speaker or headphones must be used.
5. *NTT Couplers* - couples connector from fiber optic cable to laser module.

6. *Selector Switch* - selects between "A" - which is recommended for fence applications and "B" - all other applications. Essentially, "A" turns on the high pass filter, and "B" bypasses the filter. The high-pass filter is set at 1K hertz. In the "A" mode, the system is looking at frequencies between 10 hertz and 1K hertz.
7. *Terminal Board* - connects external components such as lights, CCTV, and alarm relays (normally open and normally closed).
8. *Power Out Cable* - connects to next laser module in series.
9. *Power in Jack* - connects power cord from adjacent laser module or power module.

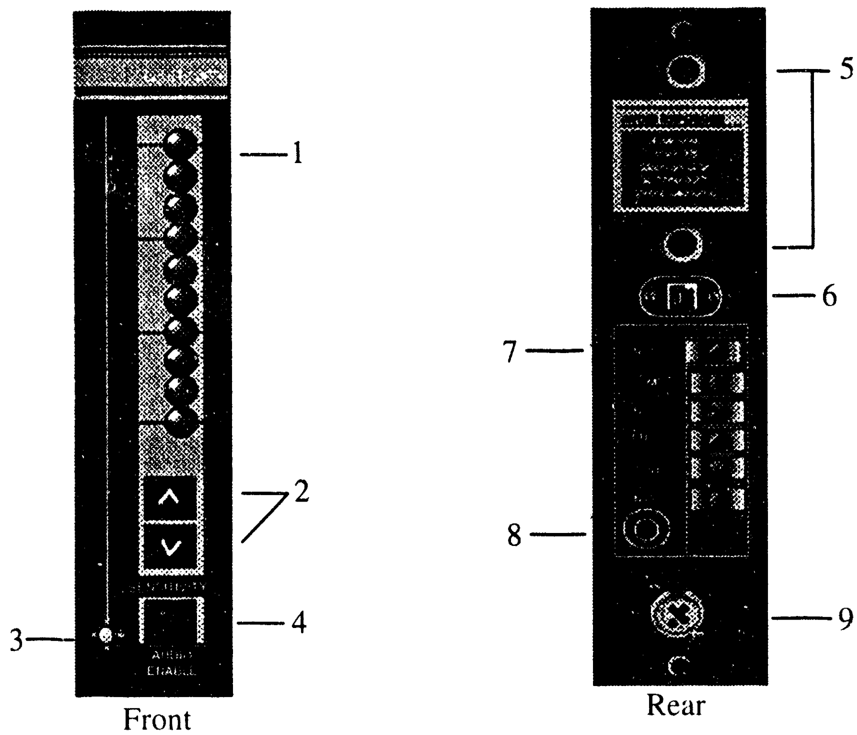

Figure 7. FOIDS 1000 Laser Module

2.4.3 System Cost

The following is a cost breakdown for the FOIDS system.

Description	Price
• Model 1000 Power/Audio Module (supports 8 laser modules)	$3,900.00
• Model 1000 Laser Zone Module	$1,900.00
• Sensor (includes connectors)	≈ .99/linear foot of fence
• Rack mounting kit	$80.00
• Optical splitter assembly (insensitive trunk line)	$460.00
• Model 500	$3,338.50
• Model 3000 Controller (other options available)	$15,000.00
• Model 3000 Laser Zone Modules	$4,000.00

3 Test Procedure

3.1 Setup and Equipment

The FOD systems were tested to evaluate their performance in different interior applications. These applications were on top of a suspended ceiling, under floor matting, and in a blanket.

A suspended ceiling in a mobile office was used for most of the tests. The objective was to detect an intruder entering the office areas through the ceiling tiles. The fiber optic cables were laid across the tiles adjacent to the offices being protected. The cables were situated where there were two strands of cable on each suspended ceiling tile, as shown in figure 9. The FOD systems were located in a nearby lab. Figure 8 shows the layout of the fiber optic sensing cable on the ceiling tiles, and figure 9 shows an actual picture of fiber optic cable on a ceiling tile.

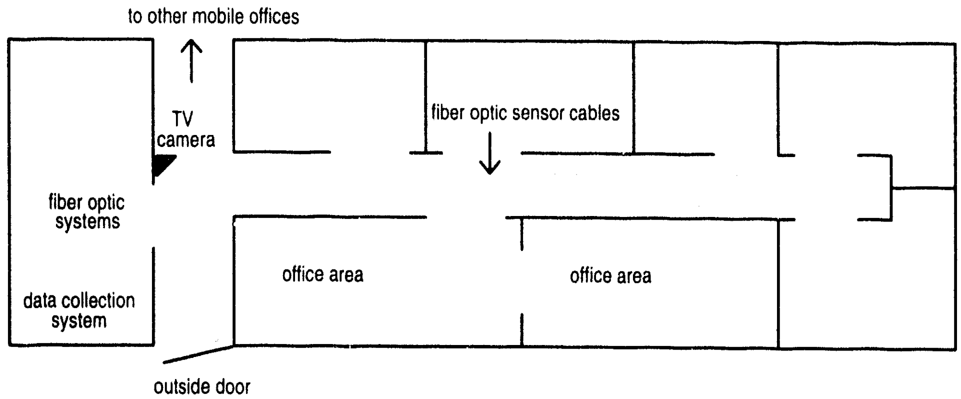

Figure 8. Top View Layout of Sensing Cables

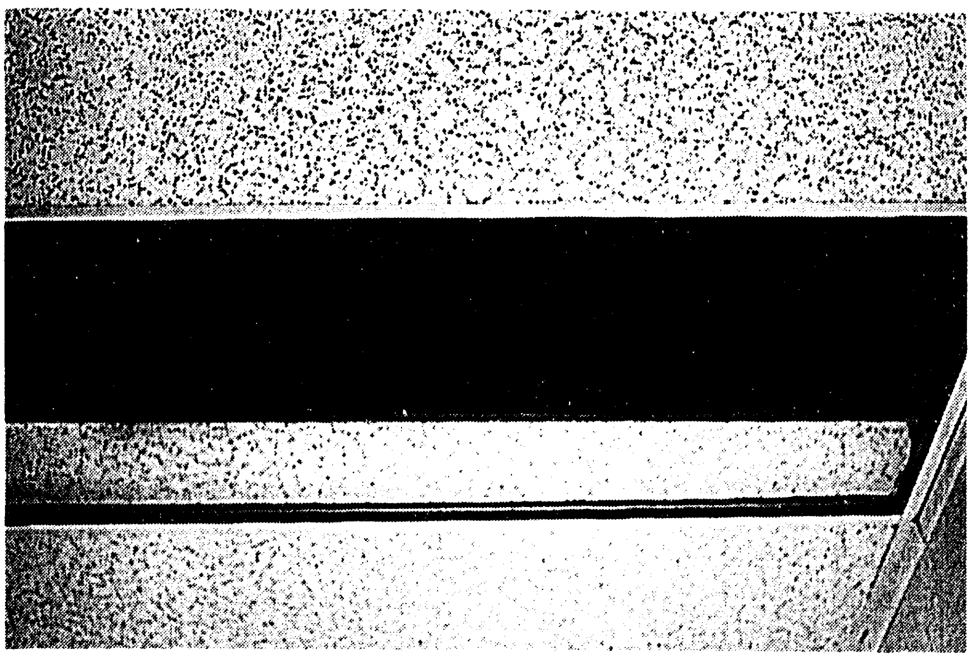

Figure 9. Fiber Optic Cable on Suspended Ceiling

3.2 Procedure

Suspended Ceiling Application

On-going detection tests were concentrated in one area and involved lifting one ceiling tile. Testing consisted of initial setup for high detection rates and subsequent detection tests to verify detection and nuisance alarm monitoring. A test consisted of (1) slowly lifting the tile, (2) sliding it over enough to where an average person could crawl through, and (3) moving the fiber optic cable far enough out of the way to where an average person could crawl through. A complete test averaged from 1.5 to 2.5 minutes.

The more times the test was done, the easier it was to maneuver the tile without much of a disturbance to the fiber optic sensor cables. Different sensitivity and threshold settings were implemented to determine high detection rates, keeping in mind nuisance alarms. A minimum of fifteen detection tests per setting were completed.

Nuisance alarm data was gathered using a video camera and a time-lapse video recorder for visual assessment and a personal computer for alarm event recording. Different thresholds were used throughout the nuisance alarm data period to determine the best setting based on the NAR for this particular application. Time-lapse video recorders were set to record in a time-lapse mode with no alarms and switch to normal recording speed during an alarm. An in-house software program called a Nuisance Alarm Data System (NADS) was used to record the time each alarm occurred, the date, the sensor manufacturer, and the amount of time the data collection system was on. A separate part of the software allowed the user to assess and enter the cause of the alarm. Figure 10 shows a block diagram of the NADS.

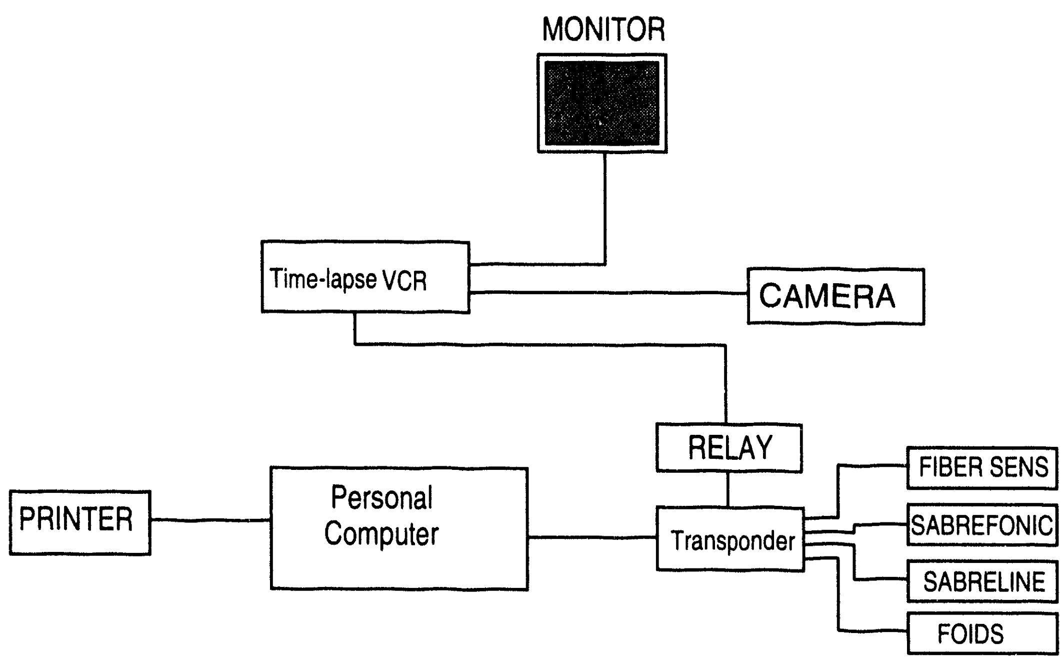

Figure 10. Nuisance Alarm Data Collection System

4 Test Results

4.1 Nuisance Alarms

The following is a list and description of the nuisance/false alarms encountered during the nuisance alarm data collection period.

Unknown Alarms

Unknown alarms are alarms for which the causes cannot be identified on the videotapes. Winds gusting as high as 27 mph may have caused these alarms. Other possible sources for unknown alarms include mice walking on the fiber cable, jets flying close to the ground, sonic booms, or power glitches.

Unassessed Alarms

Unassessed alarms are alarms that could not be assessed due to either no video or the NADS not setup to turn on the time-lapse recorder. The NADS was programmed to record 20 alarms with the time-lapse recorder; after 21 alarms, it will only count the alarms.

Door Alarms

Outside door alarms are alarms that were caused by the outside door slamming. Some of the alarms occurred on windy days, causing the door to slam very hard. Most of the door alarms were caused by a total of three doors closing, since the event count was set at three. For example, a person leaving for the day would close his office door, the lab door, and then the outside door closing within the event window. This was true for the Fiber SenSys system. Inside door alarms are alarms that were caused by office doors opening or closing. Most of the alarms occurred when a total of three doors closed or opened within the event window (e.g., the outside door and two office doors, or vice versa). Again, this was true for the Fiber SenSys system.

Windstorm

Windstorm alarms were caused during very windy days. A spectrum analyzer was connected to the Fiber SenSys during the storm. The display showed, throughout the storm, the noise level being much higher, fluctuating between 1 and 200 hertz. The building was actually vibrating; wind gusts were as high as 57 mph.

Vibration alarms

Vibration alarms are alarms that happened when the mobile office started vibrating for no known reason. It did not appear to be caused by the air conditioner.

No video alarms

No video alarms are alarms that occurred when the camera was not operating.

4.2 Fiber SenSys Model 105/106 Detection Results

4.2.1 Suspended Ceiling Application

Evaluation and testing of the Fiber SenSys, Inc., fiber optic sensor began with a Model M106. This particular unit had been on-hand for some time, being temporarily installed at various locations and demonstrated during a precursory look at fiber optic sensors. Two problems with the unit occurred during testing. The problems happened at different times. Symptoms of the problems were intermittent periods of false alarms and a noted decrease in sensitivity. The false alarm problem was due to an unstable laser in the processor module. Decreased sensitivity was related to a defective connector on a lead-in cable. It is not known whether the pre-evaluation operation and installations directly caused the problems. The Fiber SenSys staff has been very helpful and supportive in resolving problems with their system.

They recommended that an M105 would be better suited for the interior ceiling application. This resulted with continued testing using a new M105. The detection tests and nuisance alarm data gathered on the M106 was considered invalid because of the problems with the M106 and possible degraded operation for some period of time. Unfortunately, most of the data was collected on the M106.

Fiber SenSys did not recommend any specific settings for a suspended ceiling application. However, configuration hints for selecting proper settings were provided. Many different variations of the parameters were tested. The most effective settings for 100% detection, keeping in mind nuisance alarms, are shown in Table 1. For most of the tests, the low-cutoff frequency was kept at 1 Hz, the high-frequency at 50 and 100 Hz, the event count at 3, the event mask time at 1 second, and the alarm relay time at 2 seconds.

Table 1. Required Sensitivity Settings for 100% Detection

Model M105	Sensitivity	Threshold
Setting #1	50%	50%
Setting #2	35%	50%

With the above parameters, 100% detection was achieved. With these parameters, the system would detect as the tile was being pushed up. Sensitivity of 50% and threshold of 50% is the most sensitive of the two. Please note that these settings are not the only settings that will provide a high detection rate.

4.3 Fiber SenSys Model 105 Nuisance Alarm Results

Since the lead-in cable had developed a problem during testing with the M106, all of the nuisance alarm data was considered invalid. The total time amounted to approximately 1,098 hours. The degradation of sensitivity fell to a detection rate of about 70%. With the M105, a total of 612.67 hours of nuisance alarm data was collected. Two settings were used to investigate the detection versus nuisance alarm trade-off. Figure 11 shows the number of alarms for each source.

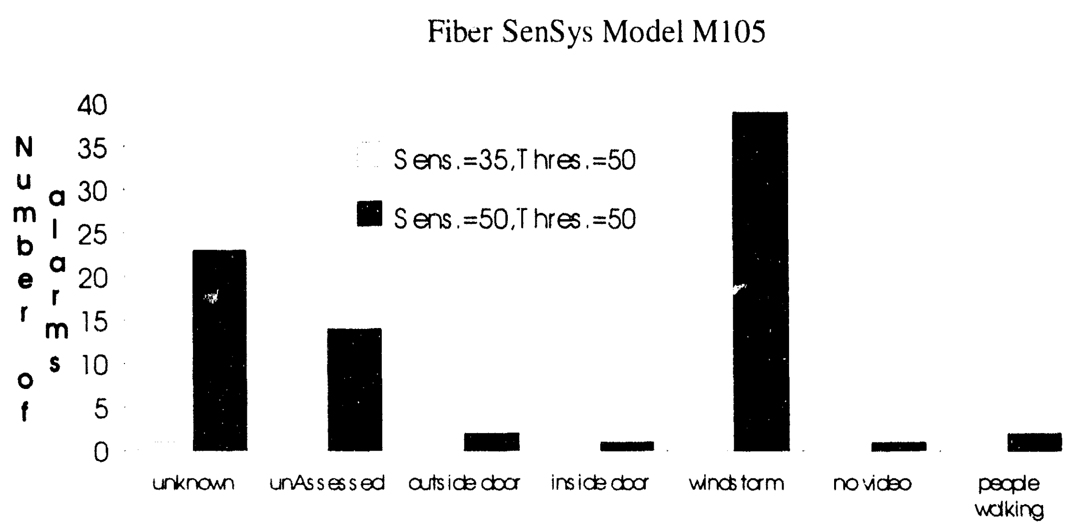

Figure 11. Fiber SenSys Model M105 Nuisance Alarms

Table 2 shows the parameters used for nuisance alarm data collection, the total hours, and the number of alarms minus test alarms.

Table 2. Fiber SenSys Nuisance Alarms

Parameters	Total Hours	Number of Alarms
Sens. = 50%, Thresh. = 50%	310.50	82
Sens. = 35%, Thresh. = 50%	302.17	1

4.4 Sabreline System Detection Results

4.4.1 Suspended Ceiling Application

The Sabreline system was able to detect 100% of the tests with the event count = 1 and the event count = 3. However, detection occurred at different movements during the tests. For example, it would sometimes detect as the tile was pushed up, at the beginning of the tile movement, towards the end of the tile movement, and sometimes during sliding of the cable. The most effective settings for good detection, keeping in mind nuisance alarms, are shown in Table 3. Besides the event count, the threshold voltage was the only parameter needed for adjustment of the sensitivity.

Table 3. Sabreline Settings Needed For Good Detection

Event Count = 1	Detection Rate	Event Count = 3	Detection Rate
Threshold = .5 volts	100%	Threshold = .4 volts	100%
Threshold = .6 volts	95%	Threshold = .5 volts	90%

4.5 Sabreline System Nuisance Alarm Results

For the Sabreline, a total of 767 hours of nuisance alarm data was collected with the event count = 1. Two threshold voltages were used to investigate the detection versus alarm trade-off. A total of 472 hours of nuisance alarm data was collected with the event count = 3. Two threshold voltages were also used to investigate the detection versus alarm trade-off. Figure 12 shows the number of alarms from each source and includes data from event count 1. Figure 13 includes data from event count 3.

Sabreline System

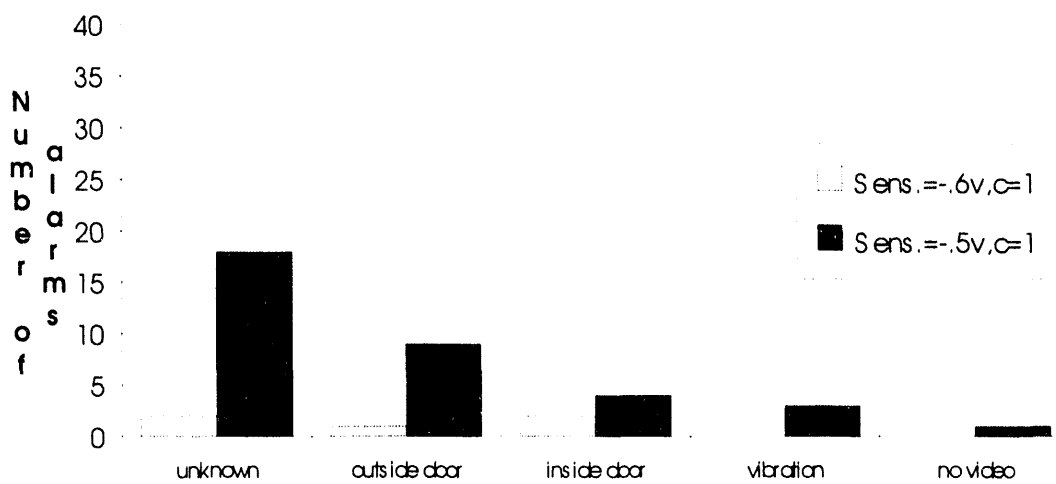

Figure 12. Sabreline Nuisance Alarms Using Event Count 1

Sabreline System

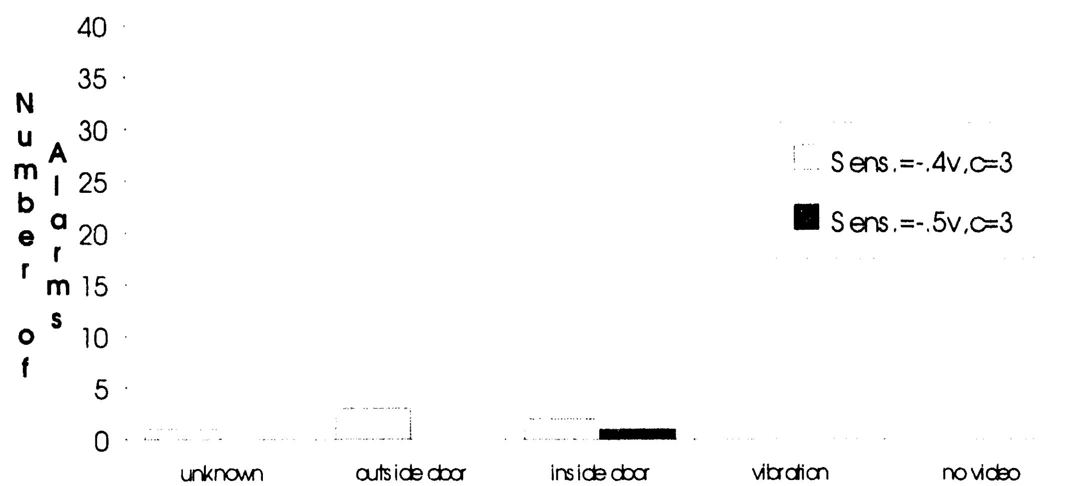

Figure 13. Sabreline Nuisance Alarms Using Event Count 3

Table 4 shows the parameters used for nuisance alarm data collection, the total hours, and the number of alarms.

Table 4. Sabreline Nuisance Alarms

Parameters	Total Hours	Number of Alarms
.5v, count = 1	407	36
.6v, count = 1	360	5
.4v, count = 3	292	6
.5v, count = 3	180	1

4.6 Mason & Hanger FOIDS 1000 Detection Results

4.6.1 Suspended Ceiling Application

The FOIDS system was very simple to find a setting for 100% detection because it only has one parameter for adjustment. The setting is adjustable from one to ten, with ten being the most sensitive. The switch setting on the back of the unit was set on "A," which is for detecting frequencies between 10 and 1000 Hz. The most effective setting, keeping in mind nuisance alarms, for 100% detection was at "4." With this setting, the system was able to detect at the beginning of the tile movement. A setting of "3" would give a detection rate of approximately 95%. However, with this setting, detection occurred at different movements during the tests. A setting of "2" would give a detection rate of approximately 70%. Table 5 summarizes the detection rates.

Table 5. FOIDS 1000 Detection Rate

Sensitivity	Detection Rate
4	100%
3	95%
2	70%

4.7 Mason & Hanger FOIDS 1000 Nuisance Alarm Results

For the FOIDS 1000, a total of 1,275 hours of nuisance alarm data was collected. Two settings were used to investigate the detection versus alarm trade-off. A total of 409 hours were collected with a setting of "4," and a total of 866 hours with a setting of "3." Figure 14 shows the number of alarms from each source and includes both settings.

FOIDS Model 1000

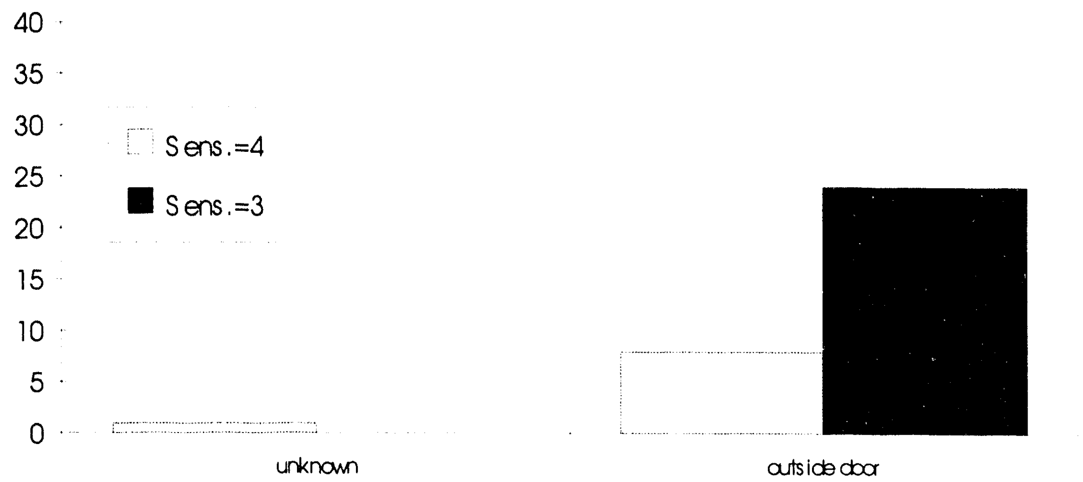

Figure 14. FOIDS Model 100 Nuisance Alarms

Table 6 shows the parameters used for nuisance alarm data collection, the total hours, and the number of alarms.

Table 6. FOIDS Model 1000 Nuisance Alarms

Sensitivity	Total Hours	Number of Alarms
4	409	11
3	866	24

5 Other Applications

Concrete Floor Application

The second set of tests were implemented in a concrete, earth burmed, storage bunker at Sandia's Video Technology Lab (VTL). The objective was to test the FOD systems under floor matting for detection of movement across the matting. The FOIDS, Sabreline, and Fiber SenSys were used in this test setup. The three fiber optic cables were placed side-by-side in a serpentine fashion across the concrete floor. The cables were spaced approximately six to seven inches apart in a 8' x 20' area. Figure 15 shows a picture of the fibers and floor mats used for the tests.

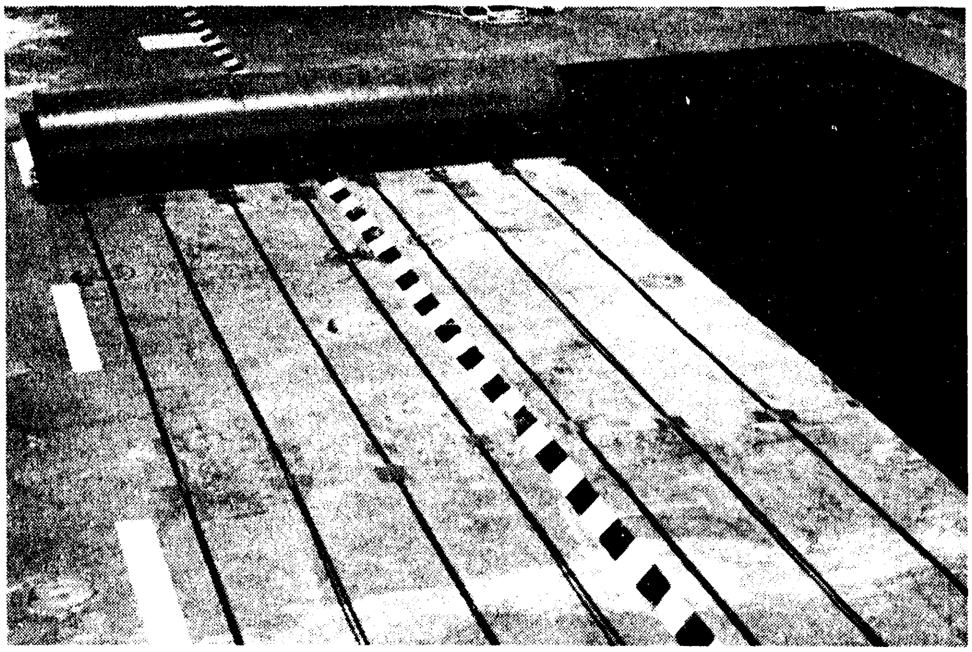

Figure 15. Fiber Optic Cable on Concrete Floor

Procedure

A short set of detection tests were implemented on the three FOD systems. Preliminary tests were done to see how different speeds affect the performance of each system. The speeds were 36 inches/second (normal walk), 5 inches/second, and 1 inch/second. A slow, soft step test was also implemented. These tests did not necessarily deal with speed, but rather concentrated on taking slow, soft, steady steps. A minimum of ten walk tests were implemented for each parameter tested. The tester weighed approximately 165 pounds. Nuisance alarm data was collected for two weeks. However, no video assessment was incorporated. All alarms were designated as unknowns.

Test Results

For all of the systems, the slow, soft steps affected detection capabilities the most. The Sabreline and FOIDS were most sensitive to the 5 inch/second and 1 inch/second speeds because of the number of steps taken. The additional steps taken makes it more susceptible for causing vibrations. In a sense, it does not really matter how slow a person walks; what matters is how soft a person walks. This was verified during testing because in some of the tests, a 1 inch/second walk would cause more alarms than a 5 inch/second walk. Therefore, the rest of the tests were done to find parameters that would detect a person taking continuously slow, soft steps.

Fiber SenSys

The Fiber SenSys M105 was able to detect all of the step tests. The slow, soft step test was the most difficult for the Fiber SenSys. It was, however, able to detect 100% of the slow, soft steps with very sensitive settings. For all of the tests, the low-cutoff frequency was kept at 1 Hz, the high-frequency at 100 Hz, and the alarm relay time at 2 seconds. Refer to table 7 for settings tested for 100% detection of the slow, soft steps with resulting nuisance alarm data.

Table 7. Fiber SenSys Nuisance Alarm Results for Concrete Application

Sensitivity	Total Hours	Number of Alarms
sens. = 90%, thresh. = 5%, count = 2, event mask time = 1 sec.	141 hrs.	2
sens. = 90%, thresh. = 5%, count = 2, event mask time = .495 sec.	65 hrs.	95
sens. = 90%, thresh. = 10%, count = 1, event mask time = .495 sec.	42.5 hrs.	8
sens. = 100%, thresh. = 10%, count = 2, event mask time = 1 sec.	25 hrs.	140

Sabreline System

The Sabreline was able to detect all of the step tests. The slow, soft steps were also the most difficult for this system. The most effective setting used to detect 100% of the slow, soft steps was a threshold voltage of -.3 volts with the event count set at one. Refer to table 8 below for nuisance alarm data and detection rates for the slow, soft steps.

Table 8. Sabreline Nuisance Alarm Results for Concrete Application

Sensitivity	Total Hours	Number of Alarms	Detection Rate
Threshold = -.3v, count = 1	254 hours	0	100%
Threshold = -.4v, count = 1	3 hours	0	70%
Threshold = -.5v, count = 1	17 hours	0	<50%

Mason & Hanger FOIDS 1000

The FOIDS system was able to detect a normal walk, but was not able to detect the slow, soft steps or the 5 inch/second and 1 inch/second steps. It detected approximately 25% of the tests. It was able to detect normal steps with the most sensitive setting. The most sensitive setting of 10 was used.

The FOIDS system was monitored for a total of 164.5 hours. Zero alarms occurred during that period. Two settings were used to investigate the detection versus alarm trade-off. The settings were with the sensitivity equal to 10 and both switch settings A and B. Refer to table 9 for below for nuisance alarm data and detection rates for normal steps.

Table 9. FOIDS Nuisance Alarm Results for Concrete Application

Sensitivity	Total Hours	Number of Alarms
10/A	114.5	0
10/B	50	0

Fiber Optic Blanket

Another application that was tested for another project involved protecting items with the use of a fiber optic blanket. A prototype fiber optic blanket assembly was constructed using the Fiber SenSys M105 system. It consisted of a canvas tarp folded once in half. Fiber optic sensor cable was tie-wrapped, in a serpentine fashion, to a plastic construction fence material and sandwiched between the canvas folds. The construction fence material served to keep the fiber sensor cable from bending to less than the minimum specified bend radius. The blanket was placed over a weapon mockup and was used to detect weapon tampering or movement. The blanket was very sensitive to slight movement and pressure. It was monitored for nuisance/false alarms for a period of 1 month. Two nuisance/false type alarms occurred over a weekend with stormy weather. The alarms may have been caused by power outages. Figure 16 below shows the blanket covering a weapon mockup.

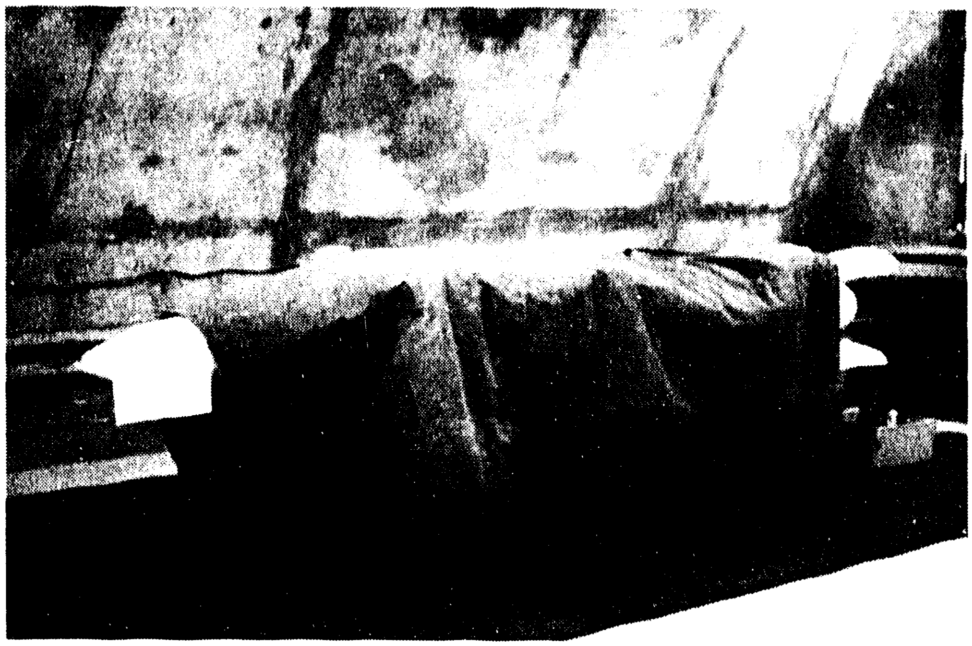

Figure 16. Fiber Optic Blanket Covering Item

6 Summary

The systems tested could be setup for high detection rates in most applications tested. The main factor was considering false/nuisance alarms. The Sabrefonic system being advertised as a fence sensor was tested in a ceiling application. The frequencies generated in a fence disturbance, which the processor is looking for, is much higher than those generated by lifting tiles or walking on carpet. The results of the test showed that the sensitivity needed for good detection in most interior applications would cause many false alarms. Also, it had a comparatively thicker and stiffer jacketing over the fiber cable, which made it difficult to install above the ceiling and would also cause problems installed under carpeting.

Suspended Ceiling Application

All of the detection testing in the ceiling application was done on one ceiling tile. After a while, this ceiling tile was very easy to remove. Keep in mind that most ceiling tiles are not very easy to remove. Therefore, the detection tests on this ceiling tile gave us a worst case scenario. The number of strands placed on the tile could also increase the sensitivity. Another way of increasing the detection capability is to actually fasten the cable to the supports with tie wraps. This would allow the user to decrease the sensitivity, thus decreasing the nuisance/false alarm rate because an intruder would now have to use more force to remove the tiles. However, this would somewhat hinder maintenance. Another problem that occurs is the assessment of alarms. While it is very easy to monitor the area below the ceiling tiles, it is very difficult to monitor above the suspended ceiling. A possible scenario would be an intruder somehow bridging across the hallway from an adjacent office above the suspended ceiling.

As far as nuisance/false alarms, the FOD systems performed fairly well. Approximately two months of data was collected with most of the data collected during the evenings on weekdays and 24 hours over the weekends. The majority of the false/nuisance alarms occurred during working hours. Most of the alarms were caused by doors closing or slamming. Keep in mind that the tests were performed in a mobile office; therefore, the construction of the building would more than likely make a difference in the NAR, because of the higher resonant frequencies found in mobile office construction.

Concrete Floor Application

In the concrete floor application, the Mason & Hanger was able to detect a normal walk, but was not able to detect 100% of the slow, soft steps. The Sabreline and Fiber SenSys were able to detect the slow, soft steps. The settings needed for high detection rates were very sensitive, which is fine, because the bunker was a very solid structure with little or no activity inside. The nuisance/false alarms were low once a reliable setting was chosen. For example, the Fiber SenSys false alarms were caused by the sensitivity being too high. When installing cables on concrete floors, it might be a good idea to install some type of material or matting that would give a little when stepped on. This might increase the sensitivity and/or would allow decreasing the sensitivity keeping in mind NAR. Be aware that it is possible an intruder might be able to see the cables installed on the floor. This would allow an intruder to walk in between the cables without being detected. The smallest diameter fiber optic cable would be recommended for under carpet applications.

Comments/Suggestions

Of the systems tested, the Fiber SenSys offers the most flexibility because of the parameters it provides to adapt to any application, such as suspended ceilings, carpet, fences, and under gravel. The Mason & Hanger (FOIDS 1000) system was the easiest system to setup. The trade-off is that it does not have any room for adjusting to a particular application, and it does not come with an event counter. The Sabreline was also fairly simple to setup, and it does have the option of having an event counter. This system requires the use of a voltmeter and the steadiness of adjusting the potentiometer for setting thresholds. The potentiometer made it difficult to zero in on a particular setting. Another problem that occurred with the Sabreline was when the lights were turned on or off, the system would sometimes alarm. A 12-volt battery was used to power-up the system, and it did not alarm when the lights were turned off/on. However, the Sabreline would not alarm every time the lights were switched on or off. The Fiber SenSys had a problem operating with a power supply that was not well filtered or regulated. It was noticed that the power supply would cause a narrow bandwidth spike at 120 Hz, 240 Hz, etc. This spike would cause the system to alarm at higher sensitivities. The problems occurred with the M106 unit that was already on hand. The Mason & Hanger was the only system that did not alarm when power was turned off.

It probably would be a good idea to keep a fiber optic OTDR, fiber viewer, or optical power meter on hand to test the cable, because a bad cable will definitely hinder performance. It can also be deceiving; take for example the problems with the Fiber SenSys. Also, be aware of the applications used for each of the FOD systems. For example, the concrete floor application required sensitive settings for detection, whereas a mobile office floor may require less sensitive settings. In other words, take into consideration the construction of the building, activity, and threat.

Vulnerability to Defeat

Probability of detection (P_d), nuisance alarm rate, and vulnerability to defeat all measure the quality of a sensor. However, any given sensor application is vulnerable to defeat, even if it exhibits an acceptable NAR and P_d. Two basic methods for defeating a sensor are spoof and bypass. Spoof refers to employment of equipment and actions either to mask the intruder signal or to inhibit the electronics from producing an alarm during an intrusion through the sensor detection zone. Bypass refers to intruder ability to avoid the sensor detection zone.

As far as using the spoof method on the fiber optic detection systems, it would be extremely difficult, if not impossible to mask the intruder signal from the fiber cable. This is true because attempting to remove the outer jacketing to gain access to the bare fiber would more than likely cause an alarm. However, as with most sensors, it is possible to inhibit the electronics from producing an alarm during an intrusion through the sensor detection zone. Of course, an intruder would need access to the junction box, in order to adjust sensor parameters for less sensitivity. The Fiber SenSys System needs a security key interface and a security access code to change the system parameters. The security key interface is usually removed from the sensor system during normal operations. However, tamper alarms, line supervision, and full end-to-end self-test capabilities can diminish certain defeat methods.

Extremely slow and steady movement along with knowledge of the system is one method to bypass fiber optic detection systems, which is true of most other sensors. The speed cannot be quantified because steadiness of moving the cable is also a factor. Since Fiber Optic Detection Systems are fairly new sensors, more experience and knowledge needs to be gained on long term performance and defeat methods.

References

1. Malone, T., Rodriguez, J., "Interior Intrusion Detection Systems Technology Transfer Manual," SAND90-2833, March 1994.

DISTRIBUTION:

1 General George L. McFadden, Director
U.S. Department of Energy
Office of Security Affairs, IS-50
Washington, DC 20585

1 Mr. Edward J. McCallum, Director
U.S. Department of Energy
Office of Safeguards and Security, SA-10
Washington, DC 20585

1 David A. Jones, Director
U.S. Department of Energy
Policy, Standards, and Analysis Division, SA-12
Washington, DC 20585

1 Marshall O. Combs, Director
U.S. Department of Energy
Headquarters Operations Division, SA-14
Washington, DC 20585

1 Bryan Siebert, Jr., Director
U.S. Department of Energy
Office of Declassification, SA-20
Washington, DC 20585

1 William J. Desmond, Chief
Darryl Toms
U.S. Department of Energy
Physical Security Branch, SA-121
Washington, DC 20585

1 E. E. Wagner, Chief
U.S. Department of Energy
Personnel Security Policy, Procedures, Analysis Branch, SA-122
Washington, DC 20585

1 Larry D. Wilcher, Chief
U.S. Department of Energy
Technical and Operations Security Branch, SA-123
Washington, DC 20585

1 David W. Crawford, Chief
U.S. Department of Energy
Materials Control and Accounting Branch, SA-124
Washington, DC 20585

1 G. Bowser, Chief
U.S. Department of Energy
Assessment and Integration Branch, SA-131
Washington, DC 20585

1 Donald J. Solich, Chief
U.S. Department of Energy.
Weapons Safeguards and Security Operations Branch, SA-132
Washington, DC 20585

1 Avitus J. Heysel, Chief
U.S. Department of Energy
Production/Energy Safeguards/Security Operations Branch, SA-133
Washington, DC 20585

1 G. Dan Smith, Chief
Carl A. Pocratsky
U.S. Department of Energy
Planning and Technology Development Branch, SA-134
Washington, DC 20585

1 Charles C. Coker, Chief
U.S. Department of Energy
Physical Protection Branch, SA-141
Washington, DC 20585

1 Floyd McCloud, Chief
U.S. Department of Energy
Technical/Information Security Branch, SA-142
Washington, DC 20585

1 Kenneth Sanders, Director
U.S. Department of Energy
International Safeguards Division, IS-40
Washington, DC 20585

1 R. Crow, Director
U.S. Department of Energy
Office of RD&T Facilities, DP-65
Washington, DC 20585

1 William Hensley, Director
U.S. Department of Energy
Office of Field Security Oversight, DP-68
Washington, DC 20585

1 Glen S. Podonsky, Director
U.S. Department of Energy
Office of Security Evaluations, EH-4
Washington, DC 20585

1 Vincent J. Moskaitis
U.S. Department of Energy
Office of Plans, Technology, and Certification, EH-4.3
Washington, DC 20585

1 U.S. Department of Energy/AL
Central Training Academy
Attn: Don Jewell, Assistant Director
Stan Laktasic
PO Box 18041
Albuquerque, NM 87185

1 U.S. Department of Energy, SNSD/AL
Attn: David A. Gurule, Director
Security and Nuclear Safeguards Directorate
PO Box 5400
Albuquerque, NM 87185

1 Robert L. Windus, Security Manager
U.S. Department of Energy/BP
PO Box 3621
Portland, OR 97208

1 Charleton Bingham, Director
U.S. Department of Energy/CH
New Brunswick Laboratory
Safeguards and Security Division
Argonne, IL 60439

1 R. Green, Director
U.S. Department of Energy/ID
Special Services Division
785 DOE Place
Idaho Falls, ID 83402

1 E. Wayne Adams, Director
U.S. Department of Energy/NV
Safeguards and Security Division
PO Box 98518
Las Vegas, NV 89193-8518

1 William G. Phelps, Director
U.S. Department of Energy/OR
Safeguards and Security Division
PO Box 2001
Oak Ridge, TN 37831-857

1 Donald J. Ornick, Director
U.S. Department of Energy/SPRO
Security Division
900 Commerce Road East
New Orleans, LA 70123

1 J. A. Bullian, Director
U.S. Department of Energy/PNR
Safeguards and Security Division
PO Box 109
West Mifflin, PA 15122

1 Richard J. Levernier, Director
U.S. Department of Energy/RF
Safeguards and Security Division
PO Box 928
Golden, CO 80402-0928

1 J. L. Spracklen, Director
U.S. Department of Energy/RL
Safeguards and Security Division
PO Box 550, Mail Stop A6-35
Richland, WA 99352

1 Douglas A. Ash, Director
U.S. Department of Energy/OAK
Safeguards and Security Division
1301 Clay Street, Suite 700N
Oakland, CA 94612

1 George G. Stefani, Jr., Director
U.S. Department of Energy
Safeguards and Security Division
Schenectady Naval Reactors Office
PO Box 1069
Schenectady, NY 12301

1 Tom Williams, Branch Chief
Safeguards and Classification
U.S. Department of Energy/SR
Safeguards and Security Division
Savannah River Operations
PO Box A
Aiken, SC 29802

1 Larry Ogletree, Director
Office of Safeguards and Security
U.S.Department of Energy/SR
Safeguards Engineering and Projects Branch
PO Box A
Aiken, SC 29802

1 Larry Brown, Director
U.S. Department of Energy/SR
Security Management Division
Savannah River Plant
PO Box A
Aiken, SC 29802

1 R. W. Ponik, Deputy Director
Security Management Division
U.S. Department of Energy/SR
Safeguards Engineering and Projects Branch
PO Box A
Aiken, SC 29802

1 Steve Shelt
Office of Safeguards & Security
Information and Protection Branch
U.S.Department of Energy/SR
PO Box A
Aiken, SC 29802

1 Joan Christopher, Security Officer
U.S. Department of Energy
Western Area Power Administration
PO Box 3402
Golden, CO 80401

1 U.S. Department of Energy
Argonne National Laboratory
Attn: K. W. Poupa
D. G. Erick
9700 South Cass Avenue
Argonne, IL 60439

1 Manny Sanchez, Manager
U.S. Department of Energy
Argonne National Laboratory
Idaho site
PO Box 2528
Idaho Falls, ID 83403-2528

1 Joseph Indusi
U.S. Department of Energy
Brookhaven National Laboratory
Building 197C
53 Bell Avenue
Upton, NY 11973

1 Kris Dahms
U.S. Department of Energy
Brookhaven National Laboratory
Building 703
53 Bell Avenue
Upton NY 11973

1 Don Wentz, Deputy Manager
Safeguards and Security
U.S. Department of Energy
Lawrence Livermore National Laboratory
PO Box 808
Livermore, CA 94550

1 D. B. Smith/J. Tape, N-DO/SG
Los Alamos National Laboratory
Mail Stop: E550
PO Box 1663
Los Alamos, NM 87545

1 E. C. McGurren, Manager
Allied Signal, Inc.
Kansas City Division
Security Operations
Kansas City, KS 64131-3095

1 Steve Zvacek, Supervisor
Allied Signal, Inc.
Kansas City Division
Technical Security Section
Kansas City, KS 64131-3095

1 Battelle Memorial Institute
Technical Services Group
Attn: Mr. Dale Moul
505 King Avenue
Columbus, OH 43201-2693

1 W. C. Rogers, Manager
Laboratory Operational Safeguards
Bettis Atomic Power Laboratory
Westinghouse Electric Corporation
PO Box 79
West Mifflin, PA 15122-0079

1 J. Dollinger, Security Department
Boeing Petroleum Services
850 South Clearview
New Orleans, LA 70123

1 Roger O. Cook, Manager
EG&G Idaho
Safeguards and Security
PO Box 1624
Idaho Falls, ID 83415

1 John Jones, Group Manager
EG&G Idaho
Safeguards and Security
PO Box 1624
Idaho Falls, ID 83415

1 Daniel Baker, Security Manager
EG&G Mound
PO Box 3000
Building 99
Miamisburg, OH 45342

1 Shirley C. Olinger, Director
EG&G Rocky Flats
Safety and Health Division
Bldg 116
PO Box 464
Golden, CO 30402-0464

1 Rudy Dorner
Fermi National Accelerator Laboratory
MS 102
Batavia, IL 60150

1 W. O. Clements, Manager
Martin Marietta Energy Systems
Y-12 Safeguards and Security
Bldg 9706-1, MS 8212
Oak Ridge, TN 37831-8213

1 James J. Hallihan, Director
Mason and Hanger-Silas Mason
Company, Inc.
Pantex Plant
Safeguards and Security
PO Box 30020
Amarillo, TX 79177-001

1 B. G. Essary, General Manager
Protection Technologies of Idaho
785 DOE Place
Idaho Falls, ID 83402

1 Raytheon Services, Inc.
Attn: Electronics Department
PO Box 93838
Las Vegas, NV 89193-3838

1 Wackenhut Services, Inc.
800 West Commerce Road
Suite 100
New Orleans, LA 70123

1 W. R. Brooksher, Manager
Westinghouse Hanford Company
Safeguards and Security Division
PO Box 1970, Mail Stop L4-01
Richland, WA 99352

1 E. L. Goldman, Manager
Westinghouse Idaho Nuclear Company
Safeguards and Security
PO Box 4000
Idaho Falls, ID 83403

1 J. M. Miller, Manager
Westinghouse Materials Company of Ohio
Safeguards and Security
PO Box 898704
Cincinnati, OH 45239

1 J. W. Dorrycott, Division Manager
Westinghouse Savannah River Company
Safeguards, Security, & Emergency Preparedness
PO Box 616
Aiken, SC 29802

1 R. E. Gmitter, Manager
Safeguards and Security Programs
Westinghouse Savannah River Company
PO Box 616
Aiken, SC 29802

1 Chief of Security Police
Air Force Systems Command
Andrews Air Force Base
Maryland 20334-5000

1 485th EIG/EICI
Attn: Charlie Winters
Griffiss Air Force Base
New York 13441-6348

1 HEADQUARTERS, USAFE
Attn: Director, Plans and Programs
Unit 3050, Box 135
APO-AE 09094-5000

1 HEADQUARTERS, ESC/AVJ
Attn: MAJ Dave MacKenzie
20 Schilling Circle
Hanscom Air Force Base
Massachusetts 01731-2816

1 HEADQUARTERS, PACAF/SPPA
Attn: Director, Plans and Programs
Hickam Air Force Base
Hawaii 96853

1 HEADQUARTERS, AFSPA/SPSS
Attn: Col David M. Taylor, USAF
Director, Physical Security
8201 H Avenue SE
Kirtland Air Force Base
New Mexico 87117-5664

1 Director of Operations (SPO)
Air Force Agency Security Police
Kirtland Air Force Base
New Mexico 87117-5000

1 Mr. Michael Toscano, Chairman
DoD Physical Security Equipment Advisory Group
OUSD(A)/TS/LS
The Pentagon
Washington, DC 20301-3100

1 U.S. Department of Justice
Federal Bureau of Prisons
Attn: Jim Mahan, Room 300
320 First Street NW
Washington, DC 20534

1 Attn: Bill Witter
Director, Defense Nuclear Agency
(ATTN: NOSA)
6801 Telegraph Road
Alexandria, VA 22310-3398

1 Priscilla A. Dwyer
NMSS Technical Monitor
Division of Safeguards and Transportation, MS4E4
Office of Nuclear Material Safety and Safeguards
United States Nuclear Regulatory Commission
Washington, DC 20555

1	MS 0769	D. S. Miyoshi, 5800
1	MS 0768	R. W. Moya, 5804
1	MS 0768	J. W. Kane, 5806
1	MS 0778	R. F. Davis, 5808
1	MS 0765	D. E. McGovern, 5821
1	MS 0761	F. O. Leutters, 5822
1	MS 0781	D. J. Gangel, 5831
1	MS 0781	R. W. Madsen, 5831
1	MS 0781	D. C. Hanson, 5833
1	MS 0781	R. C. Holt, 5833
1	MS 0781	E. R. Sanders, 5833
1	MS 0780	S. Ortiz, 5838
1	MS 0759	I. G. Waddoups, 5845
1	MS 0782	J. F. Chapek, 5848
1	MS 1131	B. J. Steele, 5849
1	MS 1131	T. P. Malone, 5849
1	MS 1131	L. D. Miller, 5849
1	MS 1131	C. E. Ringler, 5849
20	MS 1131	J. T. Vigil, 5849
1	MS 1131	F. M. Wolfenbarger, 5849
1	MS 0765	J. D. Williams, 5861
1	MS 0611	R. M. Workhoven, 7433
1	MS 9020	S. C. Gray, 8536
1	MS 9018	Central Technical Files, 8523-2
5	MS 0899	Technical Library, 7141
1	MS 0619	Technical Publications, 7151
10	MS 0100	Document Processing for DOE/OSTI, 7613-2

DATE FILMED

4/25/94

END