Handbook of Intrusion Detection Sensors

SPAWAR
Systems Center
Charleston

HANDBOOK OF INTRUSION DETECTION SENSORS

Prepared and published by

SPAWAR Systems Center Charleston
P.O. Box 190022
North Charleston, SC 29419-9022

August 2005

This Project was funded under Interagency Agreement #2003-TK-R-040, from the U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, Systems Support Division.

fitness for a particular purpose. Further, neither the United States Government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed; nor do they represent that its use would not infringe privately owned rights.

Distribution authorized to federal, state, local, and tribal government agencies only for administrative or operational use, August 2005. Other requests for this document shall be referred to the U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness Systems Support Division, 800 K Street, NW, Washington DC, 20001.

THE SAVER PROGRAM

The U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness (SLGCP) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders in performing their duties. The mission of the SAVER Program is to:

- Provide impartial, relevant, and cost-effective evaluation and validation of equipment and software.
- Enable decision makers and responders to better select, procure, use, and maintain equipment and software.
- Evaluate and validate the interoperability of products within a system, as well as systems within systems.
- Provide feedback to the user community through a well-maintained, Web-based database.

As a SAVER Program partner, Space and Naval Warfare Systems Center (SPAWARSYSCEN) Charleston has been tasked by SLGCP to provide expertise and analysis on key subject areas including communications, sensors, perimeter security, weapon detection, and surveillance. In support of this tasking, SPAWARSYSCEN Charleston developed the *Handbook of Intrusion Detection Sensors* in order to provide emergency responders, military and law enforcement security managers, and other security specialists with a reference on current intrusion detection sensor technologies, capabilities, limitations, and integration methods.

The SAVER Program is focused on evaluating processes and procedures for components as well as establishing system-level performance. The

SAVER Program databases, processes, and expertise are available to emergency responders at a national level. This sharing of information will be a life-saving and cost-saving asset to the U.S. Department of Homeland Security, as well as to federal, state, local, and tribal users of emergency response equipment. More information can be found on the SAVER Program Web site, https://saver.fema.gov.

POINTS OF CONTACT

U.S. Department of Homeland Security,
Office of State and Local Government Coordination and Preparedness,
System Support Division
800 K Street NW,
Washington DC, 20001

Dr. Pete Nacci, Director
Dr. William Billotte, William.Billotte@associates.dhs.gov

SPAWAR Systems Center Charleston
Law Enforcement Advanced Technology Engineering
P.O. Box 190022
North Charleston, SC 29419-9022

Mr. Richard Baker, Program Manager
Mr. Eddie Broyles eddie.broyles@navy.mil
Mr. Dan Heater daniel.heater@navy.mil

This page intentionally left blank.

PREFACE

PURPOSE

The *Handbook of Intrusion Detection Sensors* updates the information in and extends the utility of *The Perimeter Security Sensor Technologies Handbook* published in 1997. The *Handbook of Intrusion Detection Sensors* provides first responders, military, and law enforcement security managers, and other security specialists with a reference on current intrusion detection sensor technologies, capabilities, limitations, and integration methods. It explains each technology's operating principles, applications, and covers integration techniques that can be used to enhance security and intrusion detection planning for permanent and temporary sites.

SCOPE

Most of the sensors and devices currently used in the security field are available as Commercial-Off-The-Shelf (COTS) products and have been successfully integrated into a wide range of operating systems.

The data presented in this handbook has been restricted to those elements of a security system that relate to perimeter security and intrusion detection sensor technology. The handbook does not include information on computer or access control equipment, nor is it intended to provide an all-inclusive list of sensor suppliers or equipment models.

A market survey was conducted to ensure a balanced representation of the current state of available technologies. Although new or improved equipment is continually being developed and introduced into the marketplace, the fundamental principles and applications of security sensors have not changed. Most sensors are based on the principle of establishing, monitoring, and detecting changes from a norm. Advanced

sensors apply digital processing technologies to compare electronic frequency-amplitude spectra of events with stored models of intrusion, nuisance, and normal event spectra to determine if a significant event, such as an intrusion, has occurred.

Information included in this handbook on specific sensors and manufacturers is derived in part from information received in response to a request for information placed in the Commerce Business Daily (CBD), and posted on the FedBizOps.gov Internet site on December 5, 2003. Other research was largely conducted on the Internet for available technologies, products, and vendors. Limited direct contact was made with government, civilian, or vendor personnel to further the research process.

No assertion is made that this handbook is comprehensive in its breadth or depth. It is introductory-level information and should not be considered definitive in planning for or implementing a security sensor system. Such efforts should be undertaken only in consultation with organizations experienced in the various phases of planning, constructing, testing, operating, and maintaining integrated perimeter defense and intrusion detection systems.

Vendor information has not been altered or edited. The U.S. Government did not conduct an independent test of any of these sensor systems and, therefore, does not warrant, guarantee, or endorse any of these devices. Section 4 lists the vendors that supplied information for this handbook and provides a matrix of their corresponding products.

Sensors under development, or restricted to military use, are not included in this handbook.

TABLE OF CONTENTS

1

INTRODUCTION

GOAL

The *Handbook of Intrusion Detection Sensors* is a sensor selection reference for use during the design and planning of integrated security systems. It contains a compendium of sensor technologies that can enhance perimeter security and intrusion detection for permanent or portable/deployable exterior, interior, and aquatic security applications. This handbook provides basic information to assist organizations whose primary functions may not encompass designing, evaluating, or building security systems, but who need knowledge of the types of tools available. Such an organization might include local, state, and federal law enforcement agencies; civil and military disaster administrators; disaster control personnel; and disaster/emergency response personnel.

Any organization seeking to build a security system should do so only with the assistance of personnel or organizations that specialize in designing and building such systems. The establishment of an integrated security system will involve not only design, construction, and testing, but also the long-term issues of monitoring, training, and maintenance.

ORGANIZATION OF HANDBOOK

The handbook is organized into four sections. Section 1 is this introduction. Section 2 is an overview of the factors to be considered prior to selecting a suite of security sensors. Section 3 consists of a description of each of the twenty-one intrusion detection sensor technologies discussed in the handbook, including operating principles,

sensor types and configurations, applications, and reliability considerations. Section 4 contains a listing of vendors who responded to the Federal Business Opportunities (FedBizOps) notice and a cross-reference matrix of sensors and manufacturers. The handbook is best used (after a general review), by referring to the applications icons and graphics presented in section 2 to determine which technologies might suit the user's needs, and then reviewing the material in section 3 which relates to those technologies.

CHANGES FROM THE 1997 VERSION

The applications paragraph in each technology review section contains four subparagraphs: interior, exterior, portable and aquatic. These clarify and emphasize the availability of each sensor type in those application categories. The subparagraph on portability should make this handbook useful for those governmental and civilian organizations that must respond to emergencies and other types of incidents that require an area to be isolated and protected quickly. The subparagraph on aquatic applications responds to emerging requirements to monitor activity on and under water in a host of situations.

To improve the users' ability to determine more quickly which sensor technologies may have applications to their particular needs, this handbook uses a system of icons to highlight the appropriate applications subparagraphs. The icons are the first letter of the four subparagraph names: "**I**" for **Interior,** "**E**" for **Exterior,** "**P**" for **Portable,** and "**A**" for **Aquatic.** Appropriate icons appear at the top of the first page of each sensor review section in the hard copy of the handbook. In the CD and web versions of this handbook, the icons also appear opposite each sensor type in the contents. Clicking on an icon will take the reader directly to the appropriate sensor review section and will open a window listing all the detection sensors that carry that icon. A section 508 compliant site is available for those with disabilities.

Some sensor technologies have been eliminated and others added in this new edition. The reasons some sections have been deleted include obsolescence (mechanical switches and magnetic switches), difficulty finding actual products (passive and active ultrasonic sensors, acoustic turbulence sensors), using different names for similar products (photoelectric versus active infrared), and changes in the market (capacitance sensors and wall vibration sensors). Also, associative sections such as “interior active infrared” and “exterior active infrared” were collapsed into a single section on “active infrared.” The former sections on “fiber optic walls,” “in-ground fiber optics,” and “fiber optic fence” were combined into one section on “fiber optics.”

Technology sections were added for newly identified commercially available products including sonar, laser radar (also known as LIDAR), and magnetic sensors.

This page intentionally left blank.

2

SENSOR EMPLOYMENT CONSIDERATIONS

OPERATIONAL REQUIREMENTS

Security measures should be tailored to the needs and requirements of the resource or area to be protected. The starting point for defining needs and requirements is to perform a vulnerability assessment. The type of facility or material to be protected, the nature of the environment, the client's previous security experience, and assumptions about potential threats will influence the approach used to develop a security solution from the vulnerability assessment. These factors form the basis for the user's initial judgment; however, these perceptions are rarely sufficient to develop an effective security posture. Several other factors should also be considered in the vulnerability assessment: the nature and tempo of activity in and around the site, the physical configuration of the facility, the surrounding natural and human environment, fluctuations, and variations in the weather, permanence, training, and support. An experienced security systems development professional is an essential part of any security systems planning or vulnerability assessment team.

With modern electronics, the flexibility to integrate a variety of equipment and capabilities greatly enhances the potential to design an intrusion detection system to meet specific needs. The main elements of an

intrusion detection system include: a) the intrusion detection sensors, b) the alarm processor, c) the intrusion/alarm monitoring station, and d) the communications structure that connects these elements and connects the system to the reaction elements. In many cases integrated security systems should incorporate surveillance systems or other means to allow security personnel to determine what caused (to assess) an alarm, and to dispatch response personnel to evaluate the alarm or deal with any threat. A common choice for an assessment system is a closed circuit television camera system. In the majority of applications, intrusion detection sensors are used in conjunction with a set of physical barriers and access control systems for personnel and vehicles. However, all systems also include people and procedures, both of which are of equal and possibly greater importance than the individual technology aspects of the system. In order to use an installed security system effectively, trained personnel are required to operate, monitor, and maintain the system, while an equally professional team is needed to assess and respond to alarms. Technology should support and be supported by effective tactics and procedures to achieve an optimal security posture.

DEFINITIONS OF PERFORMANCE CHARACTERISTICS

There are at least four performance characteristics that are commonly used in evaluating a particular sensor system: probability of detection (Pd), false alarm rate (FAR), nuisance alarm rate (NAR), and vulnerability to defeat (i.e., typical measures used to defeat or circumvent the sensor).

A major goal of the security planner is to design an integrated intrusion detection system (IDS) that exhibits a low FAR, a low NAR, a high Pd and is not susceptible to defeat. Each of these characteristics should be specified as a desired level of system performance commensurate with the criticality or value of the protected resource. It is important to understand that these characteristics interact. Often, actions to increase the Pd will cause an undesirable increase in the NAR or FAR. Conversely, actions to decrease the NAR or FAR will often cause an undesirable decrease in the

Pd. These characteristics must be balanced to ensure an overall acceptable level of performance.

The *probability of detection* is a measure of sensor performance in detecting an intrusion within a zone covered by the sensor. Probability of detection is a function of the characteristics of the sensor, but also takes into account assumptions about the environment, the method of installation and adjustment, and the assumed behavior of an intruder. These assumptions should include expectations about the level of knowledge of a likely intruder.

A *nuisance alarm* is a legitimate detection caused by something other than an intruder. A nuisance alarm may be caused by an animal, a bird, wind-blown vegetation, an electrical disturbance, or some other cause. The cause of a nuisance alarm may or may not be discernible; if the cause is not immediately discernible, monitoring personnel may count it as a "false" alarm. The NAR is expressed as a number of events within a specific period of time. Since all sensor systems interact with their environment, they are subject to some level of nuisance alarming, no matter how sophisticated the alarm processing. So that security personnel do not have to respond to every alarm, an alarm assessment capability needs to be part of the design of any integrated security system. Advances in processing technology have significantly reduced the NAR of many sensor technologies compared to systems available just a decade ago. Digital processing now allows comparison of the sensor's signal to the signal spectra of known or expected disturbance sources, whereas earlier processors depended on an analog system of counts per time, duration of signal amplitude above a threshold, or some other method.

A false alarm rate indicates the expected rate of occurrence of alarms that are caused by anomalies within the sensor-processor-communications system that are not due to any sort of legitimate detection. It is expressed as a number of events within a specific period of time. False alarm rates for currently available systems should be very low. One false alarm per

week per detection zone for an entire security system is attainable with current technology.

The *vulnerability to defeat* is another measure of the effectiveness of sensors. Since there is presently no single sensor that can reliably detect all intruders and still have an acceptably low NAR, the potential for "defeat" can be reduced by designing sensor coverage using multiple units of the same sensor or including more than one type of sensor to provide overlapping coverage of the area and mutual protection for each sensor.

FACTORS AFFECTING THE PROBABILITY OF DETECTION

A detection system's probability of detection depends mostly on six factors:

- Assumptions about the potential target (size, behavior, sophistication, etc.)
- Sensors selected
- The installation
- System sensitivity settings
- Local environmental conditions
- Maintenance

The probability of detection cited for a sensor system will vary with changes in the above factors, both initially and over time. Rather than depending upon a specific number, it is sometimes better to specify in detail the conditions under which detection is expected to occur. For instance, a system may be expected to detect any person heavier than 120 pounds crawling, rolling, walking, or running perpendicular to the sensor's detection axis at a speed between 0.5 feet per second and 5 feet per second anywhere in the detection zone under any weather condition with winds less than 40 knots with greater than 90% confidence. All the parameters cited in such a requirement are testable.

It is impossible to overemphasize the importance of the quality of installation, system and infrastructure maintenance, personnel training,

and assessment capabilities to sustaining a high probability of detection. Many fence-mounted sensors depend on very well engineered fences with stable posts and taut fence fabrics. Buried sensors often require specific soil parameters, separation from nuisance sources, and drainage requirements. Failure to maintain such systems may lead to unacceptable nuisance alarm rates, for example, from loose fence fabrics or posts that cannot sustain the tensions required to allow the sensors to work as expected.

SENSOR CATEGORIES

The most basic categories of security sensors are “interior” or “exterior.” The first two of the set of graphics following this section show “family trees” of the sensors most applicable to these two environments. Those technologies that can be used in both environments are shown on both graphics. Each of the two basic categories contains a number of subsets, such as fence, door, window, hallway, and room that further catalog sensors by installation location.

Interior intrusion detection sensors are used to detect intrusion into a building, covered structure, or a specified area inside a building or covered structure. Many of these sensors are designed for indoor use only and should not be exposed to weather.

Interior sensors perform one of three functions: (1) detection of an intruder approaching or penetrating a secured boundary such as a door, wall, roof, floor, vent, or window; (2) detection of an intruder moving within a secured area such as a room or hallway; and (3) detection of an intruder moving, lifting, or touching a particular object.

Interior sensors are susceptible to false and nuisance alarms, but not to the same extent as their exterior counterparts. This is a function of the more controlled environments in which interior sensors are employed.

Exterior intrusion detection sensors detect intruders crossing a particular outdoor boundary or entering a protected zone. Many types of sensors are most effective in clear zones in open fields, around buildings, or along fence lines. Exterior sensors must be resilient enough to withstand outdoor weather conditions such as extreme heat, cold, dust, rain, sleet, snow, and winds, and reliable enough to detect an intrusion during such harsh environmental conditions.

Exterior intrusion sensors have lower probabilities of detecting intruders and higher nuisance alarm rates than their interior counterparts. This is due largely to many, often uncontrollable environmental factors, such as weather, standing water, blowing debris, random animal and human activity, electronic interference, and other sources. These factors often require lowering the sensitivity settings and adding other types of sensors to ensure an acceptable probability of detection for the entire security system.

A special category of exterior sensors consists of those systems designed specifically for use on or underwater and are labeled aquatic in this handbook. These are designed to detect or deter divers, swimmers, and watercraft of all sorts that might be of interest in situations such as ports, harbors, off-shore rigs, loading/unloading facilities, and individual vessels.

Many sensors of each category of interior, exterior, and aquatic are designed to be portable and able to be set up rapidly. These sensor systems may be of particular interest to incident response teams, who must quickly isolate an area and control ingress and egress. These systems incorporate the maximum advantages offered by recent developments in digital, miniaturization, power, communications, and computing technologies.

ENVIRONMENTAL CONSIDERATIONS

Most security zones have unique environmental characteristics that must be considered when designing the system, selecting the sensors, and performing the installation. Failure to consider all the factors can result in unacceptably high nuisance alarm rates, dead zones in the system, or a system that, for any number of reasons, fails to perform as expected.

Each potential intrusion zone will have special environmental factors to consider. Exterior zones are likely to be affected by the prevailing climate, seasonal extremes, fluctuations in weather conditions, and random animal activity. Man-made environmental factors including activity patterns, electrical fields, radio transmissions, and movements of vehicles, trucks, trains, or aircraft also influence the design and performance of integrated security systems.

There are a number of other considerations that must be assessed when placing sensors to monitor the perimeter of an area or building. A well-defined, unobstructed surveillance or isolation zone is a fundamental requirement. Such a zone results in fewer nuisance alarms caused by innocent people, large animals, blowing debris, or other factors. If fences are used to delineate the clear zone or isolation zone, they should be carefully placed and must be correctly constructed. Consideration should also be given to dividing the perimeter into segments in order to localize an attempted intrusion rapidly and direct the response force to that locale.

Interior zone sensors can be adversely affected by a combination of stimuli such as machinery noise and vibrations; air movement caused by windows, fans, and air conditioning/heating units; changes in temperature; and flickering lights. Many of these stimuli will be discussed in the individual sensor technology sections in section 3.

ALARM MONITORING SYSTEMS

In addition to the off-the-shelf intrusion technologies that are discussed in this handbook, a variety of alarm monitoring systems are available. State-of-the-art systems provide visual and audible indications of an alarm. The alarm data is displayed as text on a monitor or as symbols on a map. Most systems offer multiple levels (scales) of maps, which can be helpful in guiding security personnel to the location of the attempted intrusion. The urgency of the alarm can vary according to its nature or the location of the possible intrusion (e.g., high priority versus low priority areas). In most security systems, several of these capabilities are combined to provide the Security Operations Center personnel with a comprehensive description of the alarm situation. Although each system is unique in the number and scope of the options available, all systems perform the basic function of annunciating alarms and displaying the intrusion locations in some format.

The front-end (control function) of most of these systems is configured with a Pentium-type computer utilizing Windows, UNIX, or OS/2 as the operating system. Several operate with proprietary software, written by the manufacturer of the security system. Laptop and hand-held computers may also be incorporated as part of the monitoring system to meet missions requiring portability, integration, and distribution of information to responding personnel. Miniaturized, portable computers are also used as the primary control hardware for portable or deployable suites of security sensors and convey advantages similar to fixed systems.

ALARM ASSESSMENT

The assessment element of a security mission involves the evaluation of an alarm source and the analysis of audible and visual alarm data to determine if an intrusion or otherwise unallowable event has occurred within or approaching the secured area. The security operator performs an assessment by using closed circuit television, thermal imagery, and sometimes response force observation. Generally, the alarmed area is

automatically shown on monitors in the operations center and systematically prerecorded for future detailed analysis. The security operator dispatches the response force if required. Several control systems can automatically train video or infrared cameras toward a zone in alarm to provide the security personnel with a real-time view of the situation, to track the progress of an intrusion, and to hand off to adjacent monitoring and surveillance components as an intruder moves to other zones.

The ability to incorporate hand-held and laptop computers into many security command-and-control systems using wireless technologies allows personnel responding to an alarm to have the same information as the central monitoring personnel. These capabilities significantly enhance the safety of responding personnel and allow for more efficient and appropriate responses to actual or suspected intrusions. Such systems also allow central control station personnel to track patrol personnel during the course of their routine circuits.

SENSOR INTEGRATION

Current technology has made the integration of several types of sensors into a cohesive security system more feasible. Several companies have annunciator and command-and-control equipment designed to accept input and display information from a wide variety of sensor systems.

Since every type of sensor has vulnerabilities and can generate nuisance alarms, security systems should be supplemented with additional detection technologies to protect against the weaknesses of any one technology, to enhance the system's overall probability of detection, and to provide means for security personnel to assess alarms. Many sensor systems have the capability to notify security personnel of attempts to tamper with, cut, or bypass the sensors or the connectivity between the sensors and the processing or command-and-control stations.

Different sensor circuits can be integrated to reduce nuisance alarm rates. Sensor alarm and tamper circuits can be joined together by installing an *AND* logic circuit, which requires an alarm from more than one sensor prior to sending an alarm indication. Usage of the *AND* logic circuit can reduce nuisance alarm rates, but it may decrease the overall system's probability of detection.

COMMUNICATIONS

Communications between the command-and-control unit and the field elements (sensors, processors) employ a variety of standard communications protocols. RS-485, RS-232, Frequency Shift Keying (FSK), and Dual Tone Multi Frequency (DTMF) dial are the most common. Occasionally a manufacturer will use a proprietary communications protocol that can limit the possibility for future upgrades and system expansions. In order to reduce the tasks handled by the computer, some systems have a preprocessing unit located between the computer and the field sensing elements. This preprocessor acts as the communications coordinator to "talk" to the field elements and relieve the computer of these responsibilities.

POWER SUPPLY

Regardless of the quality of design and installation, all intrusion detection systems are vulnerable to electric power losses. Some systems may not be able to reset automatically and would require operator intervention to restore. Potential intruders may be aware of these vulnerabilities and may seek to cut or interrupt power if they cannot circumvent the system by other means. It is critical that all elements of the system have backup power systems incorporated into the design and operation to guarantee the uninterrupted integrity of the sensor field, alarm reporting, situation assessment, and the response force's reaction.

Consultations during the design phase are the best time to define power requirements, line conditioning requirements, and which elements should

have battery or other backup power sources. Backup power for fixed systems may be from uninterruptible power supplies (UPS), generators, or automatic bus power transfer switches. Portable systems may run on a central power system, batteries, or solar power.

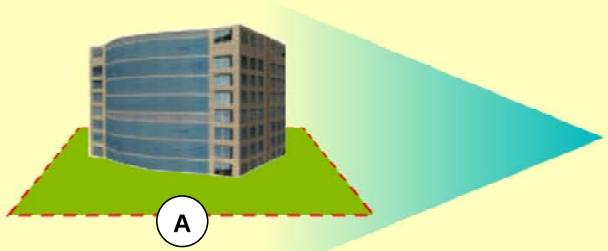
COSTS

The costs of an intrusion detection system are easy to underestimate. Sensor manufacturers may quote a cost per meter, cost per protected volume, or some other measure. This figure may represent only the hardware cost, and may not include the costs of engineering design, installation, construction, training or maintenance. Often the costs associated with infrastructure or the assessment and alarm reporting systems outweigh the costs of the sensor components. Some techniques to minimize costs include being careful when defining the threats, buying multiple types of systems, and selecting from among several technologies providing similar categories of protection. Since infrastructure can also be a significant cost driver, using suitable existing infrastructure, such as power cabling, fencing, conduit, or ducting, can help mitigate some costs.

SUPPLEMENTAL GRAPHICS

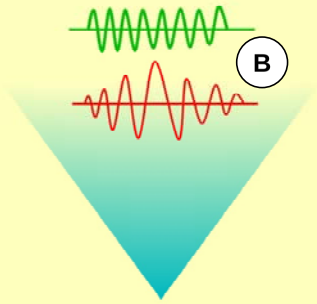
The following graphics include perimeter product categories, processes, and situational examples. They are intended for use as visual aids to provide the reader with an understanding of concepts discussed in the text.

Typical Perimeter Security Intrusion Detection Process



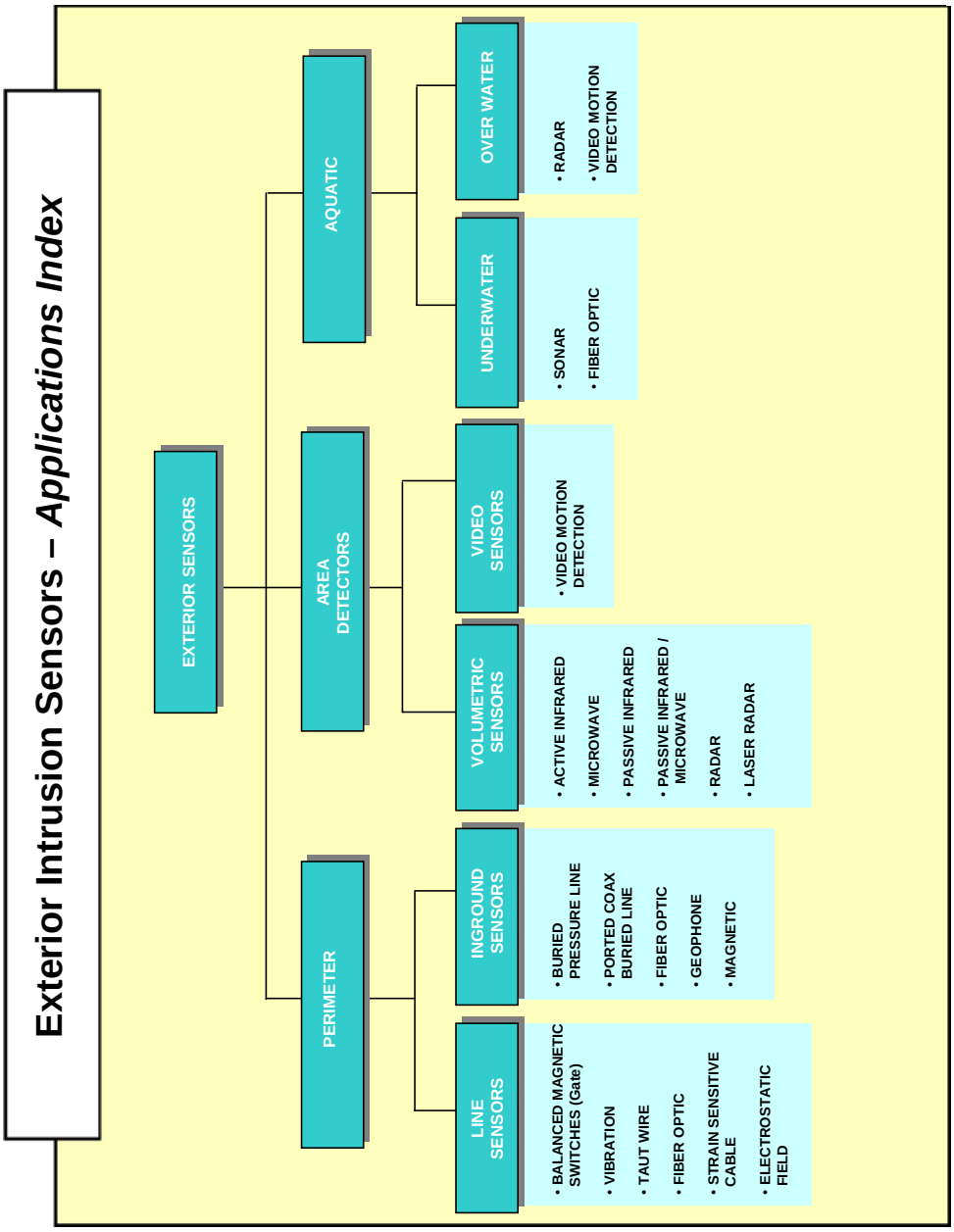
The intrusion sensor detects an intruder approaching or entering the controlled perimeter.

The sensor processor analyzes the signal to differentiate between a nuisance event and an intrusion.

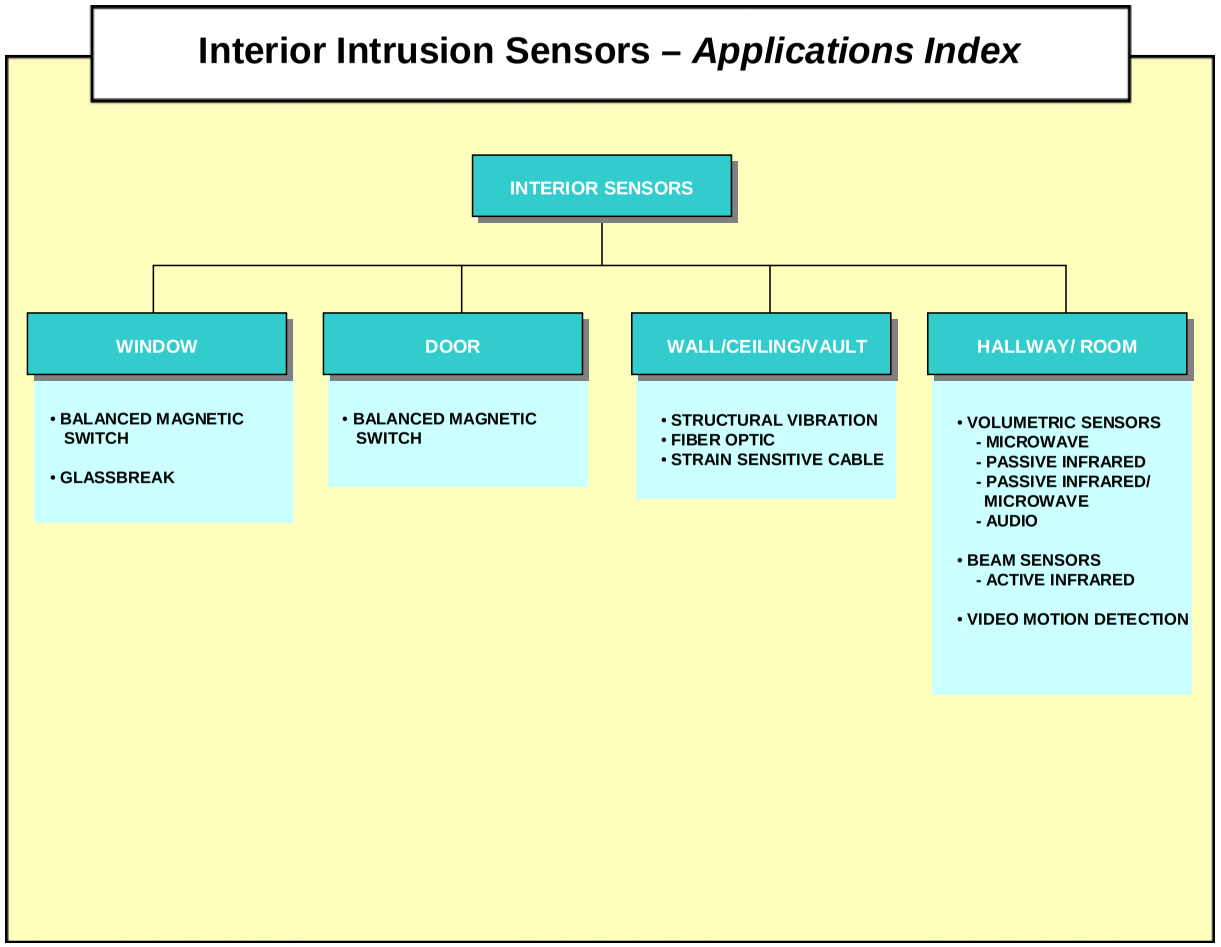


The system generates an alarm or alerts the command post. Security personnel assess the cause and location of the alarm.

The command post dispatches the response force for further assessment or interdiction.


Exterior Intrusion Sensors – Applications Index
EXTERIOR SENSORS
PERIMETER
LINE SENSORS
• BALANCED MAGNETIC SWITCHES (Gate)
• VIBRATION
• TAUT WIRE
• FIBER OPTIC
• STRAIN SENSITIVE CABLE
• ELECTROSTATIC FIELD
INGROUND SENSORS
• BURIED PRESSURE LINE
• PORTED COAX BURIED LINE
• FIBER OPTIC
• GEOPHONE
• MAGNETIC
AREA DETECTORS
VOLUMETRIC SENSORS
• ACTIVE INFRARED
• MICROWAVE
• PASSIVE INFRARED
• PASSIVE INFRARED / MICROWAVE
• RADAR
• LASER RADAR
VIDEO SENSORS
• VIDEO MOTION DETECTION
AQUATIC
UNDERWATER
• SONAR
• FIBER OPTIC
OVER WATER
• RADAR
• VIDEO MOTION DETECTION

Interior Intrusion Sensors – *Applications Index*



Suggested Sensors for Major Exterior Application Categories

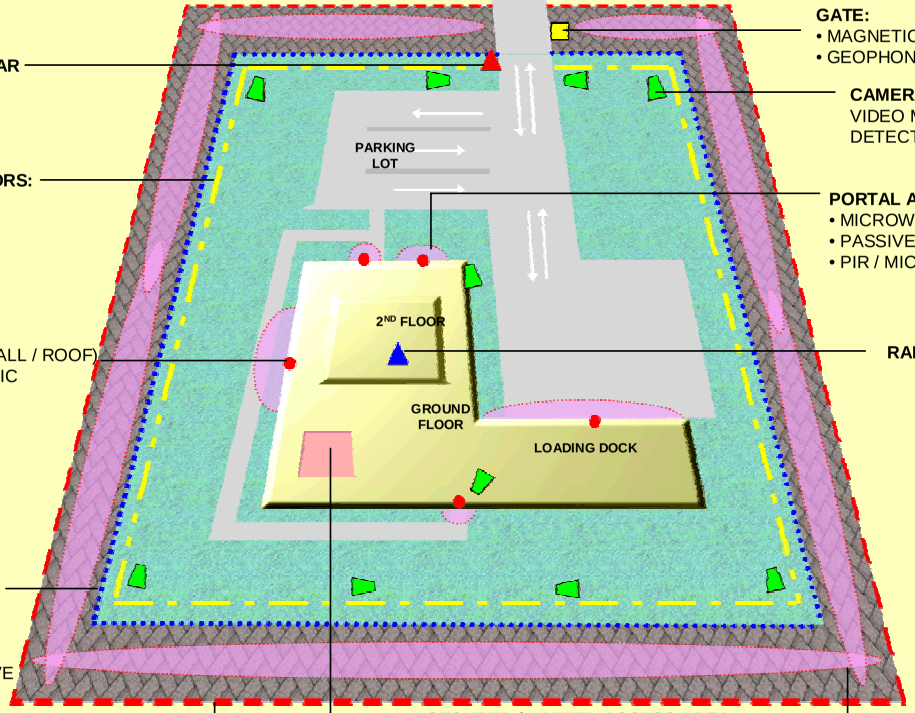
FENCE	BUILDING EXTERIORS
Fence Vibration Electrostatic Field Strain Sensitive Cable Fiber Optic Taut Wire	Microwave Passive Infrared Active Infrared Dual Technology (PIR/Microwave) Electrostatic Field Taut Wire Video Motion Detection Radar Laser Radar (LIDAR)

PERIMETER SENSORS	
BURIED	ABOVE GROUND
Ported Coax Line Buried Pressure Geophone Magnetic	Microwave Passive Infrared Active Infrared Video Motion Detection Radar Laser Radar (LIDAR)

GAPS/ACCESS POINTS	OPEN AREA	WATERSIDE
Balanced Magnetic Switch Microwave Passive Infrared Active Infrared Video Motion Detection	Geophone Magnetic Radar Laser Radar (LIDAR) Video Motion Detection	Fiber Optic Sonar Radar Video Motion Detection

Exterior Sensor Applications Model

This illustration is a schematic showing a hypothetical secured facility employing secured layers of different detection sensors operating together as an integrated security system to enhance the probability of detecting an intrusion.



GATE:
- MAGNETIC
- GEOPHONE

LASER RADAR

CAMERA:
VIDEO MOTION DETECTION

INGROUND SENSORS:
- PRESSURE
- GEOPHONE
- FIBER OPTIC
- PORTED COAX

PORTAL APPROACH AREA:
- MICROWAVE
- PASSIVE INFRARED
- PIR / MICROWAVE

ENTRY POINTS:
(DOOR / WINDOW / WALL / ROOF)
- BALANCED MAGNETIC SWITCHES
- GLASSBREAK
- FIBER OPTIC

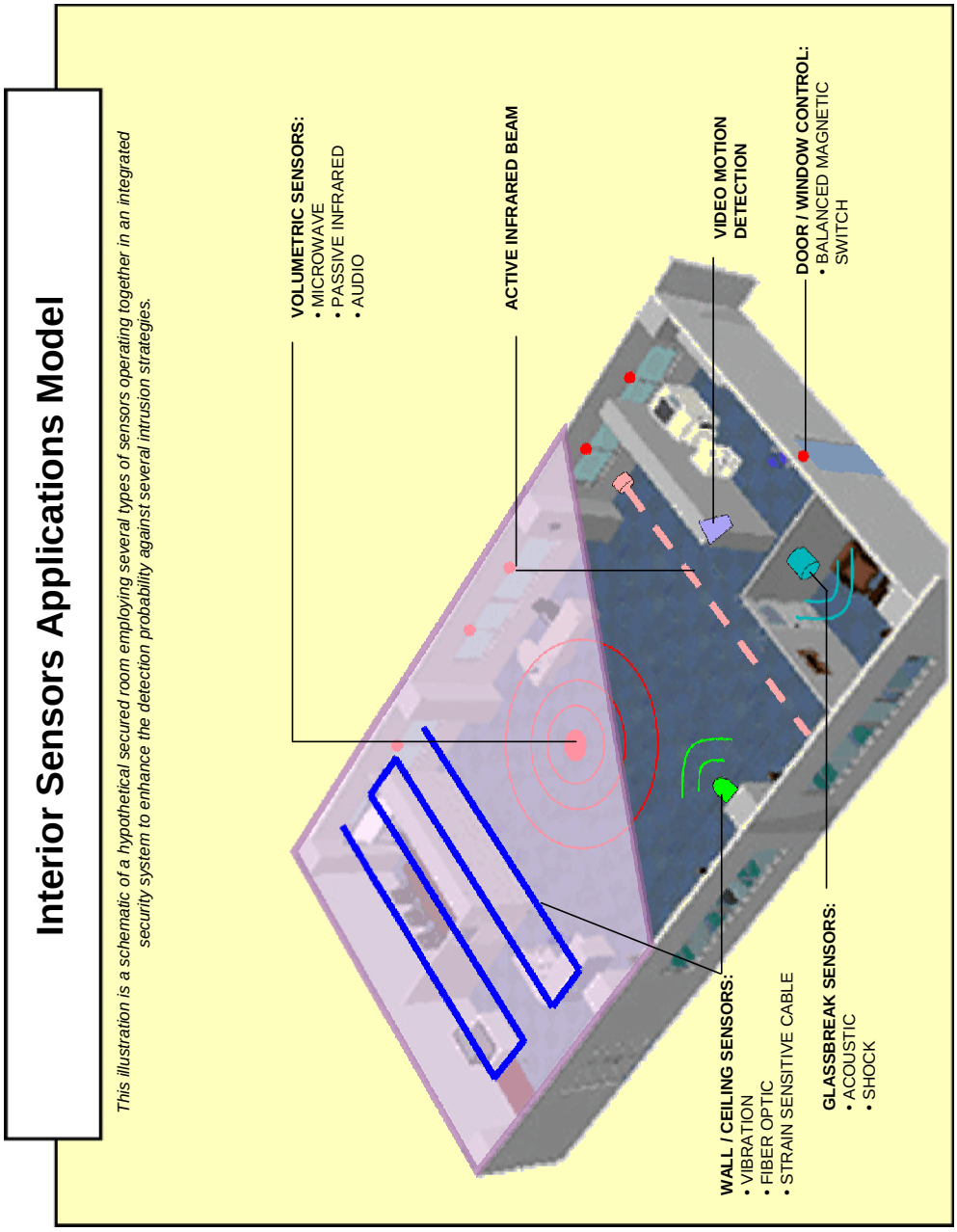
RADAR

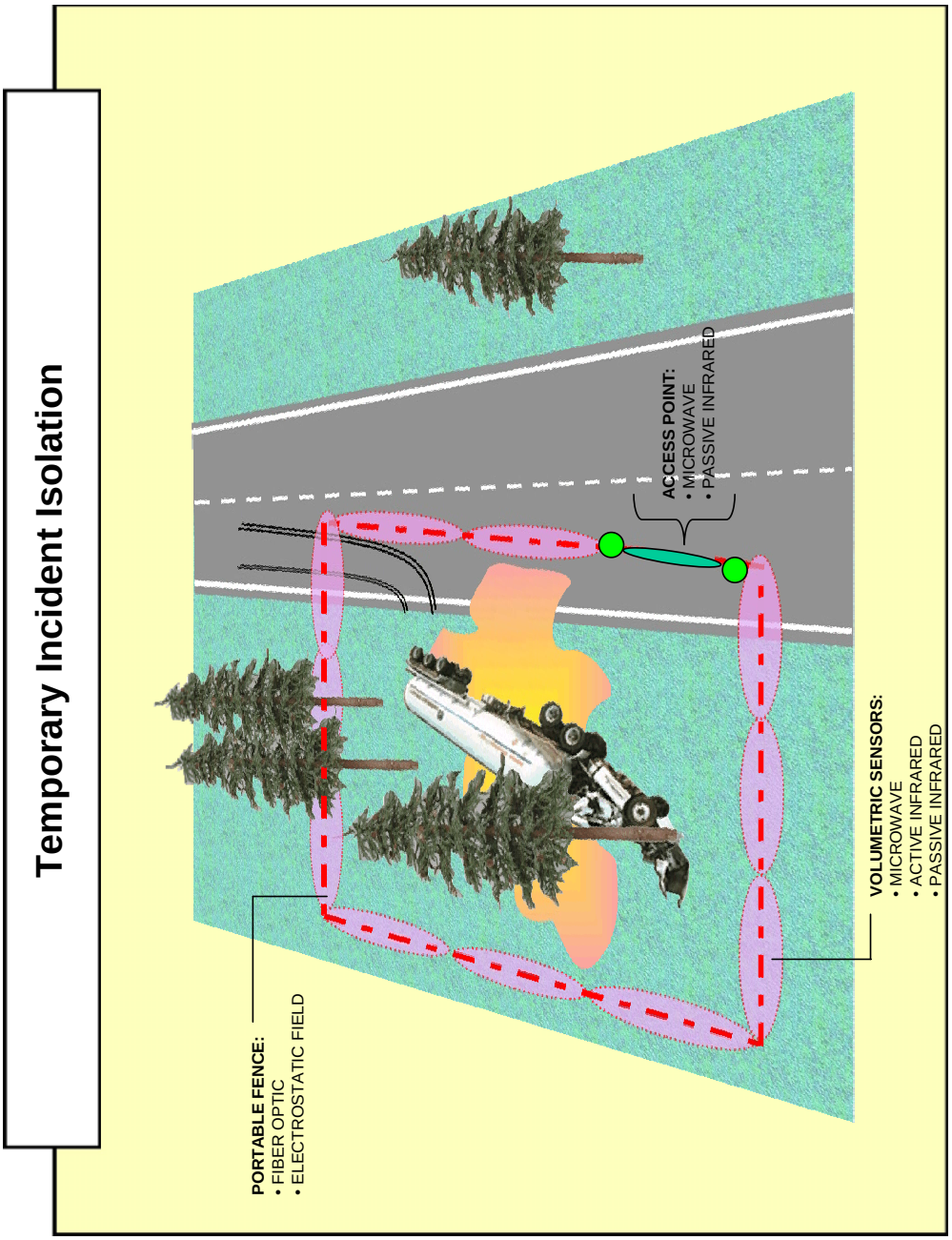
FENCE BARRIER:
- VIBRATION
- TAUT WIRE
- FIBER OPTIC
- STRAIN SENSITIVE
- ELECTROSTATIC FIELD

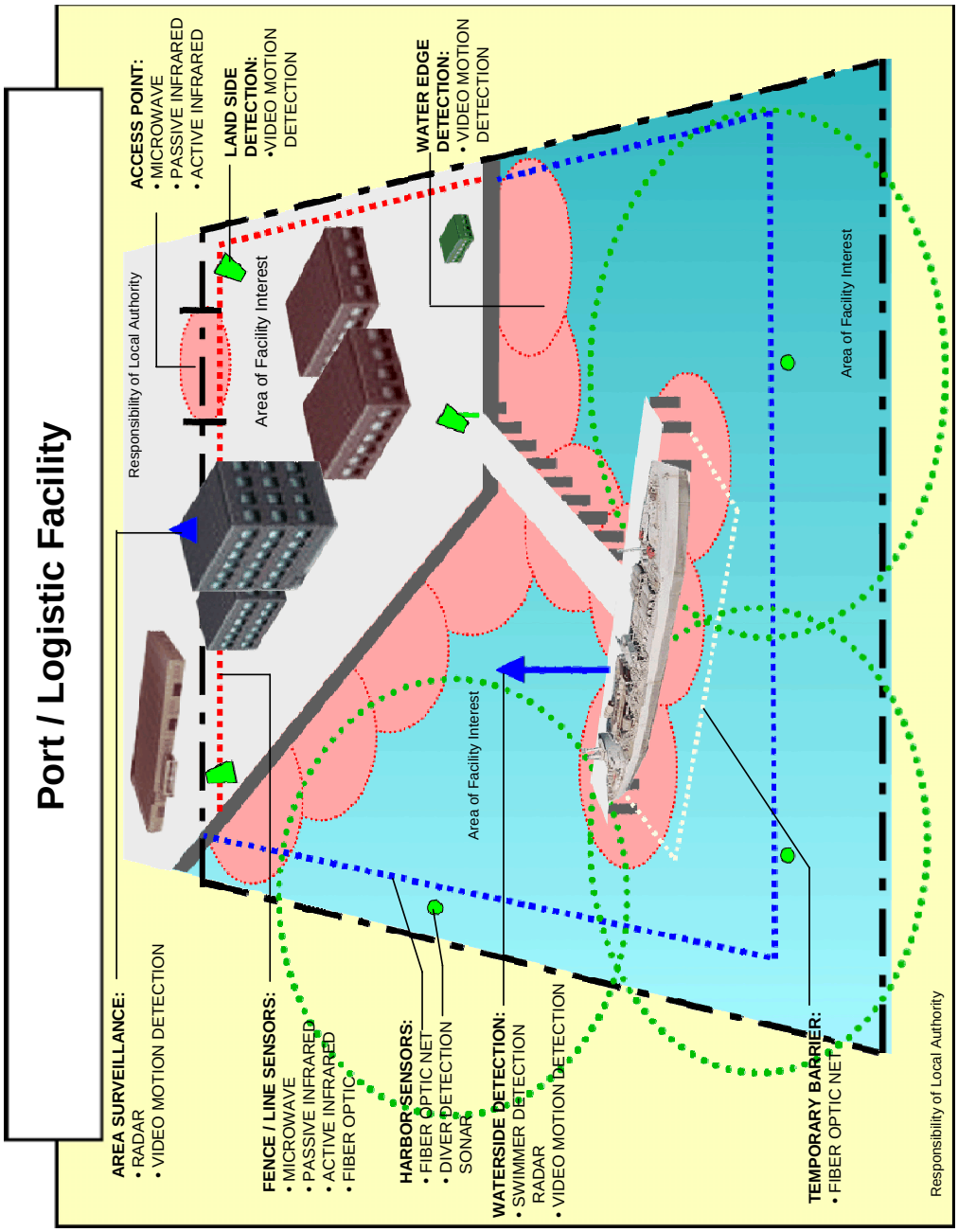
CONTROLLED PERIMETER

SECURED / LIMITED ACCESS AREA:
- AUDIO
- PASSIVE INFRARED
- PIR / MW
- MICROWAVE
- STRUCTURAL VIBRATION

CLEAR ZONE:
- ACTIVE INFRARED
- MICROWAVE


Interior Sensors Applications Model
This illustration is a schematic of a hypothetical secured room employing several types of sensors operating together in an integrated security system to enhance the detection probability against several intrusion strategies.
VOLUMETRIC SENSORS:
• MICROWAVE
• PASSIVE INFRARED
• AUDIO
ACTIVE INFRARED BEAM
VIDEO MOTION DETECTION
DOOR / WINDOW CONTROL:
• BALANCED MAGNETIC SWITCH
WALL / CEILING SENSORS:
• VIBRATION
• FIBER OPTIC
• STRAIN SENSITIVE CABLE
GLASSBREAK SENSORS:
• ACOUSTIC
• SHOCK


Temporary Incident Isolation
PORTABLE FENCE:
• FIBER OPTIC
• ELECTROSTATIC FIELD
ACCESS POINT:
• MICROWAVE
• PASSIVE INFRARED
VOLUMETRIC SENSORS:
• MICROWAVE
• ACTIVE INFRARED
• PASSIVE INFRARED


Port / Logistic Facility
AREA SURVEILLANCE:
• RADAR
• VIDEO MOTION DETECTION
FENCE / LINE SENSORS:
• MICROWAVE
• PASSIVE INFRARED
• ACTIVE INFRARED
• FIBER OPTIC
HARBOR SENSORS:
• FIBER OPTIC NET
• DIVER DETECTION SONAR
WATERSIDE DETECTION:
• SWIMMER DETECTION RADAR
• VIDEO MOTION DETECTION
TEMPORARY BARRIER:
• FIBER OPTIC NET
ACCESS POINT:
• MICROWAVE
• PASSIVE INFRARED
• ACTIVE INFRARED
LAND SIDE DETECTION:
•VIDEO MOTION DETECTION
WATER EDGE DETECTION:
• VIDEO MOTION DETECTION
Responsibility of Local Authority
Area of Facility Interest
Area of Facility Interest
Area of Facility Interest
Responsibility of Local Authority

This page intentionally left blank.

3

TECHNOLOGY REVIEWS

This section presents information on twenty-one perimeter security and intrusion detection sensor technologies. The reviews are arranged according to use: interior point security systems and wall systems, controlled area coverage systems, exterior perimeter systems (including a variety of "fence" systems), and buried "cordon violation" systems. The last several categories, video motion detection, radar, laser radar, and sonar represent newer capabilities.

Icons indicating applications for each technology are listed beside the review title. The key is as follows:

I	INTERIOR USE
E	EXTERIOR USE
P	PORTABLE
A	USE IN AQUATIC ENVIRONMENTS

There are drawings at the end of some technology reviews to illustrate selected concepts. Although there are some minor differences in sub-paragraphing in a few of the technologies, the overall framework, headings, and content are consistent.

The basic format is as follows:

1. Introduction

2. Operating Principles

3. Sensor Types or Configurations
- **a. Type One**
- **b. Type Two**

4. Applications
- **a. Interior**
- **b. Exterior**
- **c. Portable**
- **d. Aquatic**

5. Reliability Considerations
- **a. Conditions that Reduce Detection Probability**
- **b. Causes of Nuisance Alarms**
- **c. Vulnerabilities**

APPLICATION MATRIX

Perimeter Technology	Page no.	I Interior	E Exterior	A Aquatic	P Portable
Balanced Magnetic Switch	29	X	X		X
Glassbreak	33	X			X
Microwave Sensors	39	X	X		X
Structural Vibration	47	X	X		
Audio Sensors	51	X			X
Passive Infrared	55	X	X		X
Active Infrared	63	X	X		X
Dual Technology (PIR/MW)	69	X	X		X
Fence Vibration	73		X		X
Electrostatic Field	77		X		X
Strain Sensitive Cable	83	X	X		X
Fiber Optics	89	X	X	X	X
Taut Wire	97		X		X
Ported Coax Line	103		X		X
Balanced Buried Pressure	109		X		
Geophone	113		X		X
Magnetic Sensors	117		X		X
Video Motion Detection	123	X	X		X
Radar	127	X	X	X	X
Sonar	133			X	X
Laser Radar (LIDAR)	137	X	X		X

This page intentionally left blank.

BALANCED MAGNETIC SWITCH

1. Introduction: A balanced magnetic switch consists of a switch assembly with two or three internal magnets that are usually mounted on the inside of the fixed frame of a door, window, or gate and a balancing (or external) magnet mounted on the moveable portion.

2. Operating Principle: When the gate, door, or window is closed, the switch is balanced in the secure position within the magnetic field formed by the interaction of all the magnets. When a movement of the external magnet disturbs the magnetic field, the switch moves to the alarm position. An intruder trying to position another magnet or ferromagnetic material near the switch will also change the magnetic field and cause the switch to move to the alarm position.

3. Applications:

a. Interior: Balanced magnetic switches provide a high level of security for windows and doors and are one of the most prevalent security components in the security market. They are available in hardened, specially sealed casings designed to prevent the switch from electrically causing an explosion in a flammable or otherwise hazardous area. The balanced magnetic switch should be mounted on the fixed portion of the opening frame, and the balancing magnet on the moveable part. The switch should be adjusted to initiate an alarm when the moveable portion is opened between one half and one inch. For enhanced security, a balanced magnetic switch should be used in conjunction with an independently operating motion detector located inside the protected area.

b. Exterior: Balanced magnetic switches designed for uses in outdoor situations can be installed at gates, turnstiles, and wickets (pedestrian entrapment corridors) to detect intrusion or to show the position of the moveable portion of the device. Installation and operation are the same as for interior uses. They are also available in “wide gap” models for structures where the tolerance of the door or gate closing is too wide for reliable operation of a standard model

c. Portable: Small, wireless, battery-powered balanced magnetic switches are available on the open market for uses requiring portability and ease of setup. These are often components of briefcase-sized portable security systems that may be set up in hotel rooms or other venues.

d. Aquatic: Balanced magnetic switches are not designed for use in underwater applications. Balanced magnetic switches designed for use in humid environments are available.

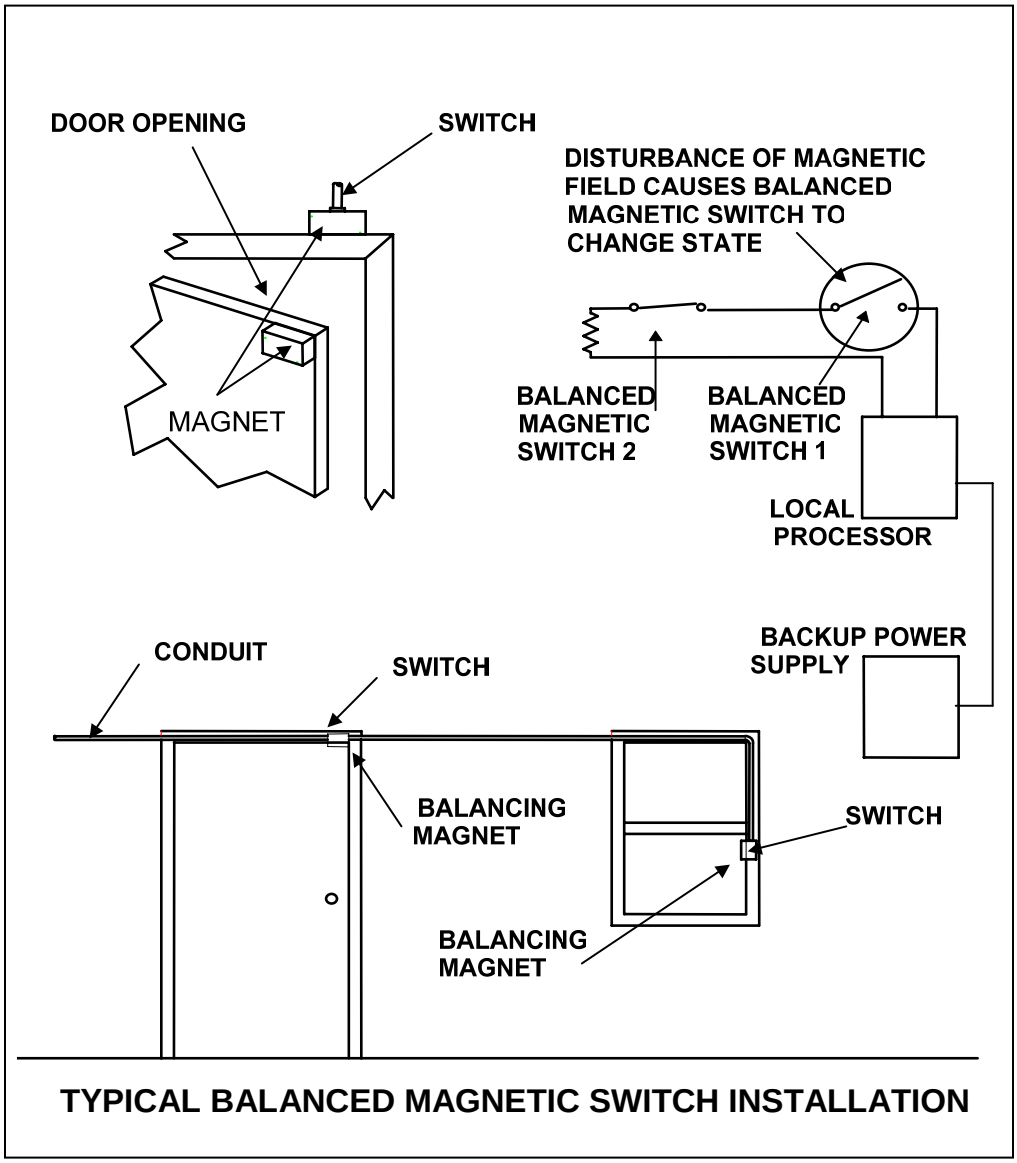
4. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Loosely fitted doors, windows, or gates can generate repetitive nuisance alarms that lull monitoring personnel into ignoring alarms. Switches should be installed only on doors, windows, or gates that are designed to minimize movement when locked or secured.

b. Causes of Nuisance Alarms: Excessive movement of loosely fitting gates, doors, windows, or locks is the primary cause of nuisance alarms. Wind, storms, extreme weather conditions, or seasonal fluctuations in the internal (heating and air conditioning) or external environments can cause loosely fitted or improperly mounted doors and windows to move enough to generate nuisance alarms.

c. Vulnerabilities: Since balanced magnetic switches use two or three independent magnets in the switch housing, it is difficult for an intruder to use an external magnet to avoid moving the internal switch and generating an alarm. This is a distinct advantage over regular magnetic switches that can be defeated by using an external magnet to stabilize the switch while the gate, door, or window is opened. The design of the balanced magnetic switch eliminates this vulnerability.

BALANCED MAGNETIC SWITCH



TYPICAL BALANCED MAGNETIC SWITCH INSTALLATION

This page intentionally left blank.

GLASSBREAK

I P

1. Introduction: Glassbreak sensors monitor glass that is likely to be broken during an intrusion. Each sensor is housed in a single unit and is mounted either on the glass itself, or on a wall or ceiling facing the main glass surface. Coverage typically does not exceed 100 square feet of glass surface. Wireless glassbreak sensors are available.

2. Operating Principle: Glassbreak sensors use a microphone to listen for frequencies associated with breaking glass. A processor filters out unwanted frequencies and only allows certain frequencies to be analyzed. The processor compares the signals received to the frequency signatures associated with breaking glass. If the received signal matches the frequency signature, then an alarm is generated. There are three basic types of glassbreak sensors – acoustic, shock, and a dual technology (acoustic/shock) sensor.

a. Acoustic Sensors: Acoustic sensors listen for the high frequency vibration noise typically created when the initial shattering impact is made on the window. Once impact is made, the breaking glass causes high frequency vibrations that travel away from the point of impact toward the outer edges of the glass surface. These vibrations are detected by the acoustic sensor and forwarded to the processor, which passes the signals through a filter, compares the frequencies for a match, and generates an alarm if appropriate.

b. Shock Sensors: When shock sensors are used, a sensor is required for each pane of glass. Shock sensors are piezoelectric transducers that detect the 5 KHz frequency shock wave that is typically created when glass is broken. When the processor detects this shock, it annunciates an alarm. There are two types of shock sensors: *electric* and *non-electric*. Most sensors are the electric types that operate using continuous, low amperage, supervisory current. When an electric transducer receives a shock wave, it bends slightly and generates a very small electric current that changes the supervisory current that the processor senses. Non-electric transducers are passive and do not use a continuous current. When a non-electric transducer receives a shock wave, it bends slightly and generates a

very small electric current that the processor senses. Non-electric sensors have a lower nuisance alarm rate than the electric sensors.

c. Dual Technology Acoustic/Shock Sensors: In dual technology glassbreak sensors, an acoustic device is linked with a shock device. This combination uses the complementary capabilities of both devices to reduce nuisance alarms from background noise, such as radio frequency interference and the noises created by office machines. The two sensing elements are located within a single casing, and are connected electronically through the use of an *AND* logic circuit. The *AND* circuit requires both input sensors to signal an alarm before the gate changes the output to the alarm state.

The acoustic portion of the sensor uses a microphone to detect frequencies associated with breaking glass. A processor filters out unwanted frequencies and only allows frequencies at certain ranges to be analyzed. Once the processor receives a signal, it is compared to those associated with glass breakage. If the signal matches the frequency characteristics of breaking glass, then a signal is sent to the *AND* circuit.

The shock portion of the sensor senses a 5 KHz frequency in the form of a shock wave created when glass is broken. When the processor detects this shock, it sends a signal to the *AND* circuit. Once the *AND* circuit has received both signals, an alarm is generated.

3. Applications:

a. Interior: Glassbreak sensors are for interior use. In addition to monitoring doors and windows, this technology is useful in applications where display cases are featured, such as museums, department stores, or jewelry counters. Sensors should be mounted on the window glass, frame, wall, or ceiling, according to the manufacturer's specifications.

NOTE: Sensors affixed to window glass use an adhesive. The mounting adhesive will need to withstand long exposure to summer heat, winter cold, and condensation that might collect on the window.

Glassbreak sensors should be used in conjunction with contact switches, such as balanced magnetic switches, to detect intrusion by opening a window instead of breaking it. Additional technologies should be employed to protect the area against intrusions through doorways, or cutting through walls or ceilings. Microwave or video motion detection offer enhanced detection capability in such scenarios.

b. Exterior: Glassbreak sensors are not typically found as components of exterior security applications.

c. Portable: Portable wireless glassbreak sensors are available. They are sometimes included with other sensors in portable packages for short-term personal security or building security applications.

d. Aquatic: Glassbreak sensors are not used underwater.

4. Reliability Considerations:

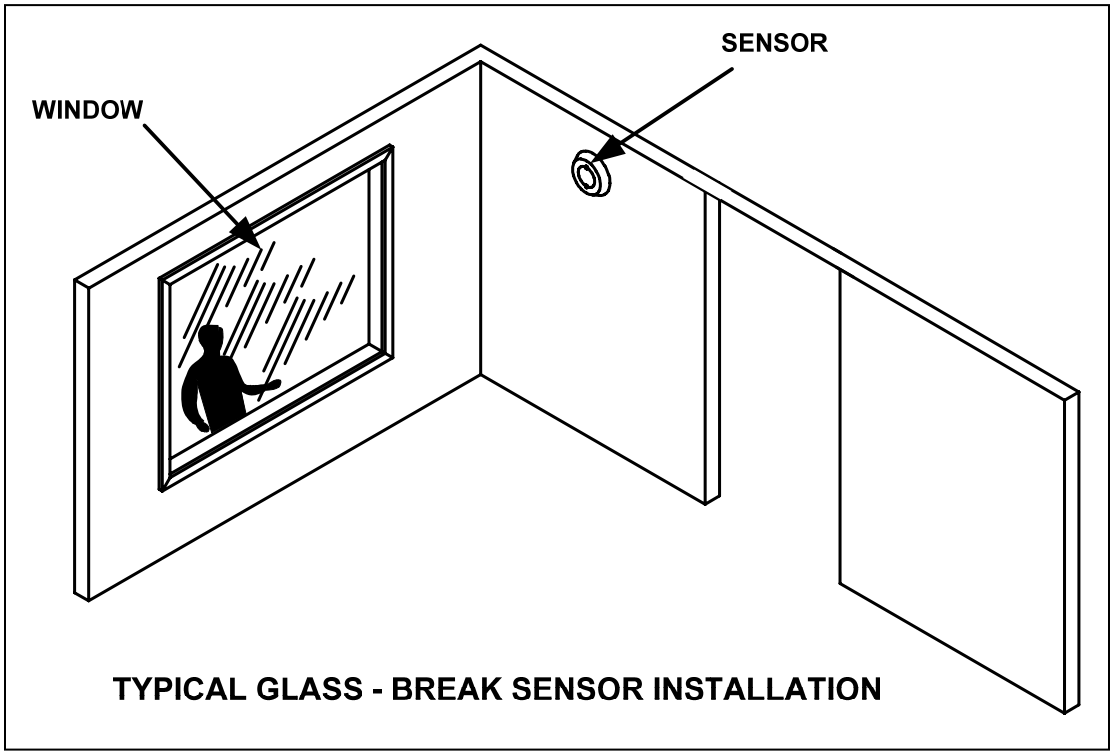
a. Conditions that Reduce Detection Probability: The most likely cause of unreliable detection is a conflict between the acoustic characteristics of a room and the sensor's performance specifications. "Soft" acoustic rooms with carpeting and draperies will absorb some of the energy emanating from breaking glass and will reduce the amount of energy reaching the sensor. Changing a room's acoustic characteristics by adding window shutters, blinds, draperies, rugs, or other objects after calibrating the sensor can diminish the sensor's reliability. Poor detection performance may also result from inappropriate placement or from attaching `a sensor on too large a window

NOTE: Windowpanes should be checked for cracks and repaired prior to installing a glassbreak sensor. This ensures that a good quality signature will be produced if a window is broken.

b. Causes of Nuisance Alarms: Improper calibration or installation, radio frequency interference (RFI), and sharp impact noises can cause nuisance alarms. Office and industrial machinery can produce noise in the glassbreak sensor's frequency detection range.

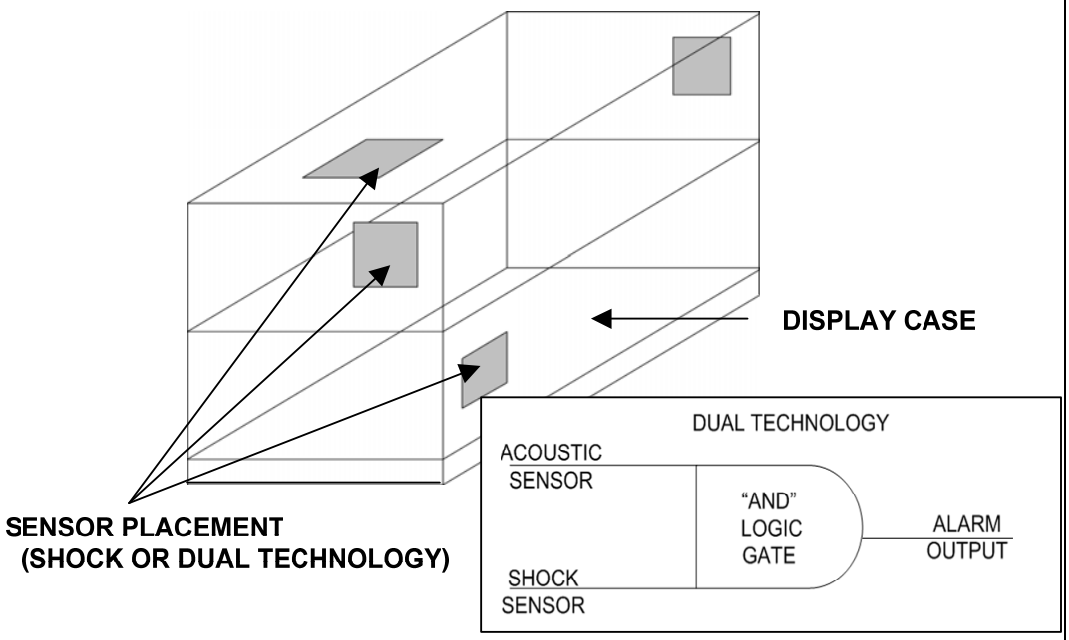
c. Vulnerabilities: Removing or cutting an opening in a window can fail to activate a sensor, including one mounted on the window glass itself. Muffling the sound of breaking glass distorts the break frequency and reduces the probability of generating a matching frequency that would trigger the alarm.

WALL MOUNTED GLASSBREAK SENSOR



TYPICAL GLASS - BREAK SENSOR INSTALLATION

SHOCK SENSORS/DUAL TECHNOLOGY



- **SHOCK SENSORS ATTACH DIRECTLY TO GLASS**
- **SHOCK SENSORS DETECT 5 KHz SHOCK WAVE**
- **DUAL TECHNOLOGY SENSORS (ACOUSTIC/SHOCK) ALARM ONLY IF BOTH SENSORS ARE IN AN ALARM STATE**

MICROWAVE SENSORS

1. Introduction: Microwave sensors are volumetric motion detection devices that establish and monitor a microwave energy field in a designated zone. A movement in the zone disturbs the field and generates an alarm. Microwave sensors are designed for interior, exterior, and portable applications.

2. Operating Principle: Microwave sensors transmit microwave energy in the "X" band (10 GHz) and "K" band (24 GHz). There are two basic types of microwave sensors: monostatic sensors, which have the transmitter and receiver encased within a single housing and bistatic sensors, in which the transmitter and receiver are two separate units creating a detection zone between them. Monostatic systems are often used to cover smaller areas or openings, or areas where it is not practical to install separate transmitter and receiver units. A bistatic system can cover longer distances and is typically used when more than one set of sensors is required. Bistatic systems are often used to monitor long perimeters, such as fence lines, gaps in fencing, or building exteriors.

a. Monostatic Units: The transmitter and receiver are contained in the same housing. Many models allow the user to configure the beam and detection zone by making adjustments to controls in the unit. They are most sensitive to movements toward or away from the sensor (radial movement). Fine control of the detection zone can be achieved by adjusting the duty cycle of the receiver. If the receiver is only briefly turned on, then only the reflections from nearby objects in the zone will be detected. The area where the transmitter can pick up all reflected frequencies is known as the receiver cut off (RCO) zone. Microwave energy reflected from objects that arrives at the receiver during the off portion of the duty cycle is not detected. Monostatic microwave sensors generally offer the user a choice of frequencies within the operating band to minimize nuisance alarms caused by emissions at the same frequency from other nearby equipment. Some monostatic sensors are multiplexed, so that the sensors transmit sequentially at different frequencies to avoid interference-induced nuisance alarms. Some systems use two alternating frequencies in the transmission phase to discriminate small objects nearby from large objects at the far end of the

detection zone. The detection of an intrusion is achieved by comparing the reflected microwave energy received with a pre-established baseline level. Deviation from the pattern of reflected microwave energy generates an alarm. Monostatic units are available with detection ranges up to 400 feet, depending on the detection pattern.

b. Bistatic Units: In bistatic microwave systems, the transmitter and receiver are separate units, creating the detection zone between them. Vendors offer several antenna configurations, which control the shape and range of the detection beam, from long and narrow to short and oval. Moving objects in the field of coverage reflect some of the transmitted microwave energy in random directions. When the receiver detects a change in the signal caused by this reflection, an alarm is generated. Bistatic systems generally offer longer detection zones than monostatic, up to 1,500 feet.

3. Applications:

a. Interior: Most interior microwave sensors are of the monostatic configuration. They can be used to monitor confined spaces, such as vaults, special storage areas, hallways, and service passageways. Using other independent sensing systems, such as passive infrared or video motion detection, with a microwave system enhances the overall detection probability.

b. Exterior: Either monostatic or bistatic systems can be used in exterior security applications to monitor an area, a perimeter line, or approaches to a door, wall, or building. In situations where a well-defined volume of coverage is needed, the monostatic system should be used. Either system can be used to detect intruders crawling or rolling on the ground within the microwave energy field. Both systems give better results when the detection zone is flat, uncluttered, and homogenous. Vegetation should be kept to three inches or less in height. Trees, shrubs, outbuildings, and large equipment all create dead pockets in the protected area. Surface irregularities can cause puddles to accumulate and increase nuisance alarms. Many vendors recommend a gravel bed surface in the detection zone for improved microwave reflection characteristics. Other detection systems, such as video motion detection or fence

sensors, may be used independently to enhance the probability of detection and improve the ability of security personnel to assess alarms.

c. Portable: Portable versions of microwave sensors are available for interior and exterior use. They are often components of deployable packages of different types of sensors for temporary or quick response situations. Interior portable sensors are small, wireless, battery-powered monostatic devices that can be attached to walls easily, moved, and set up quickly using a portable computer as the control center. They are sometimes included as components of portable security packages. Exterior portable systems can be set up on temporary stands or tripods; may be powered by generators, batteries, or solar cells; and may be connected to control centers using wireless or cable communications. Exterior portable systems may be monostatic or bistatic.

d. Aquatic: Microwave systems are not suitable for over-water or underwater applications. Moving water reflects microwave energy and generates unacceptable levels of nuisance alarms. Radar, coupled with a video assessment system, is more suited for over-water surveillance and detection applications.

4. Reliability Considerations:

a. Conditions for Reduced Detection Probability: Since microwave sensors operate in the high frequency spectrum (X and K bands), close association or proximity to other high frequency emitters can adversely affect the detection probability of these sensors. Multiple microwave sensors used in the same area must be set at different frequencies or multiplexed to operate sequentially to avoid nuisance alarms from interference. Strong electric or magnetic fields, such as those associated with radio transmitters, large electric motors, generators, or fluorescent lighting, can affect the ability of microwave sensors to function properly.

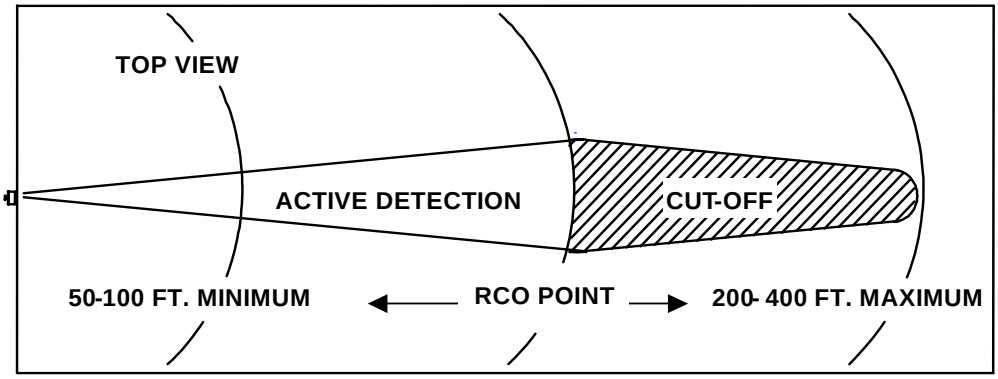
It is essential to test for and compensate for any dead spots (areas of no detection) created by metal objects such as dumpsters, shipping crates, trash cans, or electrical boxes. The dead spots create areas susceptible to intrusion attempts. Since monostatic microwave sensors are most sensitive to radial movements, it is

important to situate the sensors so that an intruder's expected movement has the greatest possible radial component.

b. Causes of Nuisance Alarms: Because of the high frequencies of microwave energy, air currents, temperature changes, and humidity do not affect the signal and sensor. The high frequency signal can easily pass through standard walls, glass, sheet rock, and wood. This can result in nuisance alarms caused by movement adjacent to, but outside the intended protected area. In addition, signals reflected off water puddles and metal objects can "extend" sensor coverage beyond the intended area and create the potential for nuisance alarms. Exterior detection areas must be engineered to be flat, to have constant slope for positive drainage, and be free of obstructions. Loose fence mesh and blowing snow can also cause nuisance alarms.

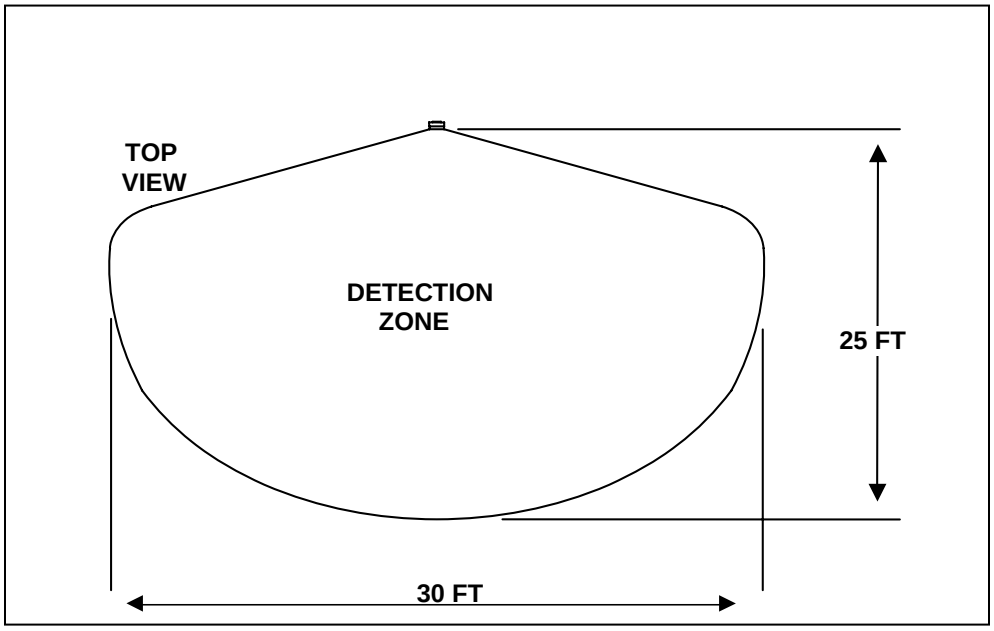
c. Vulnerabilities: An intruder may be able to take advantage of the dead zone adjacent to the transceiver assembly unless those zones are protected by an overlapping or basket weave arrangement of microwave sensors, or another detection technology. Someone with access to the protected area may be able to map the detection pattern to identify an approach path outside the bounds of detection. An intruder may use the cover of any signal obscuring or blocking objects in the surveillance field and advance with a deliberately slow rate to reduce the probability of detection. Regularly calibrating the sensors, sanitizing the area, and using other independent types of sensors are important to maintaining a high probability of detection.

TYPICAL BISTATIC MICROWAVE DETECTION PATTERN

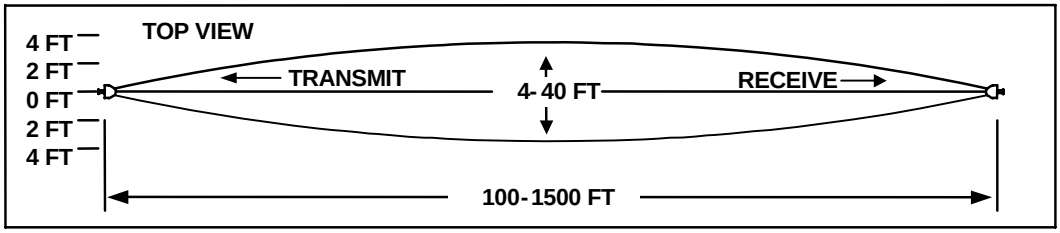


RANGE WILL VARY, DEPENDING UPON DESIGN

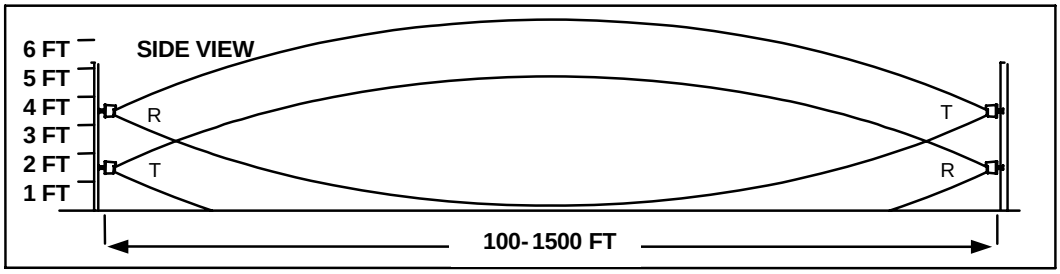
TYPICAL SHORT RANGE MONOSTATIC MICROWAVE DETECTION PATTERN



TYPICAL BISTATIC MICROWAVE DETECTION PATTERN

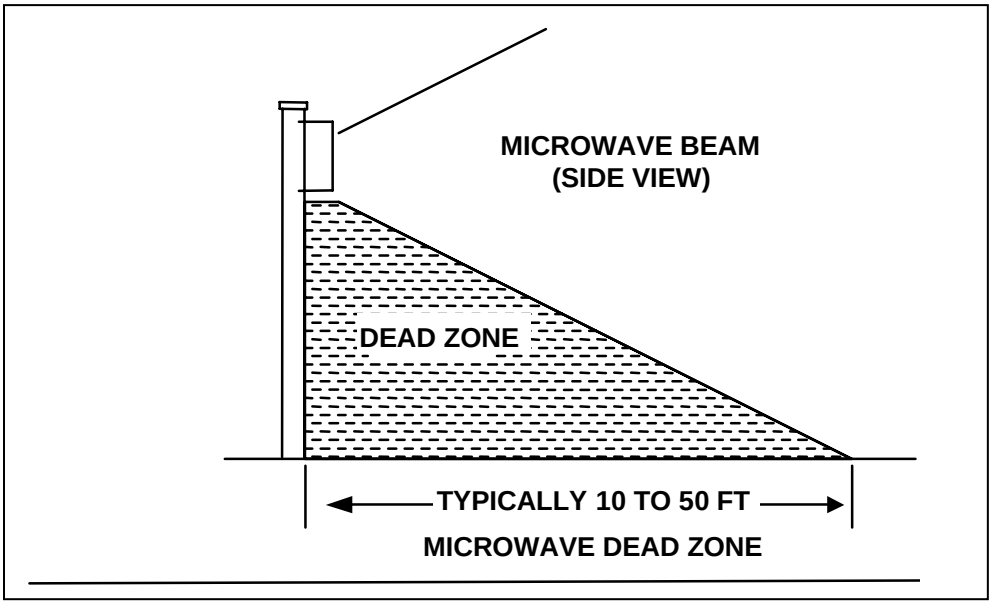


LENGTH AND WIDTH OF DETECTION PATTERNS WILL VARY, DEPENDING UPON DESIGN.

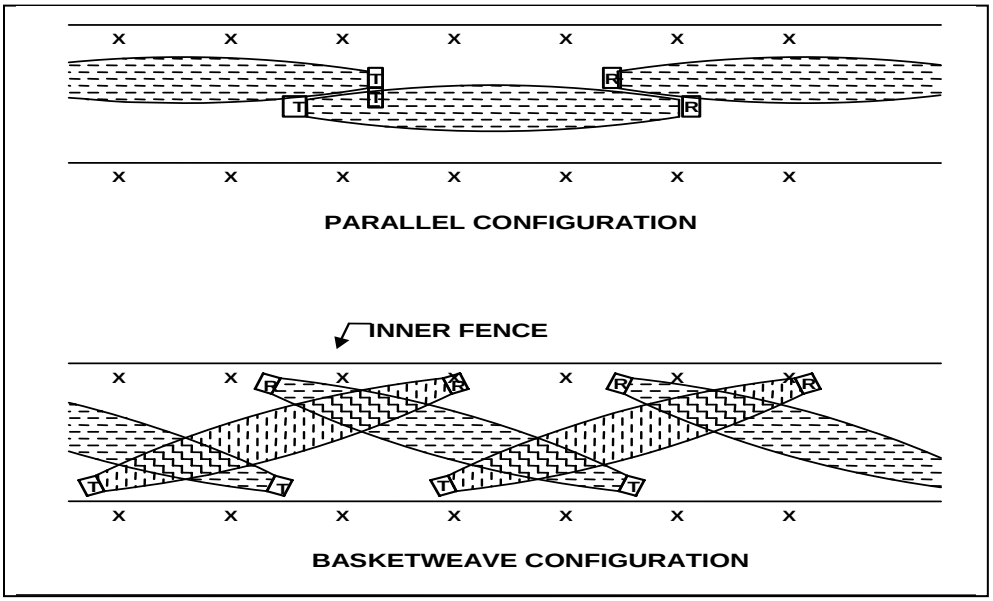


THE MICROWAVE SENSORS CAN BE MOUNTED IN A DUAL CONFIGURATION TO PROVIDE A GREATER PROBABILITY OF DETECTION.

MICROWAVE SENSOR ZONES



BISTATIC MICROWAVE LAYOUT CONFIGURATIONS



This page intentionally left blank.

STRUCTURAL VIBRATION

I E

1. Introduction: Structural vibration sensors are designed to detect attempts to break into vaults, safes, automatic teller units, and high value reinforced areas of relatively small volume. The sensors detect the mechanical vibrations caused by chopping, sawing, drilling, ramming, explosions, thermal cutting, or any other activity intended to penetrate the structure. Fiber optic or strain sensitive cable products are more often chosen to protect the walls, floors, and ceilings of large spaces such as entire rooms or buildings from breaking-and-entering penetrations.

2. Operating Principle: Current products use piezoelectric transducers to detect the vibrations generated during attempts to penetrate the protected structure. The devices are mounted on the surfaces of the protected zone where they detect changes from the ambient vibration profile. Some products allow several sensors to be wired together in a network to protect surfaces larger than the detection area of a single sensor. All products have tamper protection circuitry.

Some systems use three processing channels, each dedicated to detecting particular characteristics of amplitude, frequency, and duration. A threshold detector looks for very high amplitude, short duration signals from explosions. A counting circuit looks for moderate-to-high amplitude, intermittent, short duration signals typical of knocking from hammers and chisels. A frequency analysis circuit responds to low amplitude, long duration activity from mechanical cutting and drilling tools as well as thermal cutters. Some products have a thermal sensor instead of frequency analysis circuitry to detect the use of cutting torches.

3. Applications:

a. Interior: Vibration sensors should be placed securely near the location where an intrusion is expected. The sensors' spacing and range of detection depends on the structure's ability to transmit vibrations and should be determined by an independent security consultant's recommendations. An additional independent sensor technology, such as passive infrared, audio, microwave, or video motion detection is recommended to detect intrusion activities that lack sufficient

vibration characteristics to trigger the sensor and to allow security personnel to assess alarms.

b. Exterior: Exterior vibration sensors are commercially available to protect high value objects located out-of-doors. Such sensors are weather-tight and have enhanced durability and robustness. In most respects, their uses are similar to interior sensors. They should be augmented with other sensing or surveillance technologies to detect intrusion activities that lack sufficient vibration characteristics to trigger the sensor and allow security personnel to assess alarms.

c. Portable: These devices are not marketed as being portable.

d. Aquatic: These devices are not designed for use underwater.

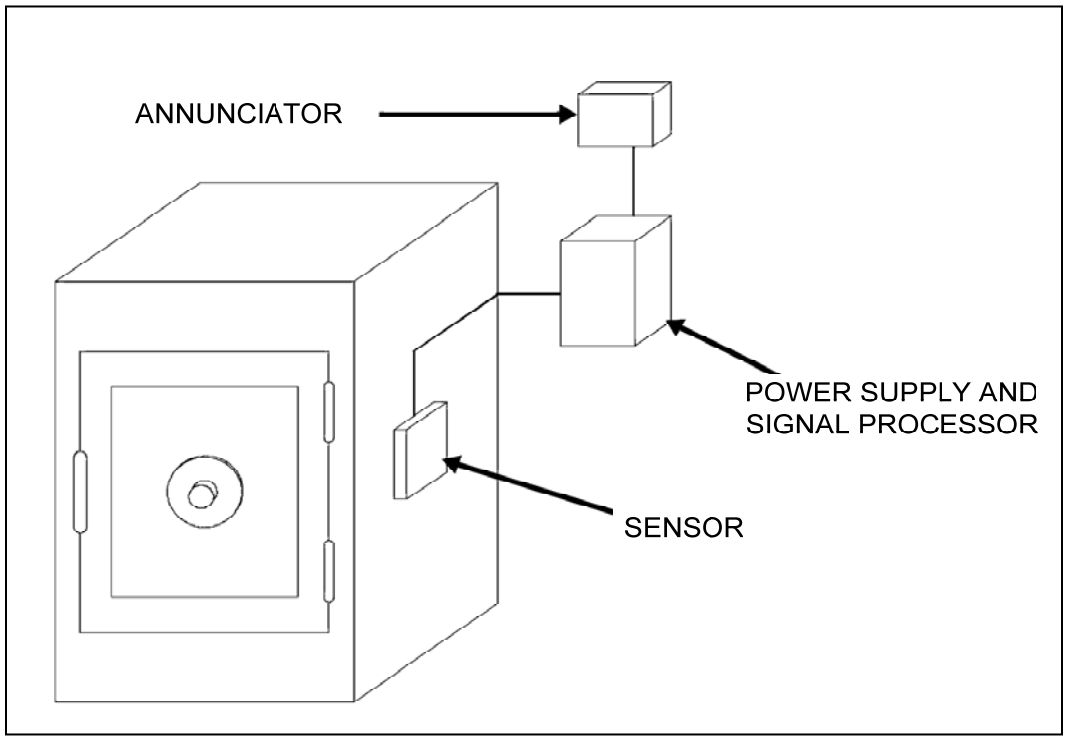
4. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Installing a vibration sensor on a surface that is unstable or subject to background vibrations will require higher than optimal sensitivity settings that may reduce the probability of detection. Surfaces of limited structural integrity, such as wallboard or thin metal, are prone to vibrations from sources other than intrusion activities. In those circumstances, vibration sensors should be positioned over a main support. Mounting sensors on materials such as rugs, fabric, or heavy wall coverings that absorb vibrations will also reduce the probability of detection.

b. Causes of Nuisance Alarms: Poor sensor placement is a primary cause of nuisance alarms. Vibration sensors may generate alarms if mounted on walls exposed to vibrations from trains, aircraft, machinery, or other strong vibration sources. Vibration sensors should not be used if such conditions are present.

c. Vulnerabilities: A properly engineered vibration sensing system is difficult to bypass during an attempt to gain access to a protected structure. Attempts to isolate these circuits would require sophisticated knowledge of the sensor system. Some systems may be vulnerable to penetration activity with vibration characteristics that are insufficient to cause an alarm.

STRUCTURAL VIBRATION SENSOR



This page intentionally left blank.

AUDIO SENSORS

I P

1. Introduction: Audio detectors listen for noises generated by an intruder's movement in a protected area. They can be used to protect interior spaces such as entrance foyers, critical data or resource storage areas, automatic teller machines (ATM), and vaults.

2. Operating Principle: The sensor is made up of two devices: (1) microphones mounted on the walls or ceilings of the monitored area, and (2) an amplifier unit that includes processing circuitry. The microphones collect sound for analysis by the processor circuit, which is calibrated to a noise threshold level characteristic of an intrusion attempt. If a threshold signal is detected from a monitored area within a selected time period, an alarm signal is generated.

3. Applications:

a. Interior: Audio sensors are used in interior applications. Sensors should be mounted in areas where the predicted intrusion noise is expected to exceed that of the ambient background noise. If background noise exists and system calibration is improperly set, the microphone may be unable to identify an intrusion noise. Audio sensors should be used in conjunction with other types of sensors (passive infrared, video motion detection, or microwave) to enhance the probability of detection.

b. Exterior: Audio sensors are not designed for exterior intrusion detection applications. Several exterior perimeter sensor technologies have an audio listening capability that can be useful for assessing alarms, but not for initial detection.

c. Portable: Portable audio systems are available for many interior applications.

d. Aquatic: Audio systems are not designed for underwater use.

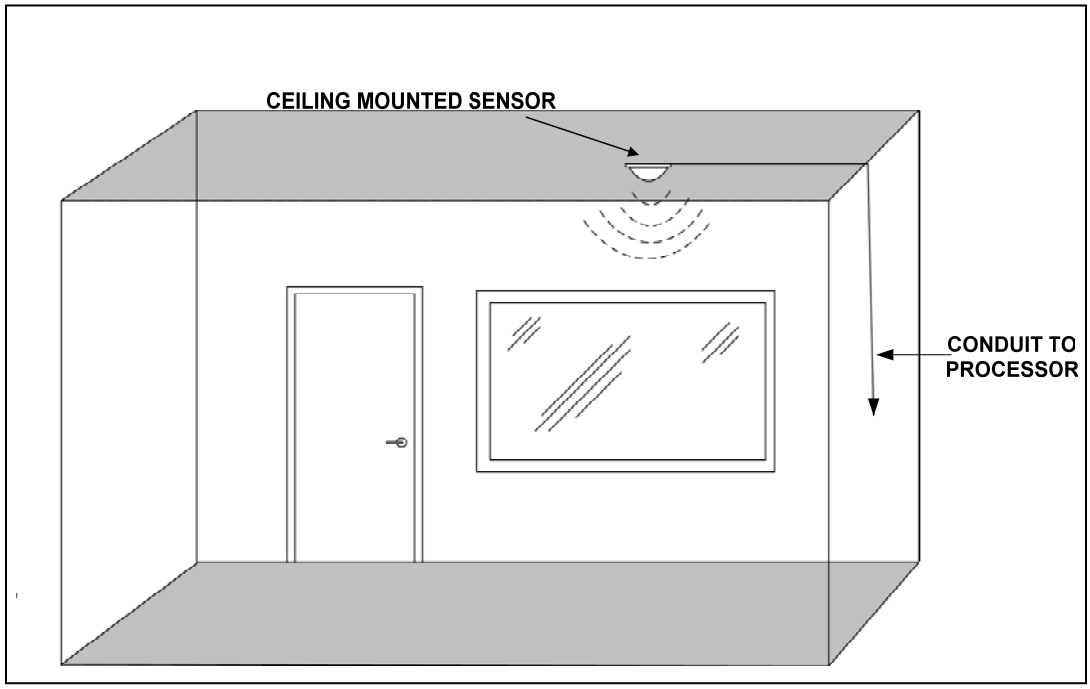
4. Reliability Considerations:

a. Conditions for Reduced Detection Probability: The principle causes of unreliable detection are improper sensitivity settings that cannot filter out extraneous background noise from clocks, office equipment, or heating and air conditioning units.

b. Causes of Nuisance Alarms: Excessive background noise from sources such as aircraft, trains, or extreme weather conditions may generate an alarm. If any of these factors are frequently present, audio sensors should not be used.

c. Vulnerabilities: An intruder using slow, deliberate entry techniques that muffle the normal sounds of movement may avoid detection. The use of a companion detection technology such as video motion detection or passive infrared can enhance the probability of detection and offset the vulnerabilities of audio monitoring systems.

AUDIO SENSOR CONFIGURATION



This page intentionally left blank.

PASSIVE INFRARED

1. Introduction: Passive infrared (PIR) sensors detect the thermal energy emitted by a heat source. The sensor is typically divided into several sectors or zones, each defined with specific boundaries. Detection occurs when an emitting heat source (thermal energy) crosses two adjacent sector boundaries or crosses the same boundary twice within a specified time.

2. Operating Principle: Passive infrared sensors detect the electromagnetic radiated energy of infrared (IR) wavelengths. They are most sensitive to movements across the field of view (tangential movement). An object emits infrared energy as a function of its temperature; therefore, infrared energy is often referred to as "thermal" energy. Infrared wavelengths are longer than the wavelengths of visible light, and infrared energy is invisible to the naked eye. Passive infrared sensors detect thermal radiation by sensing the change in contrast over time between a heat source and the cooler background. They divide the detection zone into segments. The change in infrared energy in two or more segments will generate an alarm.

In order to avoid generating an alarm in response to environmental thermal deviations, processors employ either "rate of change" measurement circuitry or "bi-directional pulse counting" circuitry. In rate of change measurement, the processor evaluates the speed at which the energy changes between segments in the detection zone. Movement by an intruder in the field of view produces a fast rate of change, while gradual temperature fluctuations produce a slow rate of change. In the bi-directional pulse counting technique, signals from separate thermal sensors produce opposite polarity. An intruder entering a field of view moving at a typical speed (walk or faster) will normally produce several signals, which results in a detection.

Optics and reflective principles play an important role in the design and function of a passive infrared intrusion detection sensor. Either a Fresnel lens or the Reflective Focusing method is used to focus the small amounts of thermal radiation received at the sensor on to the sensing elements.

a. Fresnel Lens: Fresnel optical technology allows energy to travel directly to the sensing elements and enables the detection field to be shaped for specific applications. Some examples include a wide-angle lens to monitor a room, a long focal length lens for an interior hallway or exterior fence line, a curtain lens to monitor a doorway, and a "pet alley" lens, which ignores heat signatures from below an adjustable height. Some sensors are capable of using a set of different lenses to change fields of view and zones of surveillance, as well as concentrate the infrared energy from the detection zone.

b. Reflective Focusing: In this method, the energy waves are reflected from a concave mirror inside the sensor housing and directed onto the sensing element. This type of sensor incorporates some of the components and functions of telescopes and video cameras.

3. Applications:

a. Interior: Interior passive infrared sensors should be installed on walls or ceilings, with a detection pattern covering the possible intrusion zones. Each detection or surveillance zone can be thought of as a "searchlight" beam that widens as the zone extends farther from the sensor with different segments being illuminated while others are "dark." This design characteristic allows the "beam" to be directed to areas where protection is needed while ignoring other areas, such as known sources of nuisance alarms. Ceiling mounted passive infrared sensors theoretically can provide a 360° surveillance pattern.

b. Exterior: Exterior detectors can be employed in the same manner as interior sensors, although curtain lens technology is recommended for fence lines or perimeter monitoring to provide a full barrier protection zone by eliminating the typical dead zone. Models mounted on towers may provide a 360°surveillance pattern.

c. Portable: Mobile versions of exterior passive infrared systems are available to establish temporary intrusion detection perimeters around vehicles, buildings,

construction sites, emergency or disaster incident sites, and many other applications.

d. Aquatic: Passive infrared sensor systems are not suitable for underwater or overwater use.

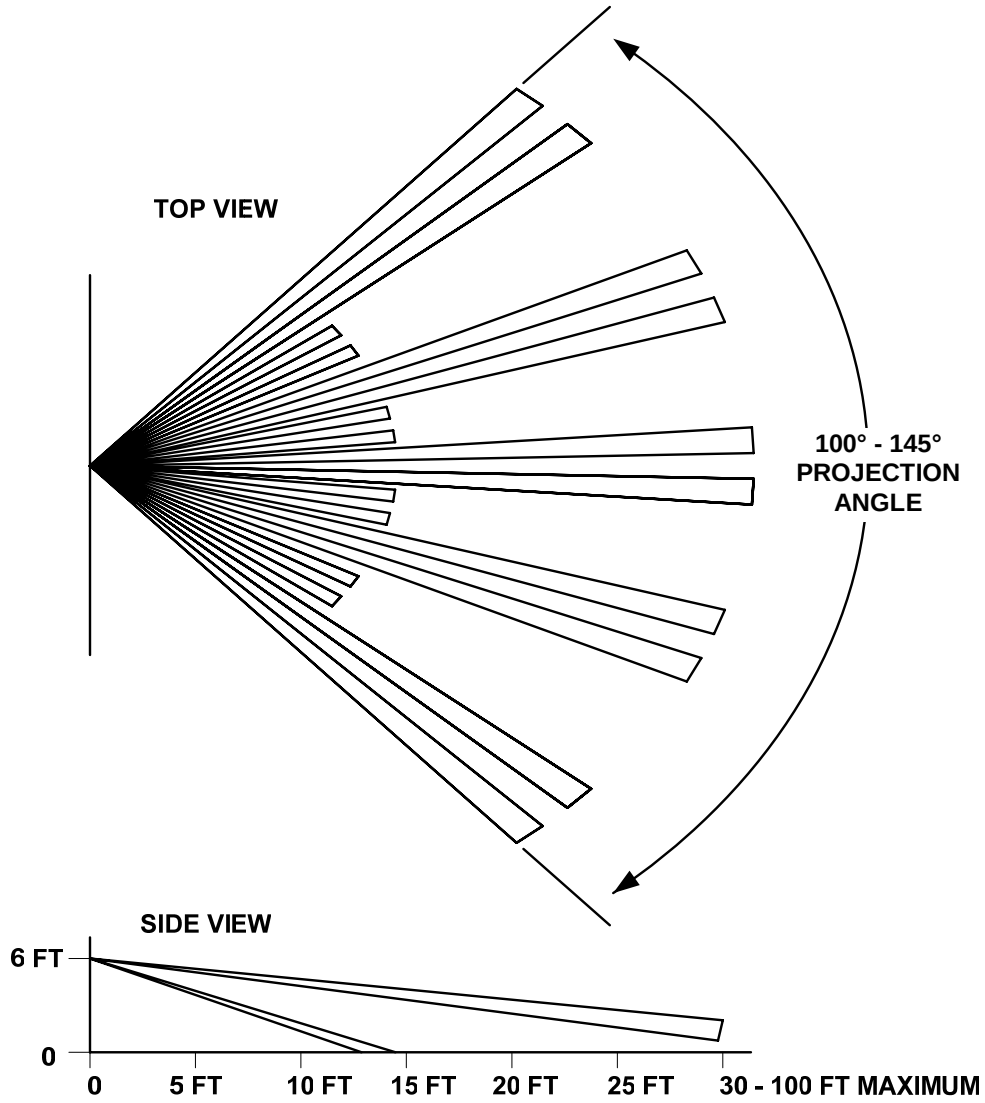
4. Reliability Considerations:

a. Conditions for Reduced Detection Probability: Since passive infrared sensors are most sensitive to tangential movements, sitting the sensor so that an intruder will pass across the sensor's field of view will result in better performance. Because passive infrared detection is based on relative temperature, detection becomes less sensitive as the environment approaches the temperature of the intruder. Another type of sensor should be used independently with a passive infrared system to enhance the overall system's detection probability. Complementary sensors for interior applications include microwave sensors, balanced magnetic switches, and glassbreak detectors. For exterior applications, video motion detection is often a good complement.

b. Causes of Nuisance Alarms: Small animals or rodents moving in the detection field can cause nuisance alarms. Facility heating and air conditioning effects, ovens, and hot water pipes can also cause nuisance alarms if they are in the field of view. Segmented detection zones provide more detailed information to microprocessors that results in more accurate detection and rejection of pets or animals. In addition, car headlights or other sources of focused light can affect passive infrared sensors that are not designed to filter visible light. Black mirror technology blocks white light from reaching the sensor and reduces nuisance alarms from sunlight or vehicle lights. Intermittent heating and cooling of objects in a room could generate nuisance alarms under some circumstances.

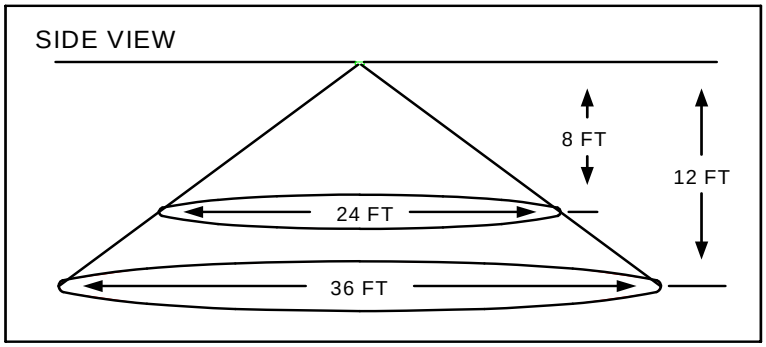
c. Vulnerabilities: An intruder using thermal camouflage techniques can reduce his infrared signature and lower the probability of detection. Walking directly toward a passive infrared sensor reduces the detection capability because the intruder may avoid breaking the boundaries of the detection beams.

PASSIVE INFRARED SENSOR

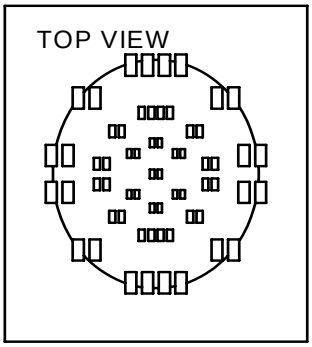


THE NUMBER, RANGE, AND PROJECTION ANGLES OF THE DETECTION BEAMS VARY DEPENDING UPON DESIGN.

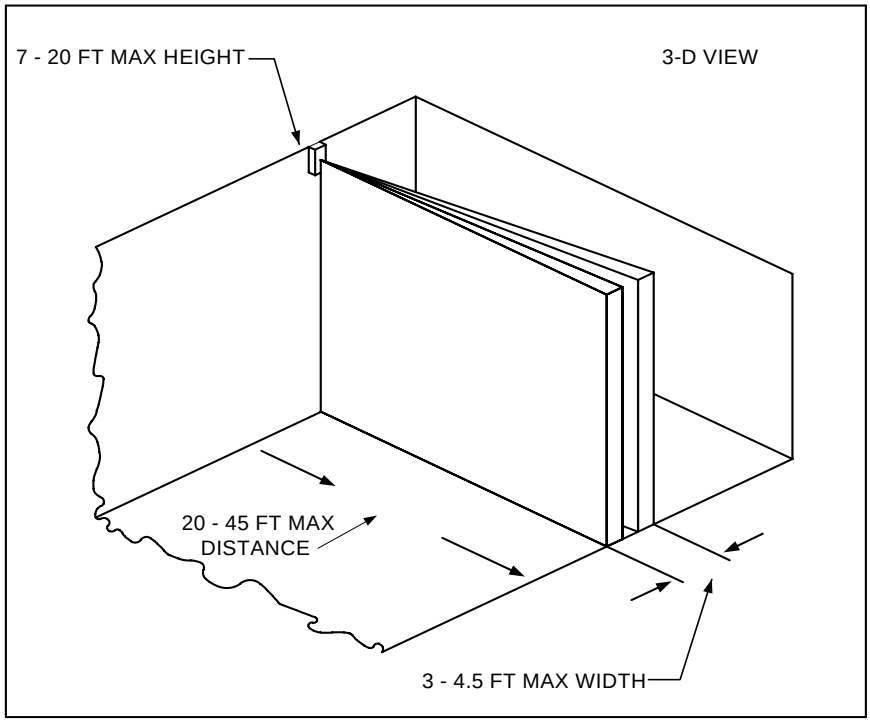
TYPICAL PIR COVERAGE PATTTERN (CEILING MOUNTED)



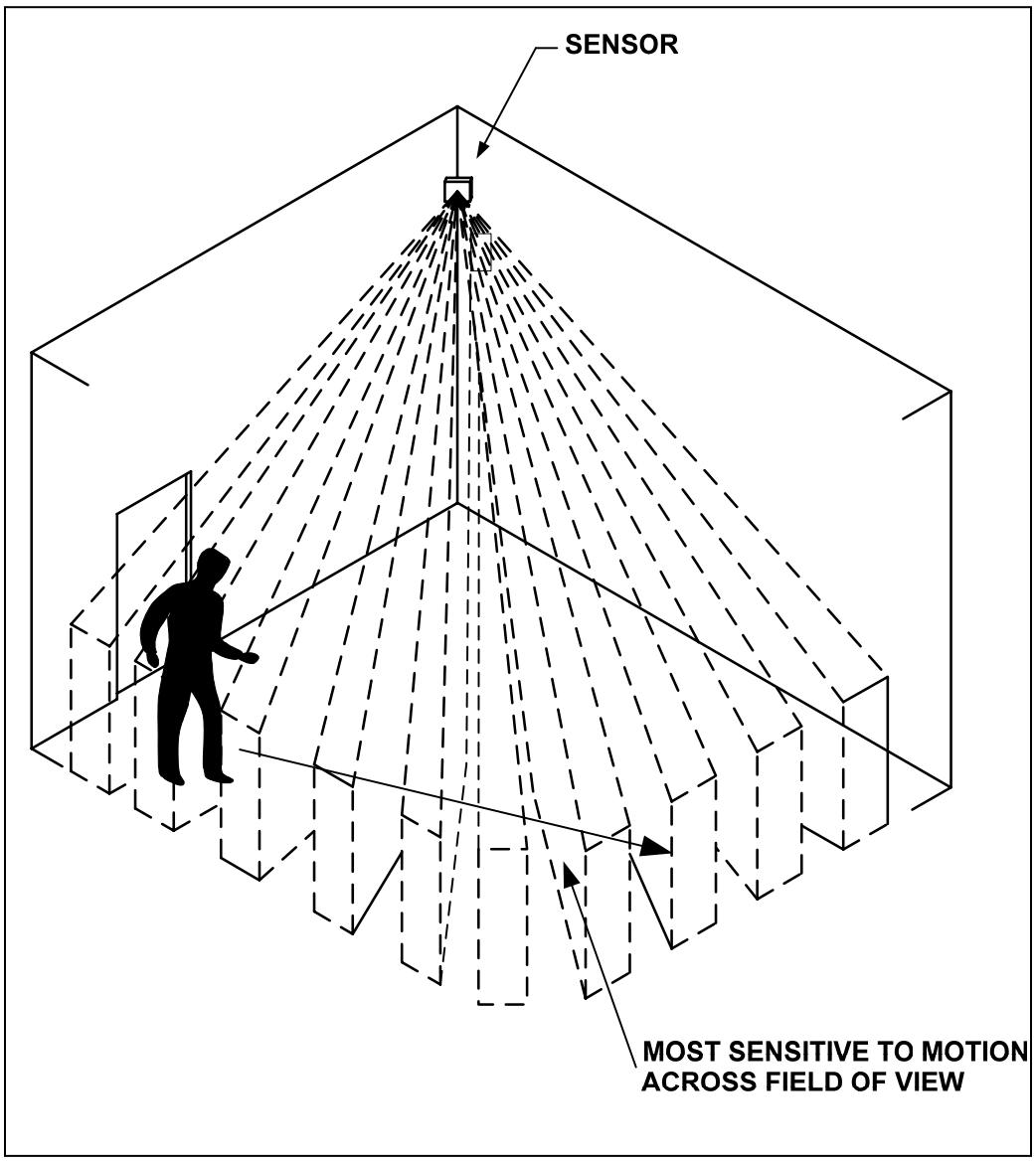
DISC FLOOR BEAM PATTERN



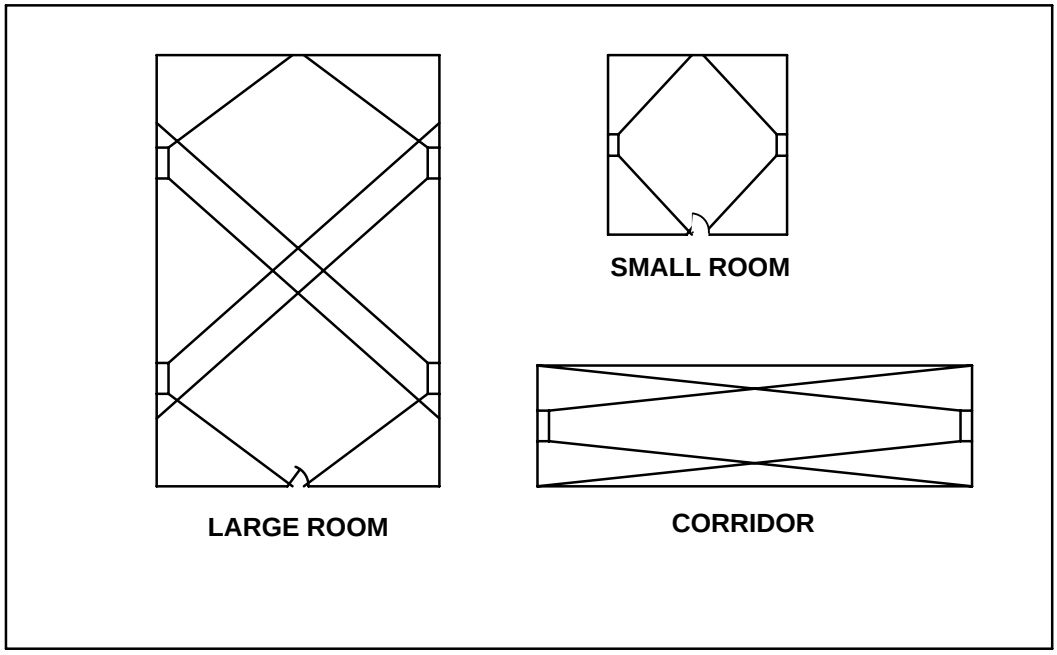
TYPICAL PIR CURTAIN DETECTION PATTERN (WALL MOUNTED)



PASSIVE INFRARED



PASSIVE COVERAGE/PLACEMENT PATTERNS



This page intentionally left blank.

ACTIVE INFRARED

1. Introduction: An active infrared intrusion sensor uses a beam of infrared light, which is invisible to the human eye, as the detection medium. The beam functions essentially as a trip wire between the transmitting and receiving units, with an alarm caused by a disruption of the beam. Often several infrared sensors are used to create an invisible fence surrounding a protected area. Active infrared sensors have both interior and exterior applications.

2. Operating Principle: An active infrared sensor system is made up of two components: the transmitter and the receiver. Generally, the transmitter uses an infrared light emitting Diode (LED) to create the detection beam. The transmitter projects the beam of infrared light toward the receiving unit. At the receiver, a lens focuses the beam onto a collecting cell. The collecting cell converts the beam's energy into an electrical or digital signal. An intruder passing through the detection field will interrupt the beam and temporarily cause the signal to fall below a preset threshold value. The receiving unit monitors the signal and generates an alarm whenever the signal exceeds that preset threshold. Threshold values can be set to generate an alarm from partial or complete interruptions of one or more beams.

3. Types: There are two types of active infrared sensors available: (a) monostatic and (b) bistatic.

a. Monostatic: Monostatic sensors contain the transmitter and receiver within a single housing unit called a transceiver. The transmitter projects a beam toward a mirror or a reflective device designed specifically for use with the transceiver. The reflected beam returns to the receiver in the transceiver unit. Changes in the strength of the beam for a specific amount of time will cause an alarm. The maximum operating range for monostatic systems is less than for bistatic systems because of signal strength losses at the reflectors. Monostatic systems are generally used to detect intrusions through gates, doors, or other openings.

b. Bistatic: Bistatic sensors have separate transmitter and receiver units to create a detection zone between them. Bistatic systems can operate over much longer ranges than monostatic systems and are the systems of choice in exterior long-range applications. The detection zone of a bistatic system can extend up to 1,000 feet.

4. Applications:

a. Interior: Interior applications may utilize either monostatic or bistatic sensors. Depending on the distances, either bistatic or monostatic systems can be used to create a fence across a doorway or hall, or to detect an intrusion within the volume of a room or hallway. A second independently operating detection system, such as microwave or video motion detection, may be used to increase the overall probability of detection and allow security personnel to assess alarms.

b. Exterior: Monostatic exterior active infrared systems are generally used to detect intrusions through gates or other openings. Longer-range sensors are generally bistatic systems that require the area between the two units to be uniformly level and clear of all obstructions that could interfere with the infrared signal. Low spots in the terrain create gaps in the detection pattern while obstructions will disrupt the detection beam. Typically, active infrared sensors are used in conjunction with a single or double fence barrier, which defines the perimeter to be protected. A bistatic active infrared detection zone can extend up to 1,000 feet.

Precise alignment of the transmitter to the receiver is essential for reliable detection in bistatic systems. The transmitter and receiver units are easily misaligned by ground movements or by objects hitting a unit. The detection beam is relatively narrow, and the units require regular adjustment and maintenance.

In areas where freezing ground or extreme winds are expected, the transmitter and receiver foundations should be installed deeply enough to restrict movement of the two units. In areas where the units are susceptible to being hit or jarred, protective barriers should be installed. Snow and grass around the units should be

removed to maintain performance and to prevent damage, misalignment, and interference with the beam. Some manufacturers incorporate logic circuitry that can accept the lower lenses in a stack being obscured as a "snow mode."

c. Portable: Bistatic systems for exterior use are available in battery and/or solar powered portable versions. The units are self-supporting with integrated tripod stands and communicate to the control station through an automated radio transmission or telephone line. Portable active infrared systems are useful as components of a rapidly deployable perimeter defense kit.

d. Aquatic: Active infrared systems are not suitable for underwater or overwater use.

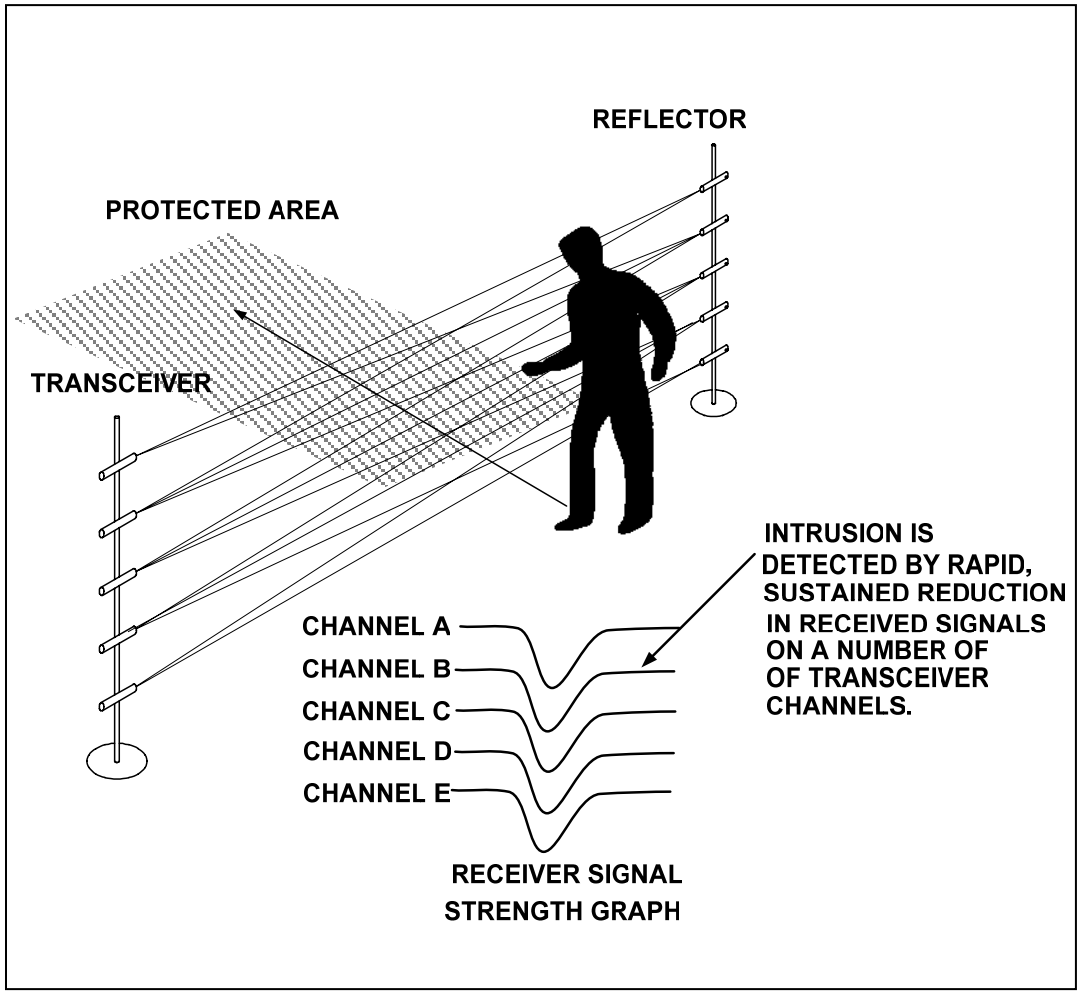
5. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Dust or other particles collecting on the receiver lenses or on the reflective surfaces of monostatic systems will reduce the detection capabilities. The infrared beam may need to be adjusted to prevent a light source from affecting detection and to avoid interference from adjacent areas. Weather conditions can also affect the performance of exterior systems. Fog, heavy rain, or airborne sand and dust can attenuate infrared energy and shorten the reliable detecting range. In areas where weather conditions are frequently severe, the use of active infrared technology may not be appropriate. Alternatively, the length of detection zones can be decreased to compensate for anticipated attenuation and scattering of the beams. Any surface irregularities between the transmitter and receiver units should be filled or graded to make the area uniformly level.

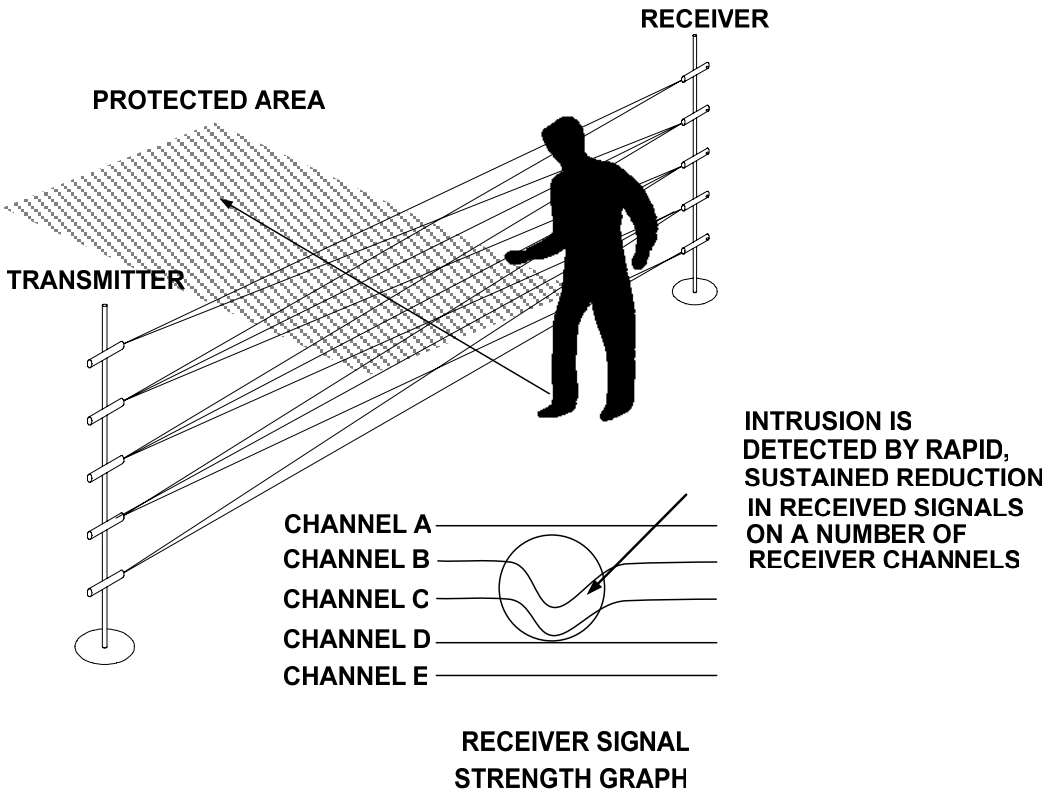
b. Causes of Nuisance Alarms: Very bright lights or sunlight shining directly into a receiver can activate some systems. Systems using digital processing may be less susceptible to light-induced nuisance alarms. For exterior systems, nuisance alarms frequently involve animal interactions within the protected area. Birds, in particular, can cause alarms that are difficult to classify. Plants and vegetation can generate an alarm, as well as provide nesting areas for food and wildlife, and should be removed from the protection zone.

c. **Vulnerabilities:** An intruder may defeat an interior monostatic system by noting the location of reflector surfaces and avoiding areas between those surfaces and the transceiver. Bistatic “fences” can be avoided by bridging or tunneling. Geophone sensors can be utilized to detect tunneling intrusions, and electrostatic field or microwave sensors can enhance detection in cases of bridging intrusions. A second typical defeat measure for exterior systems is to vault over the detection beams using the unit structure for support. Overlapping active infrared detection zones can counter this intrusion technique.

MONOSTATIC ACTIVE INFRARED MOTION SENSOR



BISTATIC ACTIVE INFRARED MOTION SENSOR



DUAL-TECHNOLOGY PASSIVE INFRARED / MICROWAVE

1. Introduction: Dual-technology passive infrared/microwave (PIR/MW) sensors use both passive infrared and microwave technologies in combination with an *AND* logic circuit to provide a sensor with a lower nuisance alarm rate (NAR) than if the sensors were used independently. This combination of sensor types is one of the more prevalent among products that combine two sensor technologies in one housing.

2. Operating Principle. In this dual-technology sensor, a passive sensor (passive infrared) and an active sensor (microwave) are combined in one housing. Both sensing elements are connected electronically through an *AND* logic circuit. The areas of coverage for each sensor are similar in size and shape, so that the detection zone is uniform. Since the two types of sensors will not detect an intrusion at precisely the same time, the system is designed to generate an alarm when both sensors detect an intrusion within a pre-selected time interval. Although a dual-technology sensor reduces the nuisance alarm rate, it also slightly reduces the probability of detection, since both sensors must have a positive detection within a time threshold before initiating an alarm.

NOTE: The technical parameters and operating characteristics of each sensor are described in the sections on microwave and passive infrared sensors.

3. Applications:

a. Interior: These sensors can be used for interior applications in the same manner as the passive infrared or microwave sensors separately. Multiple sensors with overlapping detection zones should be used to maximize the detection probability. Dual technology sensors should be supplemented with another detection technology, such as video motion detection, to enhance the detection probability and to allow security personnel to assess alarms.

b. Exterior: The sensors can be installed to protect a perimeter line, a fence, a buffer zone, or a structure. Exterior PIR/MW sensors should be supplemented with an additional detection technology, such as video motion detection, to enhance the detection probability and to allow security personnel to assess alarms.

c. Portable: PIR/MW sensors are not marketed as being portable. Interior systems, however, are small, available in wireless configurations, and relatively easy to install.

d. Aquatic: PIR/MW sensors are not designed for use overwater or underwater security applications.

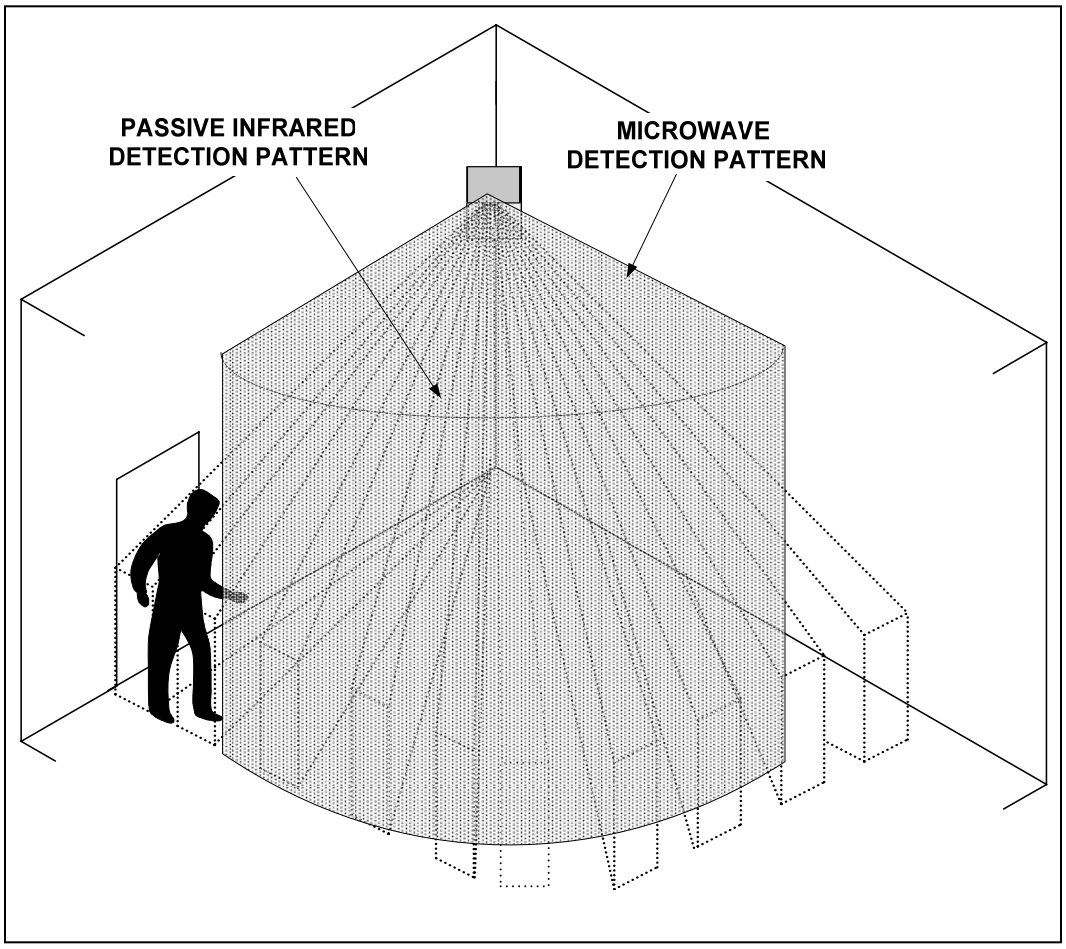
4. Reliability Considerations:

a. Conditions for Reduced Detection Probability: Passive infrared sensors have the greatest probability of detection when an intruder moves transversely to the sensor in the detection field. However, microwave sensors have the greatest probability of detection when an intruder moves toward or away from the sensor. Proper sensor placement, so that the sensor is not directly in line with or at a right angle to the protected area, is essential to maximize the probability of detection. Any condition that causes unreliable detection for either sensor will cause unreliable detection in a PIR/MW sensor. The *AND* logic circuit requires signals from both components to generate an alarm. In a controlled environment, though, dual-technology sensors can be both cost effective (cheaper than purchasing two individual sensors) and have a high detection probability and low nuisance alarm rate. More than one PIR/MW sensor should be used, with overlapping detection zones, to maximize detection probability.

b. Causes of Nuisance Alarms: Though the nuisance alarm rate for the dual-technology sensor is low, a combination of environmental conditions that would cause alarms in the individual sensors could result in an alarm from the dual sensor. Conditions that affect either sensor individually should be avoided to maintain the effectiveness of the dual-technology sensor.

c. Vulnerabilities. An intruder, with knowledge of the dead spots in the detection pattern, may be able to bypass all active regions. Otherwise, an intruder must defeat only one of the sensor systems to bypass the detector. Placement that minimizes one of the sensors' detection capabilities can result in a failure to detect an intrusion.

DUAL TECHNOLOGY DETECTION



FENCE VIBRATION

E P

1. Introduction: Fence vibration sensors are discrete devices mounted on fence fabric that detect disturbances associated with striking, sawing, cutting, climbing, or lifting the fence fabric. In a single detection zone, multiple sensors are connected in series by a cable to a signal processor.

2. Operating Principle: All of the above actions generate mechanical vibrations in the fence fabric. These vibrations are distinguishable from those caused by normal or naturally occurring environmental activity. Fence vibration sensors are either electro-mechanical or piezoelectrical transducers. The processor filters out vibration signals uncharacteristic of an intrusion. Signals characteristic of an intrusion pass through the screening filter and trigger an alarm.

3. Sensor Types:

a. Electro-Mechanical Sensors: Electro-mechanical sensors use mechanical inertia switches to detect fence vibrations. Mechanical-inertia switches consist of a vibration sensitive mass that rests on two or more electrical contacts to create a closed circuit. The mass is free to move and reacts to vibrations generated in the fence fabric during a penetration attempt. The vibrations disturb the mass, which separates from one or more of its electrical contact points, momentarily opens the circuit, and creates a signal. In some sensors, the mass is intentionally constrained or restricted by some internal guides to ensure that only a significant vibration will cause a movement, break the circuit, and generate a signal. Signal processors for electro-mechanical systems analyze one or more of the parameters related to the opening and closing of the switch: the opening event, the duration of the open event, the time between events, the length of time over which events occur, or the period of time since the last event. More sophisticated systems analyze more of those parameters to reduce the nuisance alarm rate.

b. Piezoelectric Sensors: Piezoelectric sensors convert the mechanical impact forces generated by vibrations during an intrusion attempt into electrical signals. Unlike the open/close signal generated by electro-mechanical sensors,

piezoelectric sensors generate an analog signal that varies proportionally in amplitude and frequency to the vibration activity on the fence fabric. Signal processors vary in the sophistication with which they analyze the frequency spectrum, amplitudes, durations, and other parameters of the electrical signals to discriminate between intrusions and other sources of vibrations.

4. Applications:

a. Interior: Other technologies are more appropriate for detecting intrusions into or inside of a structure.

b. Exterior: Fence vibration sensors mount directly to the fence fabric. Each sensor is connected in series along the fence with a common cable to form a single zone of protection. Some products have a maximum recommended detection zone length of up to 1,000 feet. Shorter zone lengths are sometimes installed to lower the effect of variations in the fence fabric on the probability of detection, or to be compatible with the ranges of identification of some video surveillance or monitoring systems. Vibration sensors are the most economical fence sensor and the easiest to install. The sensors have a high probability of detecting intrusion and work well when installed on properly erected and maintained fence lines. Some systems have a weather-sensing component that changes the system's sensitivity to reduce the nuisance alarm rate from weather-related vibrations. Since fence-based intrusion detection systems are all vulnerable to bridging and tunneling, other types of independent sensors, such as in-ground systems, microwave or passive infrared, or video systems should be added to enhance the overall probability of detection and to allow security personnel to assess alarms.

c. Portable: Some fence vibration systems are available in portable versions.

d. Aquatic: Fence vibration systems are not designed for prolonged periods of underwater use. Fiber optic fence vibration-sensing systems may be more appropriate for some aquatic applications.

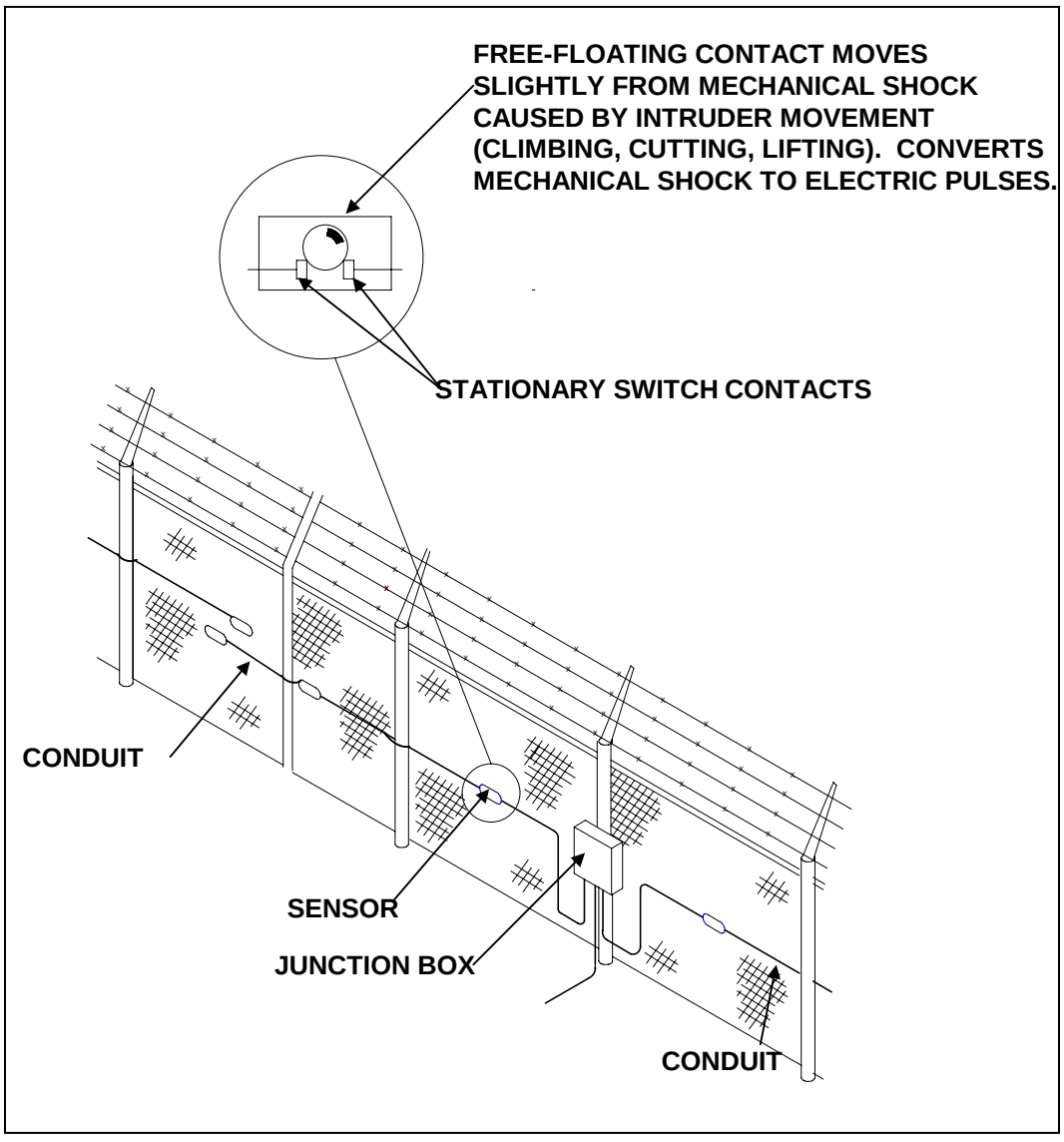
5. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Proper installation and spacing of sensors is critical for reliable detection. Poorly engineered fences with loose fabric can create enough background activity (flexing, sagging, swaying) to generate nuisance alarms. Such nuisance alarms can mask real intrusion activity or lead to operator complacency and reduced system reliability. Adverse weather conditions can also cause monitoring personnel to adjust sensitivity settings on some systems in a manner that reduces the probability of detection.

b. Causes for Nuisance Alarms: Shrubbery, tree branches, animals, and severe weather can cause the fence to vibrate and trigger a nuisance alarm. Vibration sensors should not be used in areas with high winds or numerous animal interactions with the fence line. Vibration sensors should only be used in circumstances where natural or man-made environmental vibrations are minimal. Vibration sensors are not reliable in situations where high amplitude vibrations are likely to be encountered, such as in close proximity to construction sites, railroad tracks, or highways.

c. Vulnerabilities: All fence-based intrusion detection systems are vulnerable to bridging and tunneling to bypass the sensing systems.

ELECTRO-MECHANICAL FENCE VIBRATION SENSOR



ELECTROSTATIC FIELD

E P

1. Introduction: Electrostatic field sensors generate an electrostatic field surrounding an array of wire conductors. Normally, this sensor system contains at least four solid core steel wires, two of which, called the "field wires," are used to generate the electrostatic field. The other wires are parallel to the field wires and function as sensors. The sensor wires detect changes or distortions in the field caused by the movement of a mass through the zone of detection.

2. Operating Principles: The electrostatic field system uses a field generator, which charges the field wires. The electrical charge on the field wires creates an electrostatic field in the space near the field and sensor wires. When an intruder enters the electrostatic field, the field becomes distorted and causes a change in the signal. A signal processor monitors the sensor wires for changes in signal amplitude, indicating a disturbance of the electrostatic field. The processor generates an alarm after receiving an appropriate signal from the sensor wires.

To reduce the nuisance alarm rate, a filter rejects signals caused by wind vibration and objects striking the field or sensor wires. The filter allows signals characteristic of intrusions to continue to the processor. At the processor, three conditions must be met to generate an alarm. First, the signal amplitude must exceed a preset value that discriminates for small animals. Second, the rate of signal change must be within the range that is associated with human activity. Third, the signal must persist for a set period of time. Once these conditions are met, the processor generates an alarm.

3. Applications:

a. Interior: Electrostatic field sensors are not marketed as interior security solutions.

b. Exterior: The technology is mature for exterior applications. Electrostatic field sensors follow the terrain's contours with the field and sensor wires attached to either freestanding posts or chain link fences. The wires are mounted parallel

to the ground to achieve uniform sensitivity along the length of the fence. Some configurations use springs at the attachment points to reduce the effect of wind-induced vibrations. The zone length of an electrostatic field sensor can extend up to 500 feet. The detection zone extends about three feet from the wires. The height of the detection zone in a four-wire system is approximately eight feet. Eight wire systems are available, which offer a detection zone height of sixteen feet. The electrostatic field system may also be installed along the side of a building, structure, or edge of a rooftop. Other sensors, such as passive infrared, microwave, or video motion detection, can be used to increase the probability of detection of the overall security system.

c. Portability: Portable, battery powered electrostatic field systems are commercially available.

d. Aquatic: Electrostatic field systems are not designed for underwater security applications.

4. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Adverse weather conditions such as rain, snow, or fog can interfere with the electrostatic field; however, several vendors claim that signal processing systems can compensate for such interference. Special provisions are also available to compensate for lightning. Vegetation and animal movement along the fence line can also cause nuisance alarms.

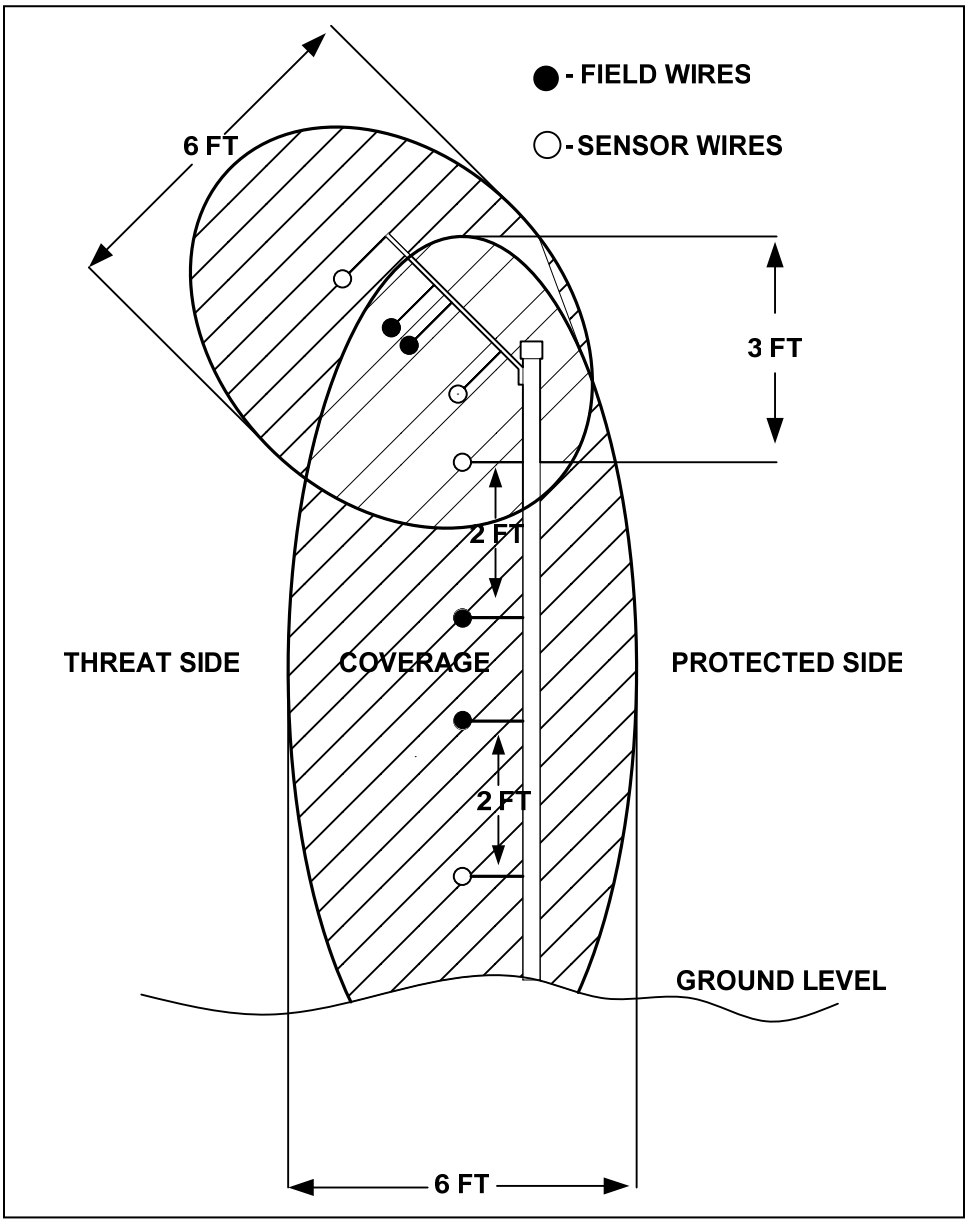
NOTE: Although electromagnetic interference (EMI) is not normally a major factor, difficulties can arise in congested areas where there are many systems nearby that emit electromagnetic energy. The recommendations of an independent security consultant should be followed to minimize the effects of this type of interference.

b. Causes for Nuisance Alarms: Excessive fence vibrations due to weather conditions, bird, or animal activity may cause nuisance alarms. Grass and

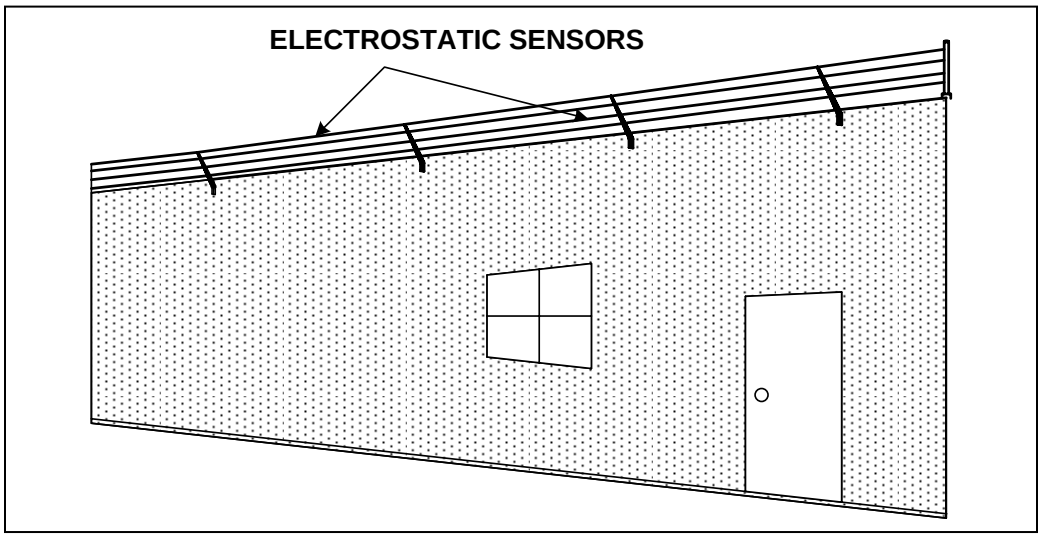
shrubbery that might attract small animals and birds should be kept clear of the fence.

c. Vulnerabilities: Although electrostatic field sensors provide some limited means of detecting underground intrusion activity because of disturbances in the field, they can be bypassed by deep tunneling (6 feet or more) or by bridging the detection zone.

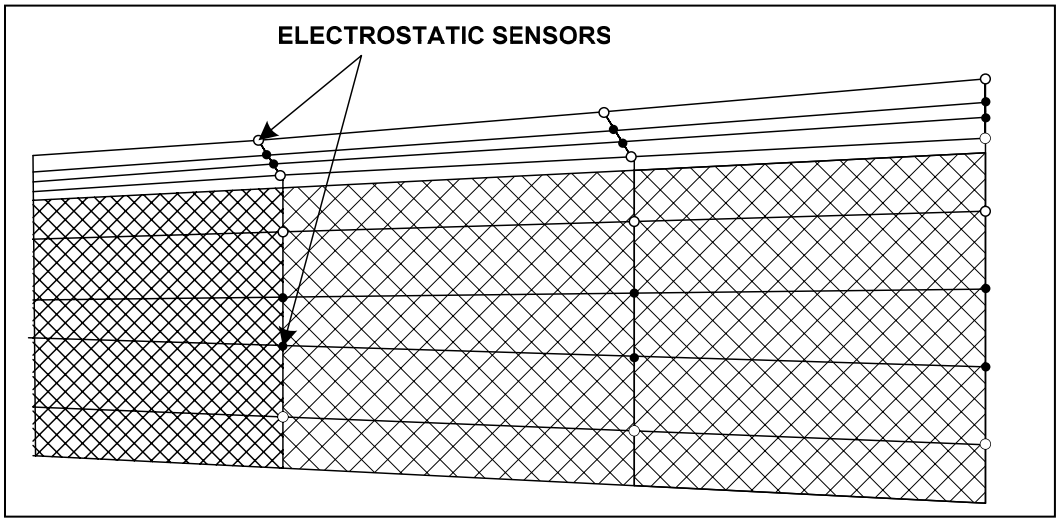
FENCE AND OUTRIGGER MOUNTED ELECTROSTATIC SENSORS



ELECTROSTATIC SENSOR BARRIER ON BUILDING



ELECTROSTATIC SENSOR BARRIER ON FENCE AND OUTRIGGER



This page intentionally left blank.

STRAIN SENSITIVE CABLE

1. Introduction: Strain sensitive cables use the electrical properties of a specially designed cable as a line sensor to detect intrusion attempts along a fence, building perimeter, coil of barbed tape, or other boundary. This type of sensor generates an electrical signal in response to any physical movement of the cable. Each cable is attached to a signal processor, which filters out signals caused by nuisance events such as wind or weather, but generates an alarm for intrusion events such as fence climbing, cutting, or lifting the fabric. Some strain sensitive cable systems have an audio listening feature that allows security personnel to assess an alarm by listening to the vibration activity on the cable. Systems with this feature may be marketed as "microphonic." Each cable uses an end of line terminator to detect tampering or attempts to cut the sensor from the system. Strain sensitive technology is a mature technology with many vendors and products in the marketplace.

2. Operating Principles: During an intrusion event, mechanical vibrations are transferred to the cable from the fence or structure. Some strain sensitive cables use a dielectric material to maintain a permanent electrostatic field or a magnetic polymer to maintain a permanent magnetic field. Inside these cables, the vibrations cause the permanent field component to flex or move with respect to the sensing conductor wires. The flexing of the dielectric material or the movement of conductors in the electrostatic or magnetic field generates small electrical currents in the sensing conductors that are monitored by the signal processor.

Another type of strain sensitive technology sends electric pulses along the sensing conductor and monitors the reflected signal. A disturbance of the cable will change the spectrum of the reflected signal that the processor will analyze using digital sampling techniques. This technology is claimed to localize a disturbance to within a few yards anywhere along the detection zone.

3. Configurations: Strain sensitive cable systems are available in two configurations: coaxial - type cable and the more complex magnetic polymer cable.

a. Coaxial Cable: Strain sensitive coaxial cable systems fall into two categories. The first category uses coaxial cable built with a permanently charged dielectric material surrounding the central sensing conductor. The dielectric material either flexes or moves with respect to the central conductor, depending on the design of the cable. In some systems, small movements of the cable flex the dielectric material and generate a current in the sensing conductor. Some other systems use cables that allow movement of the dielectric with respect to the central conductor to generate a current in the central conductor. The second category of coaxial strain sensitive cable systems continually pulses current along the central conductor and uses digital processing techniques to monitor the reflected pulses. Intrusion events alter the parameters of the reflected pulses and permit the system to localize the disturbance to within a few yards along the length of the cable.

Some products combine coaxial strain sensitive cable and barbed tape. One configuration is a coil of cable running concentrically inside the coil of barbed tape. Another uses a cable imbedded in the length of the barbed tape in a manner similar to some fiber optic products.

b. Magnetic Polymer: Strain sensitive cable systems using magnetic polymer maintain a permanent magnetic field around two or more lubricated, freely movable sensor wires arranged around a core of magnetic polymer. Various geometries of this type of cable are available from different vendors for specific enhancements or capabilities. For example, some cables use pairs of wire twisted in a specific pattern to cancel out electromagnetic interference (EMI). A movement of the sensor wire within the magnetic field produces small electrical currents that are evaluated by the signal processor.

4. Applications:

a. Interior: Interior systems are commercially available to monitor walls, ceilings, and floors against penetration attempts. The cable may be attached to frames, rafters, pipes, or other structures such as security cages.

b. Exterior: Most strain sensitive cable systems are designed for exterior use. Many fence-mounted systems are commercially available, featuring ultraviolet (UV) resistant cable jackets and cable ties. Armored jacket and conduit installations are available as well. Depending upon the height of the fence, up to three runs of cable may be required to provide adequate detection of climbing. Sensor cable lengths can extend up to 1,000 feet, but the fence construction and cable installation must meet strict specifications for reliable detection. Shorter detection zones will have greater probabilities of detection, particularly if the cable is doubled back on the same sectors of fencing. The effectiveness of the strain sensitive cable system is very sensitive to the uniform characteristics of the cable and fence. Using a second independently employed detection technology, such as microwave, active infrared, electric field, or video motion detection, will enhance the overall probability of detection and allow security personnel additional means to assess alarms.

c. Portable: Some products incorporating a strain sensitive cable and coiled barbed tape can be deployed relatively quickly.

d. Aquatic: Strain sensitive cable systems are not designed for underwater applications.

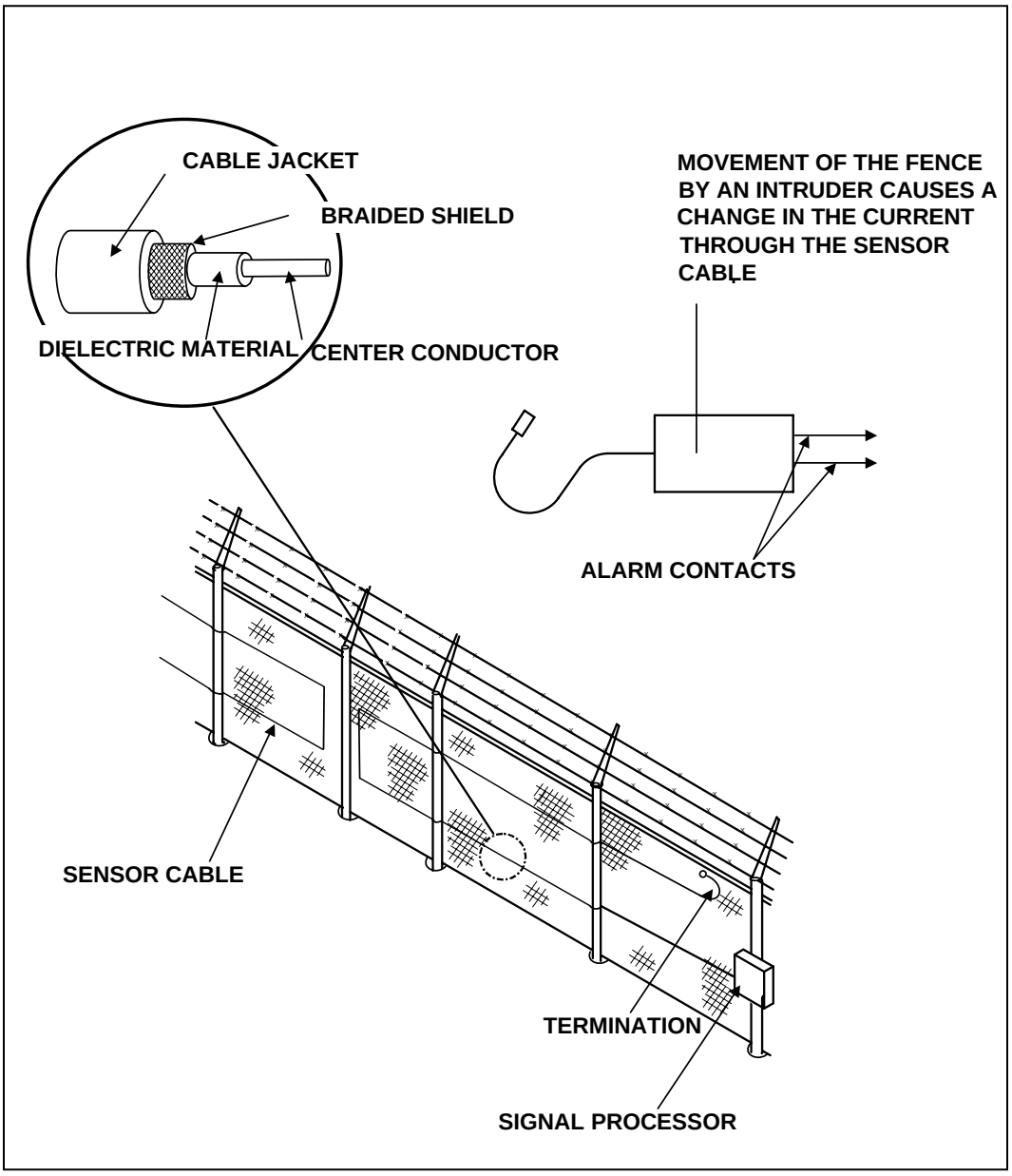
5. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Poor fence construction, improper installation, or poor maintenance will lower the probability of detection. For the cables to be uniformly sensitive along the entire length requires a high degree of care in manufacturing. Subtle variations in uniformity can cause dead zones or hot zones in portions of the cable. Improper installation can also cause variations in sensitivity.

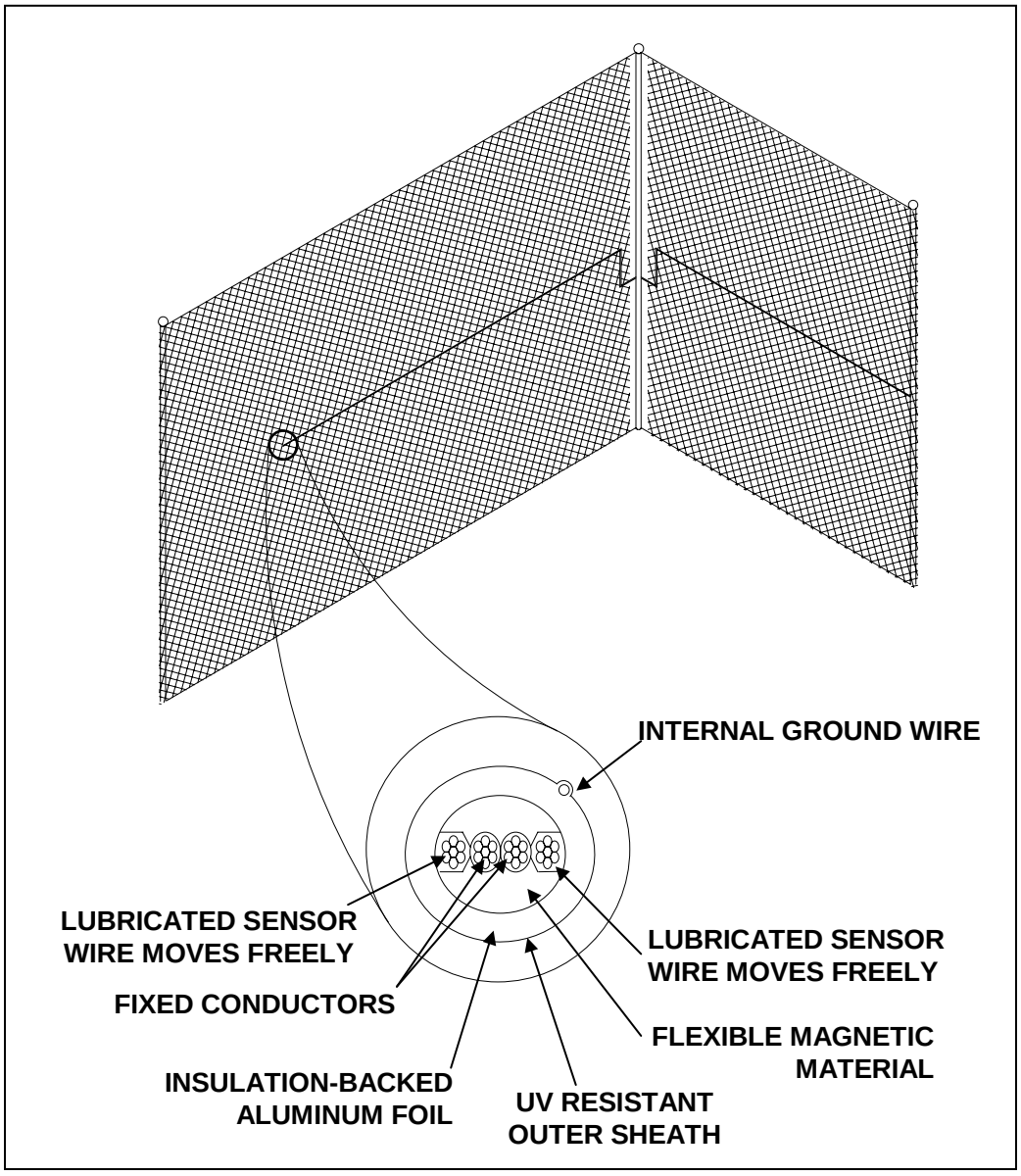
b. Causes for Nuisance Alarms: Extreme weather conditions may generate nuisance alarms; however, correctly installed, calibrated, and maintained systems are generally trouble free and provide good discrimination against minor impacts, small animal incursions, or other vibrations. Some older systems are sensitive to EMI and radio frequency interference RFI. Most current systems use a signal processing technique to reduce or eliminate sensitivity to EMI and RFI.

c. Vulnerabilities: As with other fence-based sensors, strain sensitive cable systems are vulnerable to attempts to bypass the detection system by bridging or tunneling.

STRAIN SENSITIVE CABLE (COAXIAL); SHOWING TWO RUNS



STRAIN SENSITIVE CABLE (MAGNETIC POLYMER), SHOWING ONE RUN



FIBER OPTICS

1. Introduction: Fiber optic sensor systems are among the most versatile intrusion detection systems on the market. They are available in two configurations for most applications: line cables and mesh. Fiber optic sensors use light rather than electricity for transmission and detection. Fiber optic cable is ideal for building into existing structures, such as fences and walls, attaching to those structures, or for use as stand-alone fencing. Fiber optic sensor technology is one of the few that has applications for interior security and exterior uses above ground, underground, and underwater. Barbed tape is available that is manufactured with an integrated fiber optic cable.

2. Operating Principle: The fiber component of a fiber optic cable is a hair-thin, strong strand of glass or plastic optical medium that can transmit light over many hundreds of feet from a light source to a receiver. It is often called a wave-guide, because the fiber guides light waves from a laser or LED to a detector at the opposite end of the fiber. In operation, light is pulsed through the fiber in a manner similar to electricity through a wire. Fiber optics, however, offer several advantages over electrically conductive materials. Fiber optic cable and mesh are immune to electromagnetic interference (EMI) and carry no electrical current. Fiber optic cable detection zones can be over 2,000 yards. Fiber optic mesh detection zones are limited to about 500 feet, because of greater signal attenuation. Buried fiber optic line detection systems normally use multiple passes of cable, so the zone length is highly dependent upon a site's specific requirements. Mesh is also available for in-ground applications.

3. Sensor Types and Configurations: Two processing technologies are used with fiber optic systems: continuity systems and micro bending systems. Fiber optic continuity systems require the fiber optic strand to be broken or severely damaged in order to initiate an intrusion alarm. Fiber optic micro bending systems detect minute alterations in the light pattern caused by slight movements of the fiber optic cable.

Fiber optic sensors are available as single cables and as a mesh-type net. Products are available in either configuration for almost any appropriate application. Buried fiber optic cable and mesh systems sense pressure waves and are of the micro-bending type.

Barbed steel tape is available with an imbedded fiber optic cable. Some systems using individual strands on fences appear similar to a taut wire installation. Fiber optic equipped barbed tape is available as a coil or in single strands for straight runs and can be used as a stand-alone barrier or attached to an existing fence. It can also be attached to walls and buildings. The freestanding barrier application is useful in establishing a temporary security area such as a command post for an emergency response team.

a. Fiber Optic Continuity: Continuity systems are intended to alarm only when they are cut or damaged enough to interrupt the light. As long as the fiber optic continuity sensor cable remains intact, with light passing from the transmitter to the receiver, no alarm is initiated. If the cable is broken or severely damaged, the signal reception ceases and the processor generates an alarm. Some products have the capability to sense strain in the cable and pinpoint breaks or interruptions using a signal processing technique that continuously monitors the length of the cable.

b. Fiber Optic Micro-bending: Micro-bending processors sense the minute changes in the light transmission characteristics from pressure applied to or movements of the fiber optic cable. A newer technology than continuity sensors, micro-bending systems can generate an alarm when the cable is disturbed, allowing earlier intrusion detection than a continuity-type system. Micro-bending systems are more versatile than continuity sensors and have more applications.

4. Applications:

a. Interior: Fiber optic products may be used with fenced areas inside large structures, such as warehouses; attached to the inner surfaces of enclosed spaces; or built into walls, floors, ceilings, or doors. Other intrusion detection

technologies, such as volumetric or video systems, may be used to enhance the detection probability and to allow security personnel to assess an alarm.

b. Exterior: Fiber optic fence systems are available in several configurations using runs of individual cables, mesh networks, or combinations of both. Some versions of barbed tape have fiber optic cable fabricated into the length of the tape. The barbed tape and fiber optic cable combination can be deployed in the same manner as any other barbed tape or concertina wire product.

Fiber optic sensors intended for use on fences should be mounted directly to the fence fabric. A well-engineered, stable fence is necessary for micro-bending fiber optic systems to detect intrusions reliably. Poorly tensioned, sagging fence fabric causes rattles, random noises, and excessive vibrations, each of which may mask the signals of intrusion activity or increase the nuisance alarm rate.

To enhance the potential for intrusion detection, fiber optic in-ground sensors can be installed adjacent to a protected fence. Fiber optic in-ground sensors should not be used under or in concrete or asphalt. Caution must be used when planning detection zones in the vicinity of utility poles or trees, which can generate vibrations in the ground during high winds. If a protected zone must include trees and wooded areas, an independent security specialist should be consulted to verify that the product can operate reliably under those conditions. Video motion detection cameras mounted outside or inside the protected fence area can increase the intrusion detection probability and allow security personnel to assess the intrusion zone visually. Microwave or active infrared detection systems installed along the perimeter of the fence are also good choices to enhance the system's overall detection probability.

c. Portable: Fiber optic line and mesh fencing is available for situations requiring portability and quick setup. Some systems are designed to attach to portable fencing. Barbed tape with fiber optic cable is available in rapidly deployable coils.

d. Aquatic: Fiber optic line sensors and mesh fencing are available for use underwater to detect and deter intrusions by divers, swimmers, or vehicles. Some

installations maintain the mesh permanently at a fixed location, while others allow the mesh to be lowered and raised, or pulled to one side to allow vessels to pass. Underwater barriers may not be appropriate in all situations. Currents, dredging, high silt deposition rates, and vessels transiting the area may affect the feasibility of using underwater fiber optic barriers.

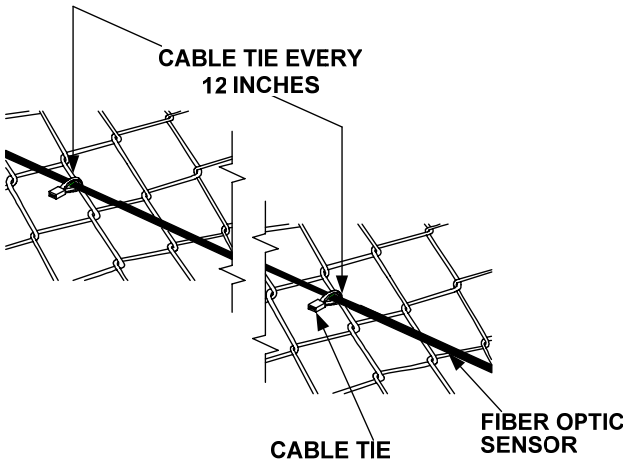
5. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Poor engineering, improper installation, and inadequate maintenance are the most common causes of unreliable detection. Loose fence fabric and poor fence post stability may require that the system's sensitivity be lowered to compensate for the ambient environment. This makes the system less likely to detect an intruder. When properly installed on a well-engineered fence or installed in a taut wire-like configuration, a fiber optic system is stable and reliable. In buried fiber optic applications, erosion can change the burial depth of the cable and reduce the probability of detection.

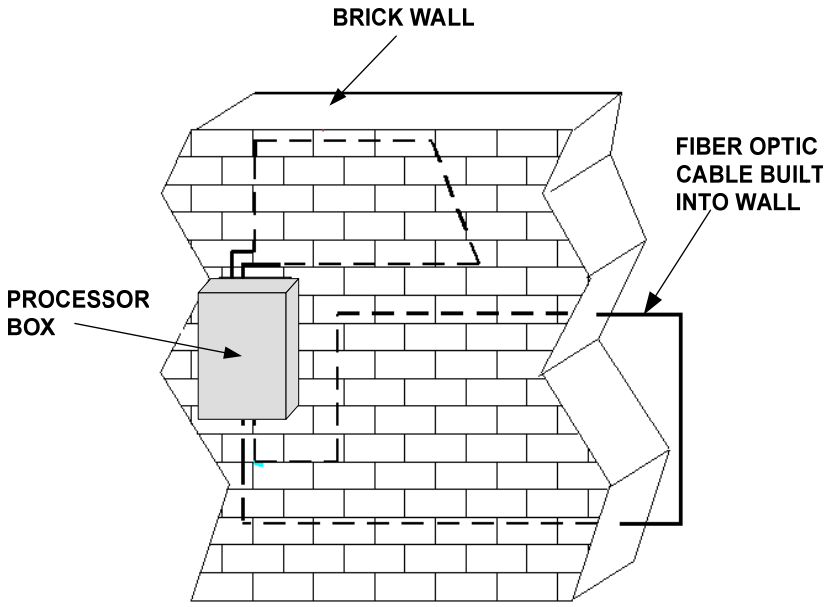
b. Causes of Nuisance Alarms: Although the alarm processor can screen out most disturbances from normal weather conditions, extreme weather turbulence that disturbs or damages the optical fiber cable can create nuisance alarms. In addition, animals coming into contact with the fence can be interpreted as human activity and generate a nuisance alarm. Vibrating machinery, aircraft, or train traffic can cause building components to vibrate and trigger nuisance alarms in fiber optic systems attached to or built into structures. Tree roots moving in windy conditions and large animals are the most common sources of nuisance alarms for buried fiber optic systems.

c. Vulnerabilities: Fiber optic systems are vulnerable to bridging and tunneling to bypass the detection zone. Using fiber optic cable with other detection technologies in an integrated system is recommended to offset these vulnerabilities.

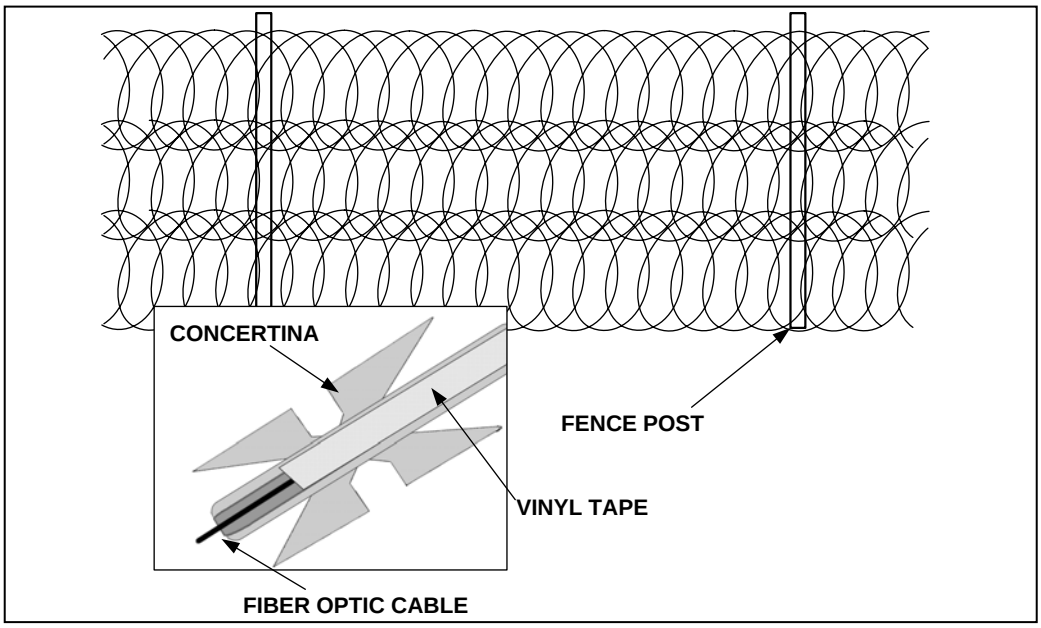
FIBER OPTIC CABLE



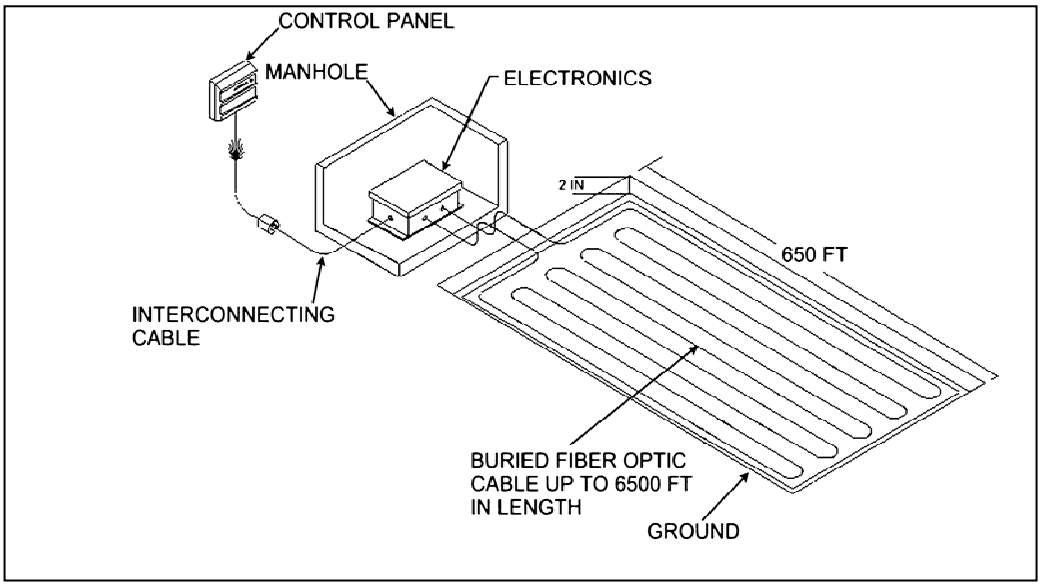
FIBER OPTIC WALL VIBRATION SENSOR



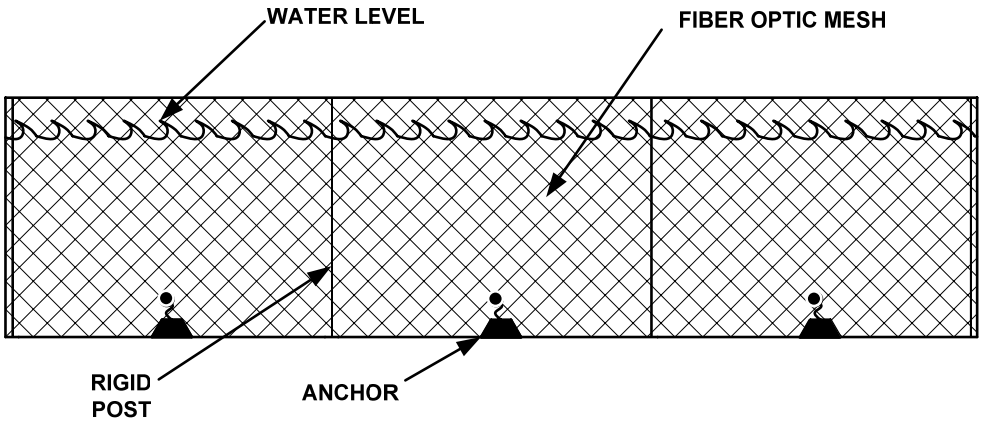
FIBER OPTIC CONCERTINA



FIBER OPTIC SENSOR



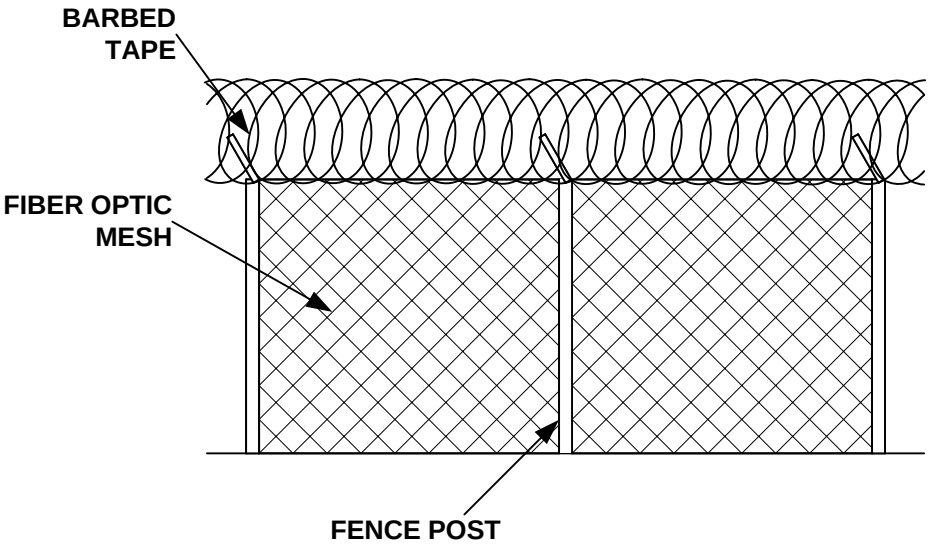
UNDERWATER FIBER OPTIC MESH FENCE



FENCE PROJECTS APPROXIMATELY 4 FEET ABOVE THE WATER SURFACE TO PREVENT SWIMMERS FROM JUMPING ACROSS.

FIBER MESH MAY ALSO BE SUPPORTED BY FLOATING BOOMS, OR BUOYS TO ALLOW FENCE TO BE OPENED FOR PASSAGE OF SHIPS.

FIBER OPTIC MESH ATTACHED TO FENCE



This page intentionally left blank.

TAUT WIRE

E P

1. Introduction: Taut wire sensor fences consist of a number of horizontal, closely spaced wires, each connected to a sensor that activates an alarm when the wire is deflected. The wires may be high tensile strength wire or high tensile strength barbed wire. Taut wire systems are designed to detect attempts to climb, spread, or cut the taut wires. A taut wire fence serves as both an intrusion detection system and as a physical barrier.

2. Operating Principle: A typical taut wire fence detection zone consists of two anchor posts, a sensor post, the taut wires, and slider posts. An anchor post at each end of the detection zone supports the taut wires. A sensor post halfway between the anchor posts contains the sensors which are connected to the taut wires. The sensors may be electro-mechanical switches, strain gauges, or piezoelectric elements. The slider posts support the taut wires and maintain wire spacing. A taut wire system may be a stand-alone fence or mounted on an existing fence. The system may be installed with or without sensored outriggers. In either case, the posts supporting the taut wire system must be designed for the loads imposed by the taut wires. A typical detection zone can extend up to 300 feet in length. Since the sensors are in the middle of the detection zone, some sensor types allow an intrusion to be localized to one half of the detection zone.

Sensors are installed in a vertical line on a fence post located in the middle of the sensor zone. The set of wires spans the full height of the fence and can be designed to include a sensored outrigger. Each strand of wire is tensioned between the anchor posts and attached to a sensor mounted on the sensor post. Attempts to climb, spread, or cut any wire will be detected by a sensor.

Signal processing varies with the type of sensor. Systems using electro-mechanical switches may have no processing; a sufficient deflection of the switch generates an alarm. Systems using strain gauge or piezoelectric sensors have more potential for signal processing, because the change in tension on a sensor will generate an electrical signal or a change in an electrical current, the parameters of which can be analyzed. The processors in some products will

examine all the sensors in a zone if activity is detected on a single sensor before generating an alarm. Systems with more sophisticated signal processing will generally have lower nuisance alarm rates than systems with minimal or no processing.

The taut wire system is not overly susceptible to wind conditions. A firm pull/force on a wire is required to cause a signal or an alarm. The deflection force varies between 15 pounds to as much as 65 pounds depending on the product and sensor settings. The materials used in taut wire systems are susceptible to expansion and contraction from temperature variations. Therefore, maintaining the tension on the wires is essential to ensure the system performs as intended.

3. Sensor Configurations: Taut wire sensors can be used on fencing and outriggers in two configurations: stand-alone or attached to an existing structure.

a. Stand-alone Fence: Taut wire fences and outriggers are rigid enough to function as barriers on their own. Stand-alone taut wire systems function as barriers and as intrusion detection systems.

b. Attached to existing structure: In situations where the taut wire systems are mounted on existing fence posts or outriggers, they are intended to detect intrusion attempts by climbing. The taut wire system is mounted on the side of the fence from which the threat is anticipated, so that an intruder (or prison escapee) must violate the taut wire system before reaching the main fence. If the taut wires are mounted only on the outriggers, it is recommended that some other type of fence sensor be used on the fence fabric to detect climbing, cutting, or raising the fabric.

4. Applications:

a. Interior: Other technologies are more suitable for detecting intrusions of interior spaces.

b. Exterior: Taut wire sensors are used most often to protect perimeter fence lines and outriggers. Outriggers or fences may also be attached to or mounted on walls to deter and detect climbing.

Taut wire systems are one of the most expensive fence sensor systems because of the careful engineering required for installation, installation labor costs, and maintenance requirements. These sensors are very reliable. They provide a high probability of detection and an extremely low nuisance alarm rate, especially from weather and small animals. Because of these features, taut wire sensors are often installed at high security facilities. At prisons, the taut wire systems would face the interior of the compound to enhance containment, rather than detect an outside intruder. Regular maintenance is required to ensure the system performs as intended.

Several other sensor systems can be used to enhance a taut wire fence system. In-ground sensors can be installed inside or outside the fence to detect attempts to bypass the fence by tunneling or bridging. Volumetric motion detection devices (microwave or active infrared) arrayed along the perimeter of the fence will increase the probability of detecting an intrusion. In addition, video motion detection cameras mounted outside or inside the protected fence area can provide another layer of detection capability and allow security personnel to assess alarms quickly and safely.

c. Portable: Most taut wire systems are not suitable for relocation or rapid deployment applications, because of the engineering requirements for an effective fence. However, a product marketed as being portable or rapidly deployable is available that uses one or more taut wires running through the centers of concertina wire coils.

d. Aquatic: Taut wire systems are not generally marketed for underwater applications.

5. Reliability Considerations:

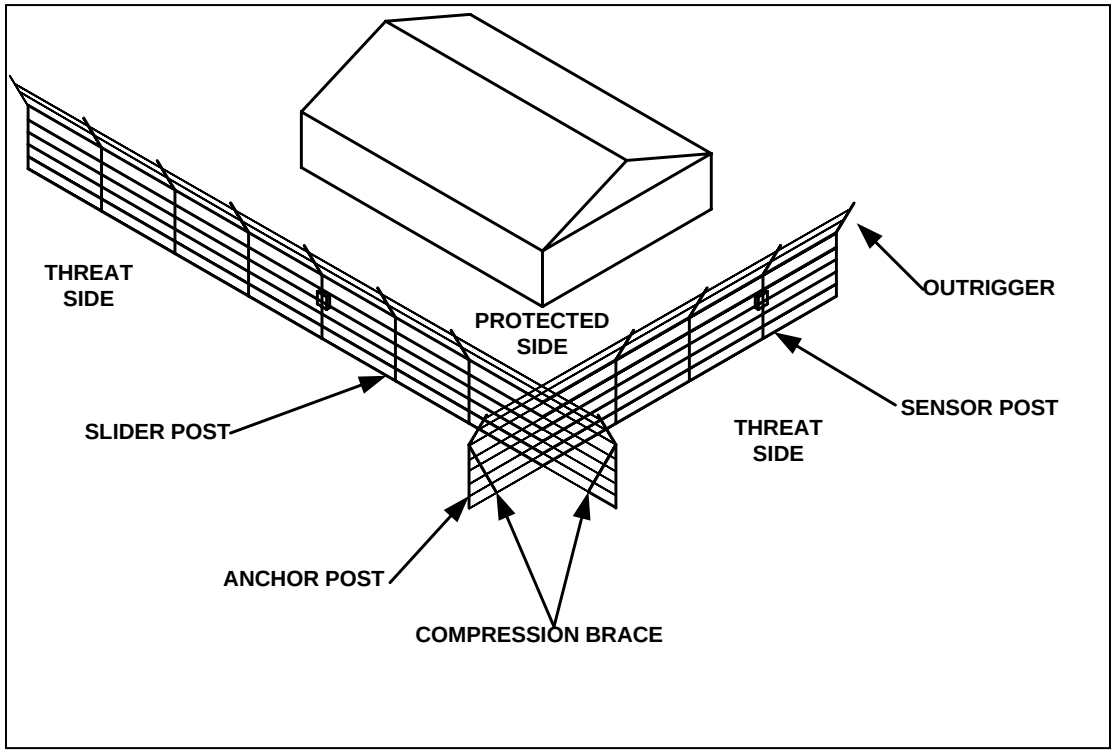
a. Conditions that Reduce Detection Probability: A correctly engineered and maintained taut wire fence has a very high probability of detection. Improper maintenance of the sensors may allow tensions to vary in such a manner that the probability of detection becomes lower or the nuisance alarm rate increases.

b. Causes of Nuisance Alarms: Medium to large animals that bump into or push against the fence while grazing or nesting may generate an alarm in some systems. Insufficient maintenance of the fence supports or wires may result in tension variations out of the specification range that result in higher nuisance alarm rates.

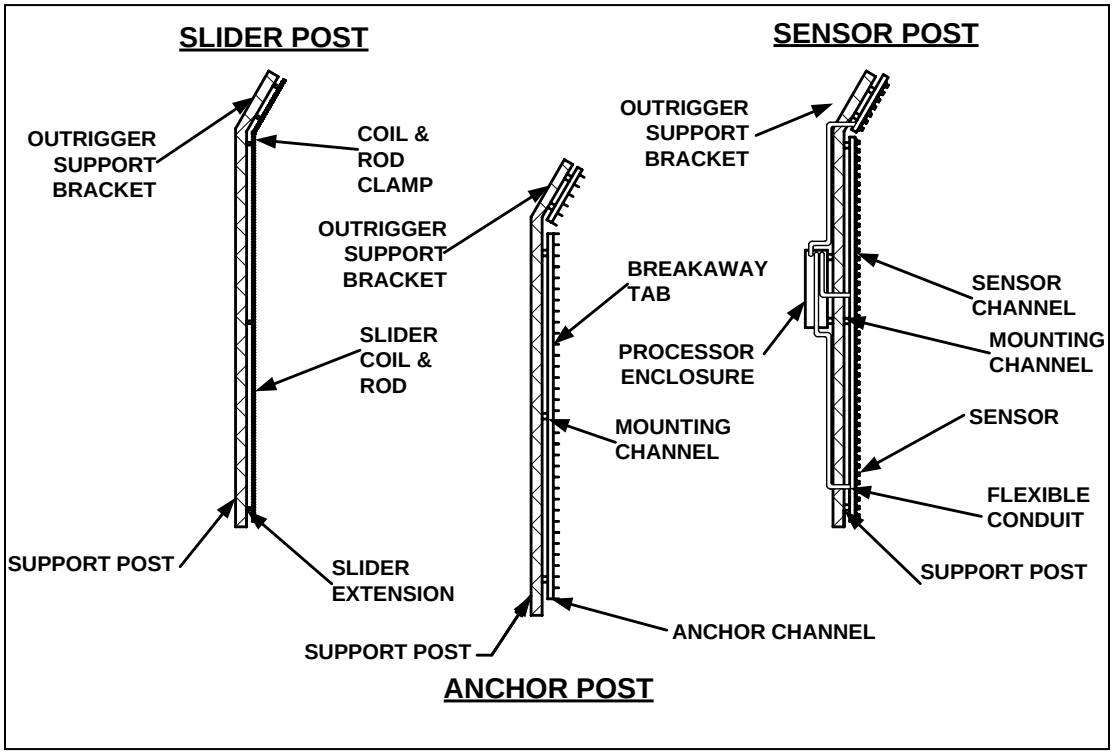
NOTE: Because of the expense of taut wire systems, they are usually installed at high security facilities where sterile areas outside the fence reduce the likelihood of unintentional contact with the fence.

c. Vulnerabilities: Intruders can avoid taut wire systems by tunneling under or bridging over the fence.

TAUT WIRE CORNER CONFIGURATION



POST CONFIGURATIONS



PORTED COAX LINE

E P

1. Introduction: Ported coax line sensors are coaxial cables that have small, closely spaced holes in the outer shield. These openings allow radio frequency (RF) energy to radiate a short distance. Emissions from these cables create a RF field, which is disturbed when an intruder enters the zone of detection.

2. Operating Principle: Ported coaxial cable systems consist of a pair of sensing cables manufactured in single or dual cable configurations. The single cable configuration is a single cable housing both sensing cables. The single cable is buried in one trench. The dual cable configuration uses individual sensing cables installed in parallel trenches approximately five feet apart. Processors emit RF energy through one conductor and receive it through the other. The electrical conductivity of the burial medium and above-ground environment will result in a signal with steady parameters that can be monitored for changes. The processing system continually monitors the signature and updates the stored parameters to account for gradual changes in the burial medium and environment. When an intrusion is attempted, the signal processor notes the changes in the signature. If the variation falls outside of preset parameters, an alarm signal is generated.

3. Sensor Types: There are two basic types of buried ported coax sensors available: (a) continuous wave sensors, and (b) pulsed sensors. Both types are available in either the single cable housing version or the dual cable version.

a. Continuous Wave: With continuous wave sensors, the RF energy is transmitted simultaneously by each cable and received by each opposite cable. The energy emission is constant and creates a detection zone above ground that is continuous along the cable runs. When an intruder enters the detection zone, the RF field is disturbed. The signal processor detects this disturbance and generates an alarm.

b. Pulsed: Pulsed sensors emit a pulse of RF energy through one cable and receive it through the other. The conductive characteristics of the burial medium and the above ground environment result in a standard amplitude signature that is

picked up by the signal processor. This signature is stored and continually updated to account for small changes in the burial medium and environment. When an intrusion is attempted, the signal processor detects the changes in the pulse signature. If the variation falls outside of allowable parameters, the processor generates an alarm.

4. Applications:

a. Interior: This technology is not well suited for interior applications because of vulnerability to EMI from interior electrical systems and conductive materials used in building construction.

b. Exterior: This technology is most often used as a buried exterior perimeter sensor. These systems are covert, terrain following, and insensitive to seismic, acoustic, or pressure changes. The cables are buried approximately nine inches below the surface of the ground. The burial depth may be adjusted based on the soil conductivity. The RF energy detection field will be three to six feet wider than the distance separating the sensor cables and extend approximately three feet above the ground level. The variation in zone size depends on the cable separation distance, the burial depth, the conductive characteristics of the burial medium, and the sensitivity setting. With this sensor cable, zone length can extend up to approximately 500 feet. The dual cable configuration offers a wider detection field, but has higher costs in materials, engineering, installation, and labor. Buried systems should be used with fences, volumetric sensors, or video systems to delay intrusions, to enhance detection probability, and to allow security personnel to assess alarms. Current processing technologies used on some systems show the location and can track the progress of an intrusion along the length of the buried coaxial sensor.

These systems are used frequently in the zone between two perimeter fences. Where there is a perimeter road, a coaxial system installed along the road may be able to detect patrolling vehicles and allow central monitoring personnel to follow the progress of patrolling personnel as well as detect an intruder.

c. Portable: Ported coaxial systems intended for burial are not portable. Portable systems are available that are designed to be installed in areas and on surfaces where burial is not possible or necessary.

d. Aquatic: This technology is not designed for use underwater.

5. Reliability Considerations: This system is vulnerable to electromagnetic interference. Metallic utility pipes or conduits should lie at least three feet below the ported coaxial cable. Routing the cables underneath chain link fences should be avoided. When installing the cables along or near fence lines, the cables must be placed between six and ten feet from the fence to reduce nuisance alarms caused by the motion of the fence fabric disrupting the detection field. Buried cable systems should be used in conjunction with other types of sensors to provide redundancy and to allow security personnel to assess alarms.

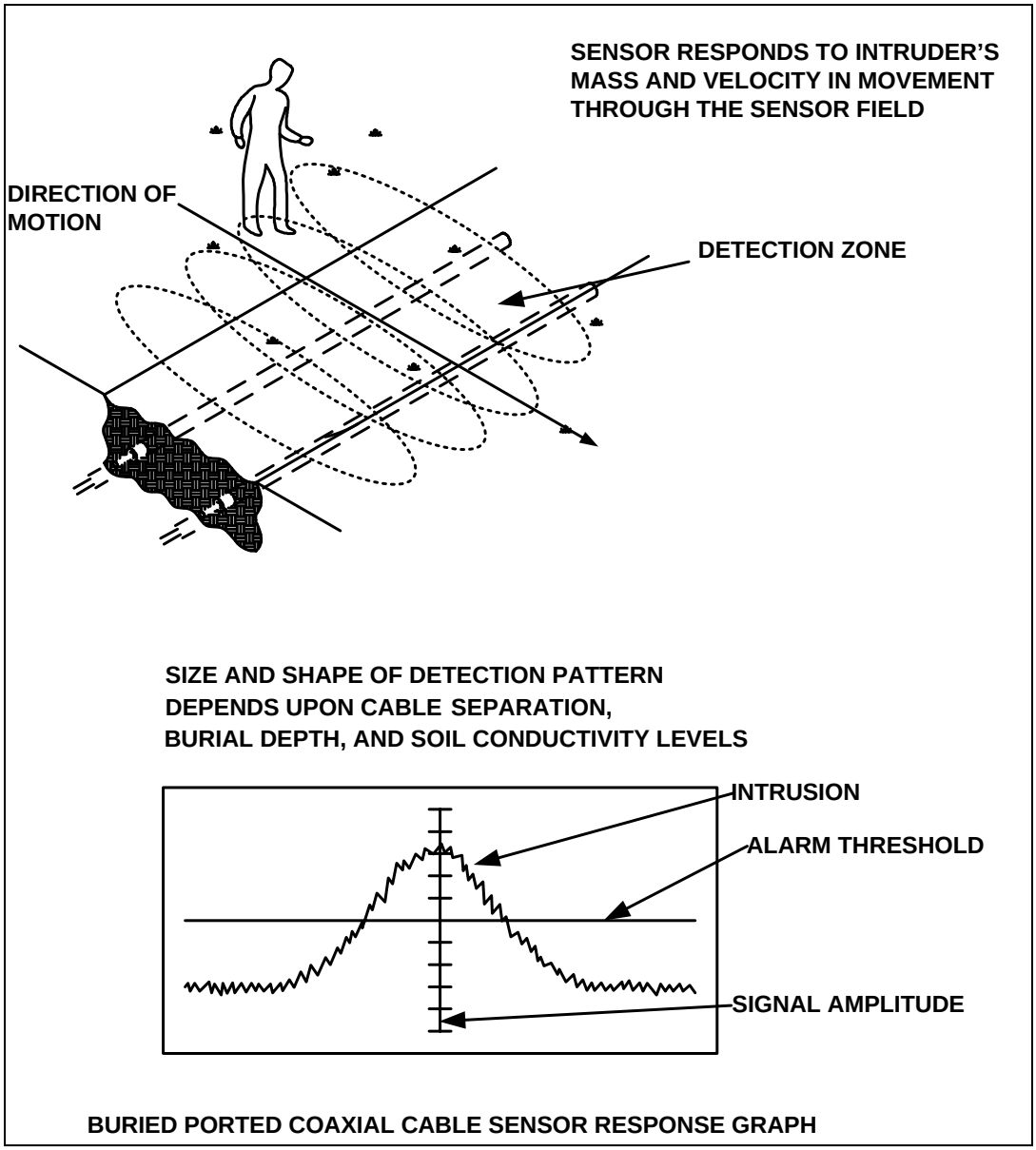
a. Conditions that Reduce Detection Probability: Because of the limited height of the detection zone, sites that experience heavy snowfall are prone to unreliable detection. Also, drainage ducts located beneath the buried cables may pose a problem. Wind disturbance of standing water over the cables can cause erroneous signals, so the burial zone should be graded to provide immediate runoff and good drainage. Nearby stationary metal objects and standing water can distort the field and create areas insensitive to detection.

NOTE: Ported coax sensors are affected by electromagnetic interference from sources such as large electrical equipment or electrical substations and should not be used in close proximity to these types of installations.

b. Causes of Nuisance Alarms: Movement of nearby metallic fence fabric, vehicles, signs, people, animals, or vegetation can cause alarms. One or two small animals typically do not affect the system; however, several small animals may generate an alarm. Keeping the sensor field clear can significantly reduce the nuisance alarm rate.

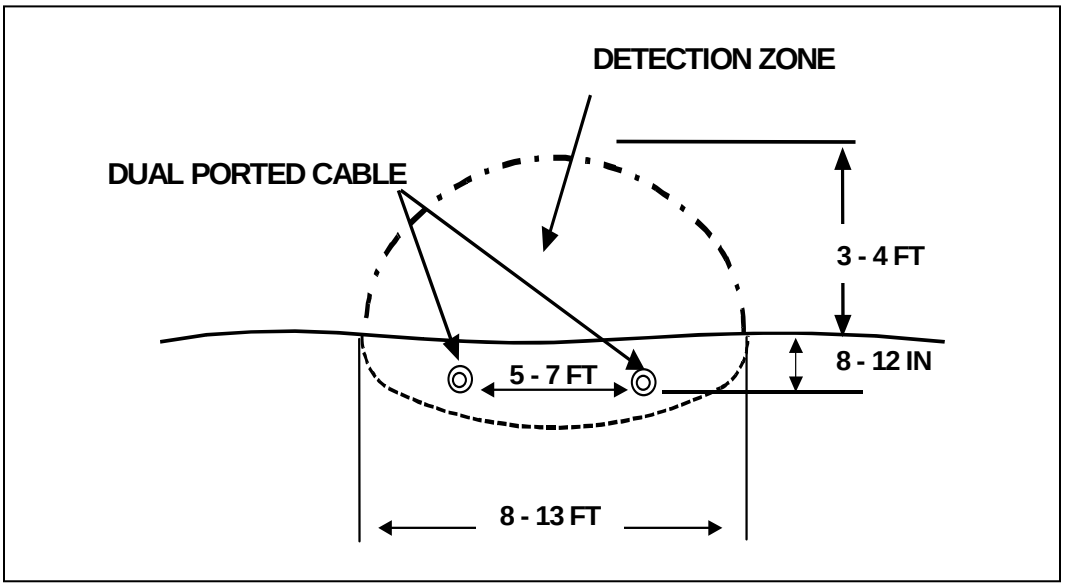
c. Vulnerabilities: An intruder who bypasses the sensor by bridging over the detection zone may avoid detection.

BURIED PORTED COAXIAL CABLE SENSOR

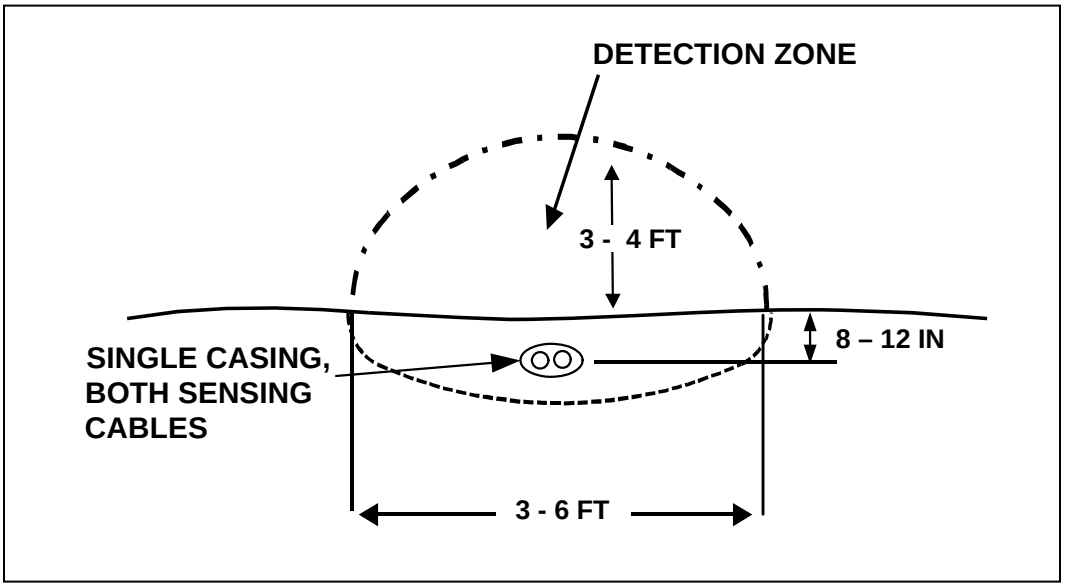


BURIED PORTED COAXIAL CABLE SENSOR RESPONSE GRAPH

DUAL CASING PORTED CABLE DETECTION PATTERN



SINGLE CASING PORTED CABLE DETECTION PATTERN



This page intentionally left blank.

BALANCED BURIED PRESSURE

E

1. Introduction: A balanced buried pressure line sensor is a passive in-ground, terrain-following system that detects low frequency pressure waves in the soil. Personnel, animal, or vehicular movements across the surface of the ground in which the sensors are installed will generate this type of energy. Pressure sensors are sensitive to lower frequency pressure waves in the sediment in contrast to seismic sensors, which react to higher frequency vibrations.

2. Operating Principle: Pressure line sensors consist of pressurized, closed end, pliable tubes or hose segments filled with water or an antifreeze-like solution. Balanced systems use two sensor tubes per zone, and the difference in pressures in the tubes is monitored continuously. The detection zone size will vary depending on soil density, composition, and the nature of any surface material. The tubes are very sensitive to changes in pressure exerted on the medium in which they are buried. A processor monitors and regulates the pressure inside the tubes and generates a signal if the pressure difference between the tubes deviates from a preset norm.

When an intruder or vehicle approaches the detection zone, the pressure waves propagating through the ground with amplitudes directly related to the intruding body's weight and impact of movement begin to reach the sensor tubes. A pressure wave will propagate concentrically from each impact point as adjacent soil particles react to the compression-decompression cycle. The impact caused by a runner will create a pressure wave of greater amplitude than a person walking, while a heavy person walking upright will create a greater pressure than a smaller person moving on hands and knees. The pressure in the buried tube sensor nearer the point of impact reacts earlier to the energy carried through the soil and changes relative to the pressure in the more distant tube. The pressure sensing unit detects the change in pressure between the tubes and transmits an electrical signal to an analyzer proportional to the difference in the pressures. When the pressure difference between the two tubes exceeds a pre-set value, the analyzer generates an alarm signal.

NOTE: A self-compensating valve is used to maintain equal pressures in the tubes, adjusting to gradual or moderate changes in the burial medium such as moisture content (rain) or temperature changes (frost or drought). However, this valve does not adjust to the rapid changes in pressure typical of personnel and vehicle movements and other man-made or sudden natural movements, such as explosions or earthquakes.

3. Applications:

a. Interior: Buried pressure sensors are not generally designed for use inside buildings or other structures.

b. Exterior: Buried pressure sensing systems are intended for exterior in-ground installation. The detection zone is created by burying the tubes approximately four feet apart, with the pressure-sensing unit linked to and placed between the sensor tubes. Depending on the nature of the soil, this type of system can create a detection zone up to 350 feet long. Multiples of the 350 foot sensor zones can provide full perimeter coverage. The depth at which the tubes are placed depends on the composition of the medium. Normally, ten inches is sufficient for soil and sand. Soil with an asphalt covering requires tubes to be placed at a depth of four to eight inches. When working with a concrete surfaced area, the sensor tubes should be buried just beneath the lower surface of the concrete. The sensitivity settings for pressure systems used under hard surfaces will be higher than would be optimal for systems under soil; therefore, systems installed under hard surfaces should be separated from systems used in soil. Buried sensors should be used in conjunction with barriers and other types of perimeter intrusion detection systems to enhance security, detection probabilities, and the ability to assess alarms.

c. Portable: Buried pressure sensing systems are not designed for portable or rapidly deployable applications.

d. Aquatic: These systems are not designed for underwater use.

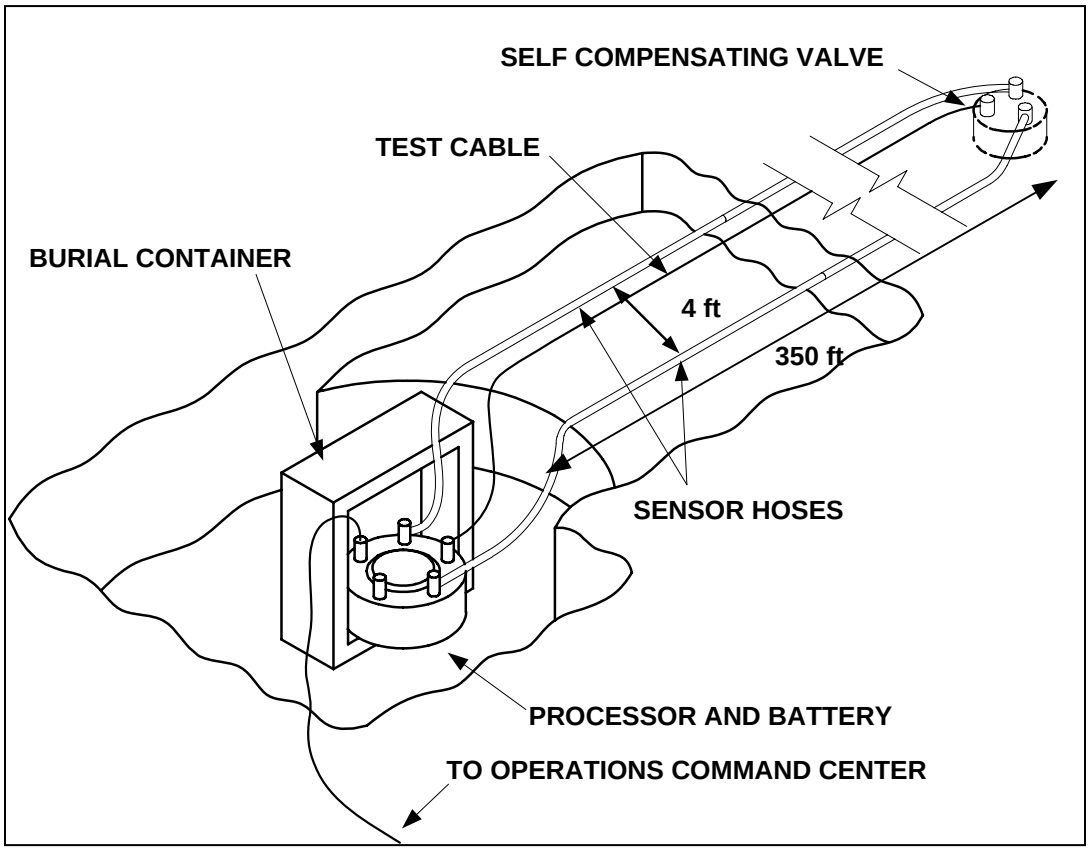
4. Reliability Considerations:

a. Conditions for Reduced Detection Probability: Because of the differential pressure principle employed and the nature of the self-compensating valve, the system has a high degree of immunity to many environmental noise and weather conditions. Sediment conditions are the most important factor influencing the sensitivity and engineering requirements of the balanced buried pressure system. Sensitivity and optimal burial depth are functions of sediment conditions that can change with weather conditions. There is a trade-off between a high detection probability with a narrow detection field at a shallow burial depth versus a lower probability with a wider field at greater depths. Installers should test pressure systems in their ambient conditions to determine the most desirable burial depth. Frozen sediment significantly lowers the pressure sensitivity of the system.

b. Causes of Nuisance Alarms: Improper installation or calibration can cause normal activity to be interpreted as an intrusion. Also, proximity to heavy road or rail traffic or seismic activity from pulsating or shock machinery can cause nuisance alarms. The primary natural cause of nuisance alarms is wind-induced movement of nearby fences, poles, or trees and their roots.

c. Vulnerabilities: Avoiding the potential zone of detection, cushioning movement vibrations, reducing impact energy, and bridging or planking over the detection zone are all measures which can lower the probability of detection.

BALANCED BURIED PRESSURE LINE SENSOR



GEOPHONE

E P

1. Introduction: Geophone systems detect the low frequency seismic energy created in the ground by human, animal, or vehicle activity in the zone of detection. They are available as separate transducers or as seismically sensitive piezoelectric coaxial cable. Separate geophones are designed to be buried, stuck into the ground, or placed on the ground. They may be monitored individually or wired together in strings. Cable sensors are designed to be buried. Geophones may have applications where the landscape cannot be changed because of environmental or legal concerns. Geophone sensors can be used as components of perimeter protection systems or placed at a distance along avenues of approach to provide early warning of potential intrusions.

2. Operating Principle: Geophone sensors detect seismic energy vibrations created by an intruder. Running, crawling, walking, and vehicular movement in the detection zone cause seismic vibrations, which travel from the intrusion site to the sensor through the ground. The detection zone radius of discrete sensors is normally about seven feet for personnel; vehicles can be detected at about 25 feet. Detection zones will vary, though, with the specific characteristics of the soil. The detection zone of a seismic cable will extend about seven feet on either side of the cable for personnel movements. Geophone sensors convert the seismic vibrations to electrical signals that are sent to a processing unit, which ignores signals not characteristic of an intrusion attempt. Some geophone systems, both cable and separate transducers, incorporate an audio listening feature that allows a security monitor to assess alarms.

One technique to reduce nuisance alarms from ambient disturbances and improve the detection probability for perimeter systems is to use two lines of geophone sensors: the detector line and the discriminator line. Piezoelectric cable can also be used in this two-line configuration. In a detector line using separate sensors, the sensors are arranged with overlapping detection zones at about 10 foot intervals. The sensors on the discriminator line are attached at about 40 foot intervals. The two lines of sensors, or two lines of cable, are installed so that their detection zones are separated and do not overlap. The processor compares the signals from the detector and discriminator lines to filter out ambient

disturbances. Normal background signals from the ambient environment are present in both lines and are ignored by the processor. An intrusion event first causes a signal in the detector line but not the discriminator line. When the characteristics of the two signals satisfy the processor's trigger criteria, an alarm is generated.

3. Configurations:

a. Buried: Buried geophone sensors are available as separate transducers or as piezoelectric coaxial cable. They can be buried in soil, asphalt, or concrete. Separate transducers may be used individually or connected into a multi-sensor network.

b. Above Ground: Above ground geophone systems are discrete units used primarily for portable or temporary security situations. Each transducer is attached to a vibration sensitive spike for insertion into the ground or to a platform for placement on the ground. The transducers may communicate with the processor by cable or wireless means.

4. Applications:

a. Interior: Geophone systems are not normally used for indoor security applications.

b. Exterior: Geophone sensors are primarily used as components of exterior perimeter security systems. Systems using separate sensors have typically 20 to 50 geophones per line. Geophone systems follow the terrain and are useful in hilly or irregular areas, where other detectors that require line of sight transmission or uncluttered detection fields have marginal utility. Buried geophones should be placed in accordance with the manufacturer's directions, usually 6 to 12 feet apart. The recommended burial depth for separate sensors and for cable systems is between 6 to 14 inches in soft to compact soil and 6 inches in asphalt. The soil of the burial field should be stable and relatively compact. If possible, the geophones should be installed between layers of sand because compact sand conducts seismic vibrations efficiently. Lines of separate

transducers can extend up to 300 feet. Piezoelectric geophone cable can extend up to 3,600 feet. Geophone systems should be complemented with fences and volumetric systems (passive infrared or microwave) or video systems. Geophone transducers may detect low flying helicopters or aircraft under some conditions and can be used to detect digging and tunneling activities.

c. Portability: Portable geophone systems consist of packages of discrete transducers with spikes or platforms connected to a central processing unit. Since seismic energy propagation varies significantly with ground characteristics, the sensing range of portable systems may be less than properly engineered buried systems. An audio listening feature is available on some of these systems.

d. Aquatic: Geophone systems are not used for underwater security applications.

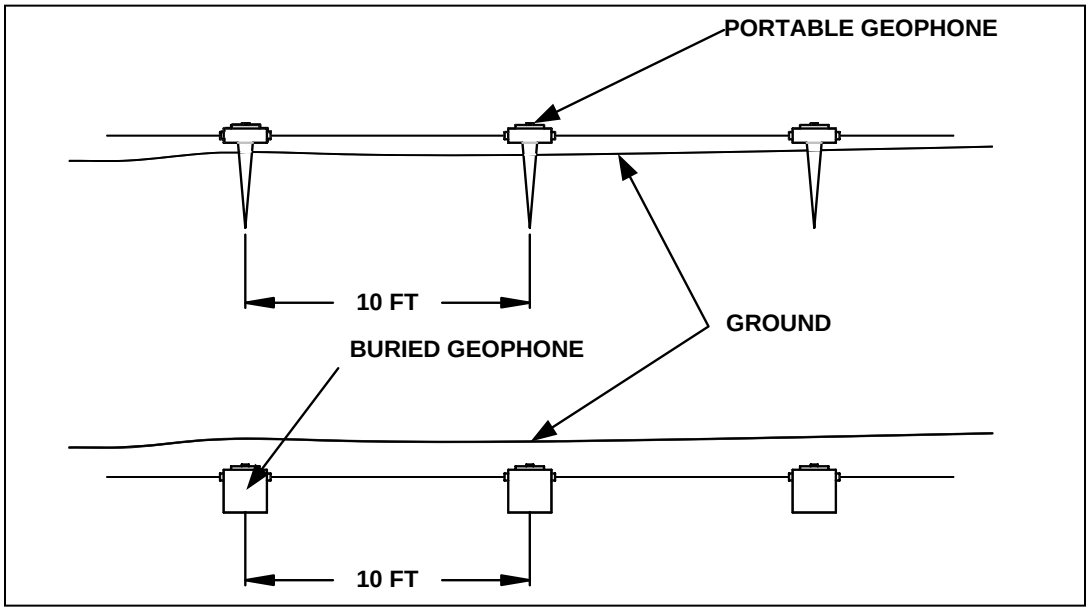
5. Reliability Considerations:

a. Conditions that Reduce Detection Probability: The main cause of unreliable detection for buried systems is improper engineering of the burial medium. Loose soil, or soil of the wrong consistency and chemistry can attenuate seismic energy before it reaches the geophones. Geophones should not be used in areas affected by high levels of seismic noise or poor seismic characteristics.

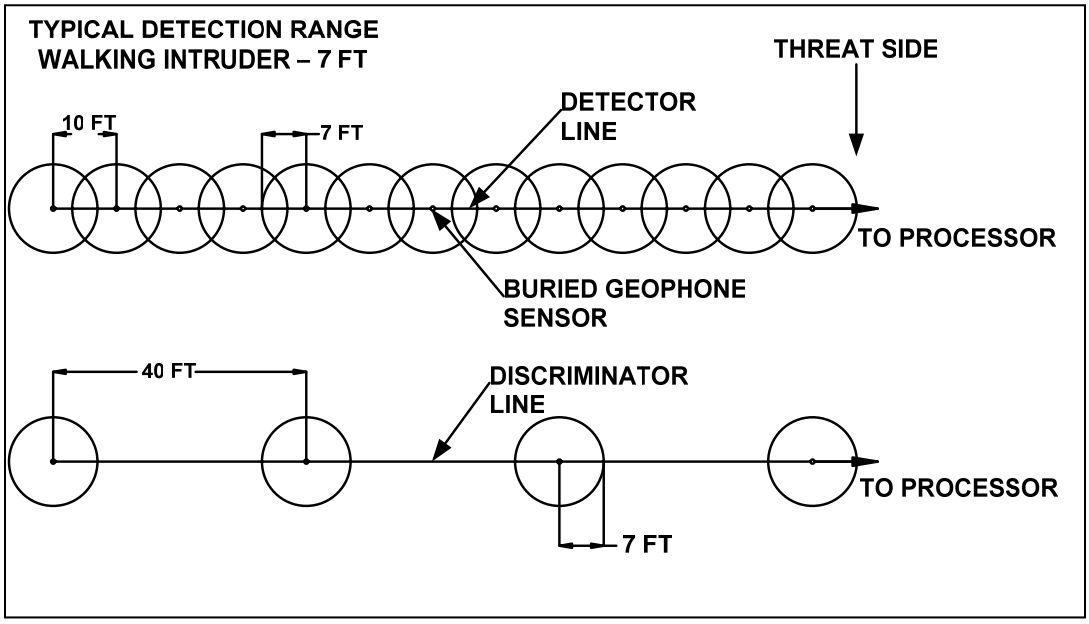
b. Causes of Nuisance Alarms: Geophones can detect very low levels of seismic activity. Trees, fences, light poles, and telephone poles generate significant seismic vibrations during high winds. Geophones should be installed at least 30 feet from trees, 10 feet from fences, and at a distance equal to the height of any utility pole in the vicinity. Following the vendor's installation instructions will reduce the nuisance alarms from these sources. Large animals passing through the detection zone may also generate an alarm signal.

c. Vulnerabilities: Bridging the detection zone will bypass the system. The use of a second technology, such as microwave, video motion detection, or passive infrared is recommended to enhance the probability of detection and to allow security personnel to assess alarms.

GEOPHONE DETECTOR GROUND APPLICATION



GEOPHONE DETECTOR AND DISCRIMINATION LINE CONFIGURATION



MAGNETIC SENSORS

1. Introduction: Magnetic sensors are passive intrusion detection devices used to detect disturbances in the Earth's magnetic field caused by movement of ferrous materials such as iron and steel, particularly vehicles or firearms. Currently, magnetic sensors are common components of military tactical perimeter security systems, commercial security products, and traffic control systems. Such systems can be sensitive enough to detect the nails used in shoes and boots, a person with a rifle at 15 feet, and a vehicle at about 50 feet.

2. Operating Principles: Magnetic sensors work on the principle of magnetic anomaly detection (MAD), which uses signal processing to detect disturbances to the Earth's magnetic field near the sensor. The magnetic field in the vicinity of a sensor will be the resultant of the Earth's magnetic field interacting with all nearby magnetically sensitive objects and any devices that generate magnetic fields. When magnetic sensors are installed sufficiently far from these man-made sources of interference, they will sense the Earth's magnetic field and react to changes in that field. For the purposes of detecting intruders, magnetic anomaly sensors detect movements of ferromagnetic objects, which will disturb the normal magnetic lines of force. Since these sensors are completely passive and do not create their own electromagnetic field, they can be used in the vicinity of facilities, such as communications sites, that would be sensitive to detection systems that generate EMI or RFI.

3. Configurations: Magnetic sensors are available in both line sensor and point sensor configurations.

a. Line Sensors: Magnetic line sensors record the pattern of the local magnetic field, which serves as a baseline for comparison during disturbances caused by an attempted intrusion. They consist of buried loops of specially constructed cable and signal processing units. The detection zone of a magnetic line sensor can be approximately 1,000 feet long and 12 feet wide. Some signal processors can support simultaneously up to three detection zones. Systems that arrange the cables in concentric loops can determine an intruder's direction of movement.

b. Point Sensors: A magnetic point sensor is a discrete unit consisting of a magnetometer encased in a durable housing with either a wireless or a cable connection to a signal processor. Some models are buried, while others have a spike that is pushed into the ground and the sensing unit remains above ground. Different models offer varying detection ranges for both personnel and vehicles. Personnel must be carrying some type of ferromagnetic material, such as weapons or personal items with iron or steel components, and are generally detected at 5 to 15 feet. Vehicles can be detected at approximately 50 feet. Magnetic point sensors detect the movement of ferromagnetic material. Stationary ferromagnetic objects will not trigger an alarm in these systems.

4. Applications:

a. Interior: Magnetic anomaly detection systems are not marketed for interior uses.

b. Exterior: Magnetic intrusion detection systems are marketed for exterior applications. Systems are commercially available with the ability to classify the vehicles used in an intrusion, as well as determine their speed and direction of travel. Such determinations are made based on measurements of the disturbances of the Earth's magnetic field and signal processing analysis, comparing the target's magnetic disturbance signature against a software library of known vehicle signatures.

c. Portable: Magnetic point sensors are highly portable and rapidly deployable. Magnetic line sensors, which are normally buried, require a higher level of installation effort. In remote situations, point sensors are often placed at a distance from the protected location along likely avenues of approach to provide early warning of an intruder's approach. The units are battery powered and may communicate with a command center using cable or wireless means.

d. Aquatic: Magnetic sensing systems for perimeter security and intrusion detection for use underwater are not commercially available.

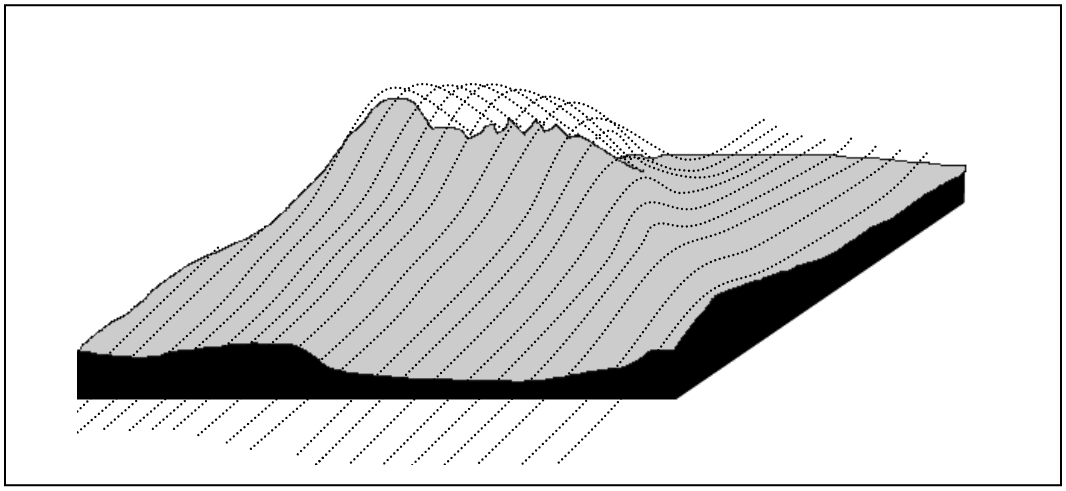
5. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Magnetic detection systems will only detect a person who is carrying or wearing some ferromagnetic material.

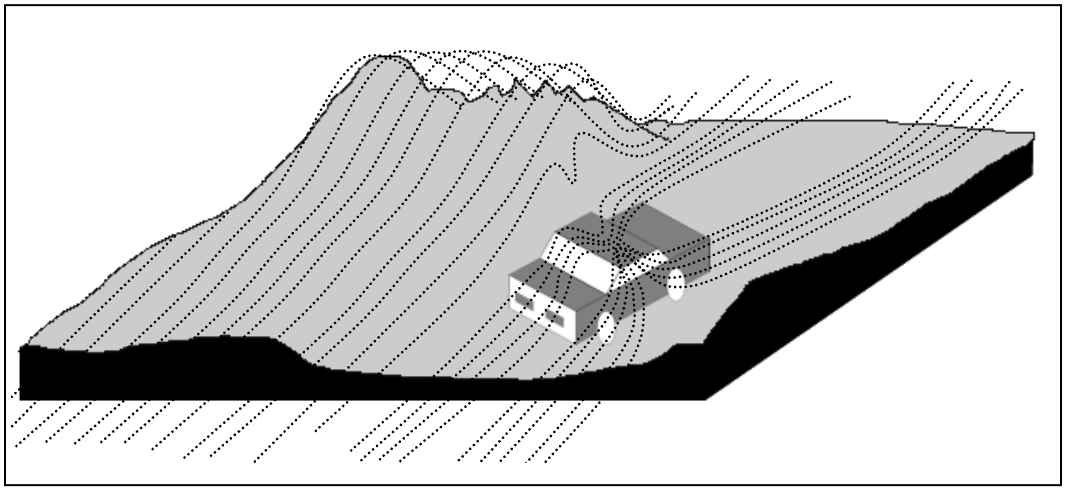
b. Causes of Nuisance Alarms: Some vendor literature admits vulnerability to electromagnetic interference. An independent security specialist should be consulted before installing a system in an area prone to the effects of electromagnetic interference, such as areas close to radio transmission towers or a satellite communication station. Environmental conditions such as lightning or magnetic storms during periods of increased sunspot activity may raise the nuisance alarm rate. Natural or man-induced vibrations transmitted through the Earth will cause minute changes in the position of the sensor with respect to the Earth's magnetic field and may cause nuisance alarms.

c. Vulnerabilities: Since magnetic systems will only detect the movement of ferromagnetic objects, it is often prudent to augment magnetic systems with other intrusion detection technologies.

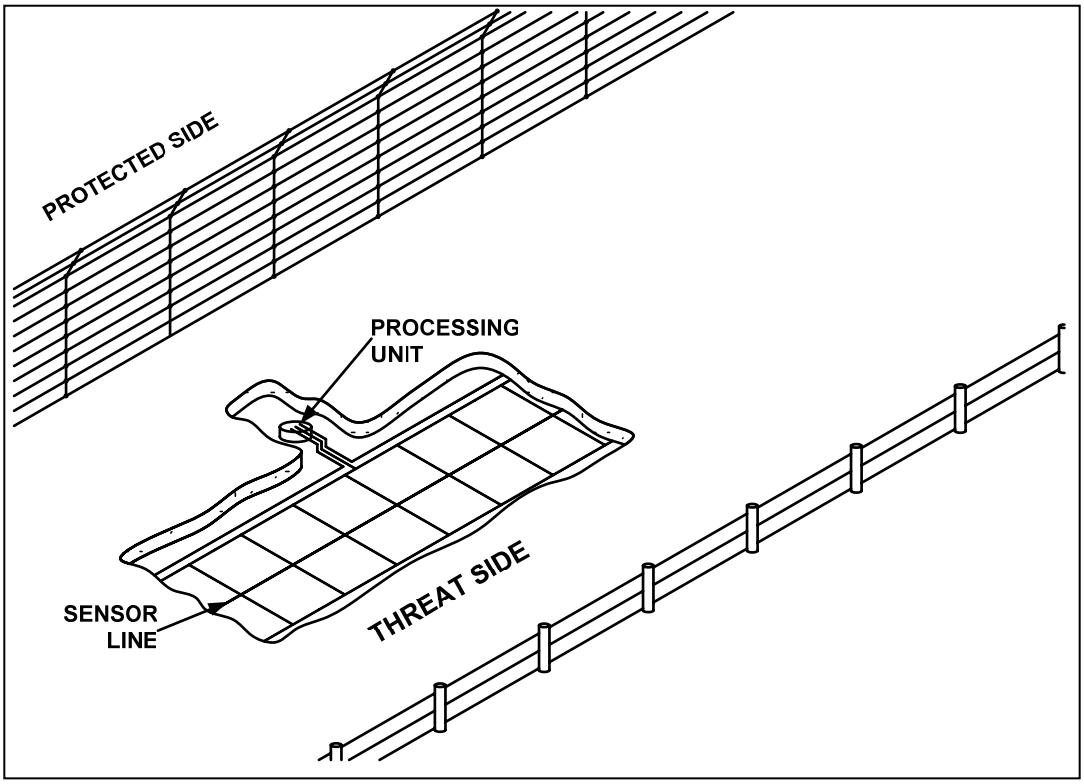
EARTH'S MAGNETIC FIELD



DISTURBANCE TO EARTH'S MAGNETIC FIELD



MAGNETIC LINE SENSOR CONFIGURATIONS



This page intentionally left blank.

VIDEO MOTION DETECTION

1. Introduction: A video motion detection (VMD) system uses software that analyzes the images captured by closed circuit television (CCTV) cameras to detect motion indicative of an intrusion or, in some cases, to detect a stationary object placed in or removed from the field of view. A personal computer or laptop can function as a monitoring station with appropriate hardware and software. Although camera selection depends on the specific security requirement, products using visible light, low light, or thermal imaging technologies are readily available and can be incorporated into video motion detection systems. Since video motion detection is a maturing technology, organizations contemplating such systems as part of an integrated security system would be prudent to test the products of several vendors against their specific requirements and situations. Video motion detection should not be confused with the use of CCTV cameras for surveillance or alarm assessment, although the same cameras can often be used for both functions.

2. Operating Principle: A video motion detection system analyses the imagery transmitted from the camera to detect changes in the field of view. When a change is detected that exceeds preset thresholds, an alarm is generated, and the intrusion scene is displayed at the monitoring station.

Many products offer enhancements or options that complement the motion detection capability. "Automated video surveillance" is a selectable mode designed to detect loitering and objects removed or left behind in situations where motion in the field of view is routine. Many products permit the detection area to be tailored to include or exclude areas within the camera's field of view. Some products can operate with pan/tilt/zoom cameras within certain limitations. A variety of methods exists to establish the criteria for an alarm. Vendors use proprietary algorithms offering different strategies to compensate for natural changes in the environment. Some products can discriminate direction of travel.

3. Applications: The capability for security personnel to have an image that correlates the source of the alarm and the assessment on the same video monitor

makes video motion detection a valuable tool for assessing alarms and determining the appropriate response. The information storage and alarm indexing capabilities of many systems provide an investigation tool that can document the intrusion event and correlate an alarm with its CCTV image.

a. Interior: Overt and covert video motion detection systems can be used in some situations where video surveillance is appropriate. The motion detection function may be turned off during periods of personnel or vehicular activity and activated to monitor areas after hours. Products with automated video surveillance capability may be appropriate in some situations.

b. Exterior: Exterior environments are more complicated than interior ones and are more challenging for some systems. Examples of exterior surveillance locations include, but are not limited to clear zones between two fences, outside storage lots, approaches to doors and other vehicle and pedestrian entry points, and loading docks. Video motion detection systems are often chosen to enhance the detection probability of an integrated security system and to improve the ability of security personnel to assess alarms.

c. Portability: Video motion detection systems using overt and covert cameras are available in portable versions using a variety of power sources. Systems are available for interior and exterior uses. Laptop computers and wireless communications allow security personnel to control these systems from almost any fixed, mobile, or remote site.

d. Aquatic: Video motion detection systems are not designed for underwater use. Systems intended for use overwater should be tested in all expected wave states and lighting conditions.

4. Reliability Considerations: Video motion detection systems may not be appropriate in some situations, even though there may be a significant role for video surveillance and assessment capabilities. These systems work better in more uniform environments. In all circumstances, care must be taken to mount the CCTV cameras securely, deny easy access to them, and keep the field of view as open and uncluttered as possible. Vegetation and obstacles to visual

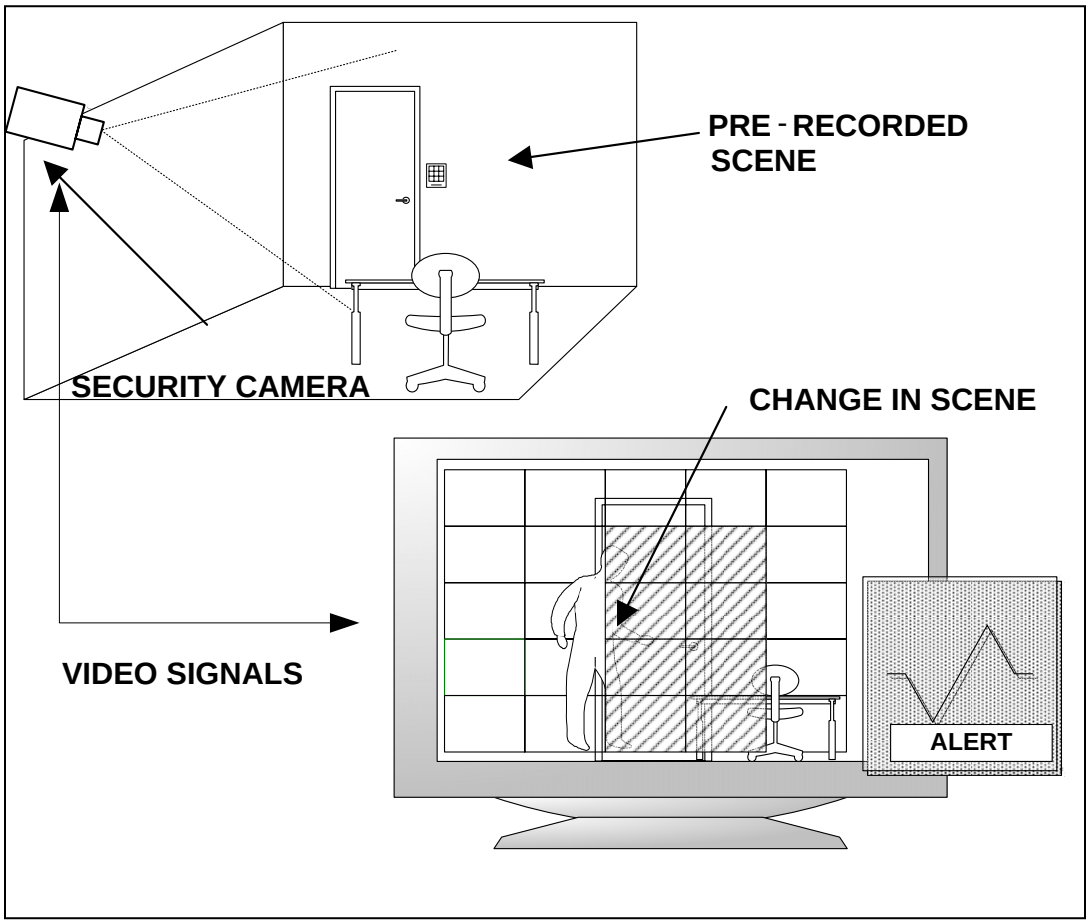
observation must be eliminated or reduced so they do not degrade the performance of the system.

a. Conditions that Reduce Detection Probability: Areas that have poor lighting or extended periods of darkness may challenge the detection capabilities of some systems. A high activity level of authorized personnel, uneven illumination, or an environment where an intruder may be expected to blend into the background present significant challenges to some video motion detection systems. Under these conditions, either thermal or low light level camera systems may be employed to mitigate the challenges.

b. Causes of Nuisance Alarms: When installing CCTV cameras for video motion detection systems, careful consideration must be given to the placement of the cameras to ensure the field of view will not be affected by natural or man-made changes in ambient light. Cloud motion, sweeps of headlights across dimly lit areas, or high contrast from shadows cast by aircraft or large vehicles may cause changes in the scene that generate nuisance alarms. Insects flying close to the lens of the camera may initiate an alarm, the system having interpreted them as larger objects moving in the field of coverage; however, a trained operator can assess this situation correctly on the monitor. Improvements in software and signal processing have reduced nuisance alarm rates and improved the ability of some systems to more finely tune the detection parameters for the specific installation.

c. Vulnerabilities: An intruder may try to avoid the field of view of an exposed, openly placed camera. It is, therefore, recommended that some cameras supporting video motion detection systems be situated as covertly as possible and networked to one or more other sensor systems. Since the “rate of change” in the scene is a variable setting on most video motion detection systems, an intruder moving at a very slow rate may not be detectable on some systems.

VIDEO MOTION DETECTION CONFIGURATION



RADAR

1. Introduction: RADAR (Radio Detection and Ranging) technology has undergone substantial development and refinement since its introduction in the early 1940s. Radar systems were first used in WWII to detect and track surface ships, aircraft, and surfaced submarines. This technology uses a directional broadcast of radio waves, which are reflected from objects within a field of surveillance. Today, many different radar systems are commercially available for a wide variety of purposes including perimeter surveillance and security.

2. Operating Principle: Radar systems transmit a radio signal in the microwave frequency range of 100 MHz to approximately 40 GHz. A portion of this signal is reflected back from targets and physical features in the field of surveillance: geographic features, structures, vehicles, and living organisms. A processor analyzes the returned signals and reports the distance, speed, and direction of travel of targets to the system operator. The size of the target can sometimes be inferred from the strength of the returned signal. This information can be displayed as part of an integrated security system report. Advances in processing and integrated display technologies allow security specialists rather than highly trained radar technicians to operate some newer systems.

The term “radar cross-section” is a measure of how well an object reflects the transmitted signal. Most ground vehicles, ships, boats, aircraft, and metal structures have relatively large radar cross-sections. The cross-section presented by an automobile is several square yards. Individuals or large animals reflect much less of the signal, and have smaller radar cross-sections. A person crawling presents less than half the radar cross-section of an upright person walking or running. The radar cross-section of a personal watercraft with a rider is about one-half square yard. A surface swimmer, carrying a breathing apparatus and a payload, presents a radar cross-section of less than one square foot.

Radar systems designed for perimeter security and intrusion detection use higher scan rates and frequencies and have shorter ranges than some other surveillance radar systems. These characteristics are necessary to detect targets with small

cross-sections and separate them from the background clutter. Several of them are designed to be operated at heights close to ground level and are known as "ground-based" personnel detection radars. They are line-of-sight systems with ranges that vary from 300 yards to approximately 25 miles. Radars designed to detect personnel emit at frequencies up to 40 GHz. Some systems designed for personnel detection claim to be able to detect an upright moving person at a range of about 6 miles and large vehicles at about 25 miles. The effective detection range of a particular type of target will vary with its radar cross-section: the detection range for a crawling intruder will be significantly less than for an upright intruder.

3. Applications:

a. Interior: In some situations radars can be used to monitor large interior open areas, such as a stadium, empty warehouse, or aircraft hangar. However, volumetric sensors such as passive infrared or microwave sensors are more commonly used in confined spaces.

b. Exterior: Radars are used primarily to monitor exterior areas and consist of either a rotating electro-mechanical assembly or electronic components with a fixed field of surveillance mounted in a weatherproof housing. Radars may be mounted on almost any stable support, such as a building, fence post, tower, tripod, vehicle, aircraft, or vessel. They can be connected to a computer control system using cable or wireless technology. Some radar systems are designed to detect large moving objects such as vehicles, aircraft, or boats, while others are designed to detect intruding personnel or small, fast moving objects. Radar systems can also be used to detect aircraft or helicopter-borne intrusion attempts, which can bypass most ground-oriented perimeter sensors.

c. Portable: A wide variety of portable radar systems are available. Portable systems range in size and weight from man-portable units weighing less than 50 pounds to vehicle mounted systems. Systems are available in either cable-connected or wireless configurations and can be powered using generators, batteries, or solar energy. Some portable radars are intended to detect large objects, while others are designed to detect personnel. Compact, self-powered

portable systems may be used along likely avenues of approach to the protected zone to provide early warning of a potential intrusion.

d. Aquatic: There are many models of surface search radars used to monitor waterborne traffic. Radar energy does not penetrate the water surface; in fact, water is an efficient reflector of radar energy. Radars designed to detect surface swimmers or personal watercraft incursions use a variety of mechanical and electronic enhancements to compensate for the very small radar cross-sections of those small targets. Additionally, the difference in the rate of movement of these two target types, from the very slow swimmer to the relatively fast movement of personal watercraft requires enhanced signal processing. Very small, slowly moving targets are difficult to track when waves are high enough to block the radar emissions.

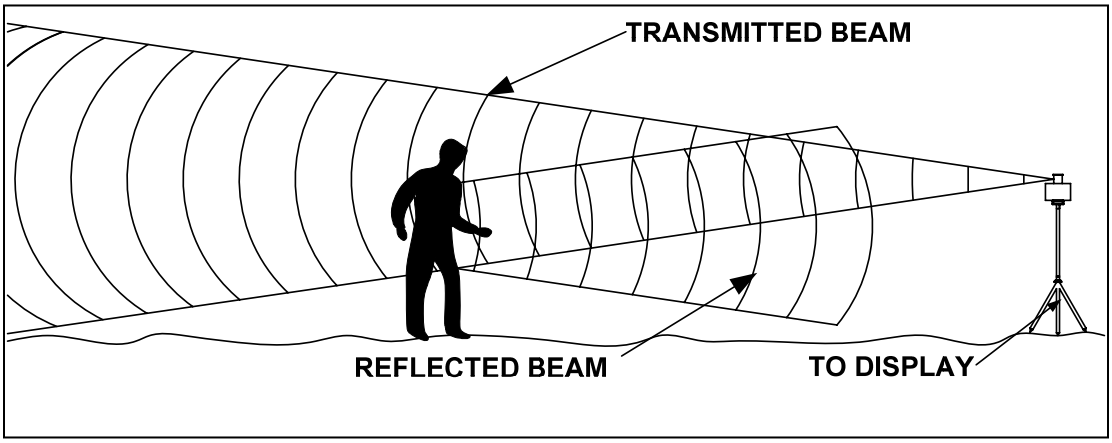
4. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Radars designed for perimeter security and intrusion detection are line-of-sight devices. Any object that reflects radar energy will have a shadow that may be exploited during an intrusion. In both interior and exterior applications, the ground should be reasonably level and the perimeter boundaries straight. If necessary, the radar unit may be elevated to provide a better field of surveillance. Large objects, buildings, hills, or depressions create radar shadows that intruders can use to avoid detection. Extreme weather conditions, such as rain or snowstorms, can also decrease the detection potential of some systems. Steady rain can reduce normal detection ranges, and heavy rains can produce excessive clutter that degrades detection performance and can produce nuisance alarms.

b. Causes of Nuisance Alarms: Objects moving outside the protected area or random reflections of radar energy may generate nuisance alarms. Enclosed spaces with walls that reflect radar energy can produce multipath signal returns that may be processed and displayed as phantom targets. Some personnel search radars may generate nuisance alarms when overgrown vegetation in the detection zone moves with the wind. Wave activity can generate nuisance alarms on some surface search and swimmer detection radars under some conditions.

c. Vulnerabilities: Uneven terrain and other obstructions may create enough radar shadows to create a pathway of approach, allowing an intruder to avoid detection by using a low/slow approach technique through the protected volume. A wide-area surveillance radar can become a single point of failure for an expansive section of perimeter. Using a companion technology, such as video motion detection, infrared, or buried fiber optic cable is highly recommended to enhance detection probabilities and allow security personnel to assess an alarm more effectively. Other intrusion detection systems can also be used to protect the radar itself and to detect movement in the dead zone very close to the radar. The width of the dead zone will vary with the radar's height and radar beam geometry.

INTRUSION DETECTION RADAR



This page intentionally left blank.

SONAR

P A

1. Introduction: Sonar (Sound Navigation and Ranging) systems are available for use in both deep and shallow water applications, and can utilize both passive and active technologies. The sensors and signal processing in sonar systems have undergone substantial refinement since the first passive systems were developed during the First World War. Passive sonar systems use a transducer to listen for acoustic energy emitted into the water by a surface, air, or underwater sound source. Active sonar projects acoustic energy into the water and then listens for the acoustic energy reflected from objects in the water. Developments in digital processing, miniaturization, and communications technologies have resulted in the availability of sonar systems designed for use in shallow water. Coastal industrial areas, port facilities, harbors, waterways, and reservoirs are some sites where incorporating sonar into a perimeter surveillance and intrusion detection program may be feasible. A thorough feasibility study should be conducted for each site before a decision is taken to incorporate a sonar system into a perimeter control and intrusion detection program. Sonar systems are costly to design, install, and maintain. They often require highly trained personnel for maintenance and operation.

There are three categories of sonars appropriate for surveillance and intrusion detection. General surveillance sonars are used to monitor traffic on and under water, but are unlikely to detect small targets such as divers. Sonars designed to detect divers, swimmers, and swimmer delivery/assistance vehicles are active multibeam systems that use electronic scanning techniques to generate narrow angle, short acoustic pulse beams in the 60 - 100 KHz range. Sonars designed to examine underwater surfaces from a few yards use frequencies of several hundred KHz into the MHz range and are capable of discriminating small objects and structural features in turbid water.

2. Operating Principle: The predominant type of sonar used in physical security systems combines the acoustic receiver and transmitter in a single housing. Perimeter security sonars operate in both active and passive modes. In the passive mode underwater sonar receivers “listen” to acoustic energy

(frequencies in the kilohertz range) created by divers, vessels, sea animals, surface waves, and low flying helicopters or aircraft. In the active mode, an underwater transmitter projects acoustic energy into the water and a receiver listens for reflections.

Active systems monitor a detection zone in one of two ways. Some systems emit individual non-directional pulses of acoustic energy that cover the entire detection zone. These systems have some applicability to general surveillance requirements, but are not useful for diver detection applications. Multibeam systems generate a large number of narrow, shaped beams to cover a detection zone. A signal processor then analyzes the reflected sound waves to determine the quantity of reflected acoustic energy (known as "target strength"), distance, speed, and direction of travel. The signal processor forwards information to the monitoring station for an operator to interpret. Advances in processing and integrated display technologies allow security specialists rather than sonar technicians to operate some newer systems.

3. Applications:

a. Interior: Sonar is not used for land-based applications.

b. Exterior: Sonar is used only in underwater applications.

c. Portable: Portable sonar systems are available from several vendors. These sonars vary from single sonar heads to multiple unit networks. Some systems utilize a transducer placed on the bottom of the protected area, while others allow the transducer to be raised and lowered from a fixed location or a watercraft. Diver portable systems are commercially available, as well as systems capable of being mounted on small boats and underwater remote controlled vehicles. Diver portable and remote vehicle systems are particularly useful for scanning piers, vessel hulls, and other underwater structures. They use much higher frequencies than surveillance sonars and have a shorter range. Some of these products can produce nearly video quality images that allow divers to examine underwater surfaces with high confidence, even in turbid waters.

d. Aquatic: Sonar systems may be used for detection and surveillance in both deep and shallow water applications. Sonar systems can vary from single transducers to networks with many transducers. Shallow water applications include the protection of harbors and ports, waterside industrial areas, fresh water lakes, dams, reservoirs, hull scanning, and coastal defense programs. The utility of sonar in shallow waters can vary considerably, especially in tidal areas where the sound velocity profile of the water changes continually. Physical security applications in deep water include ship and oil rig protection. Sonar systems should be backed up with radar and video systems to improve the ability to detect and assess potential intrusions at or near the water surface.

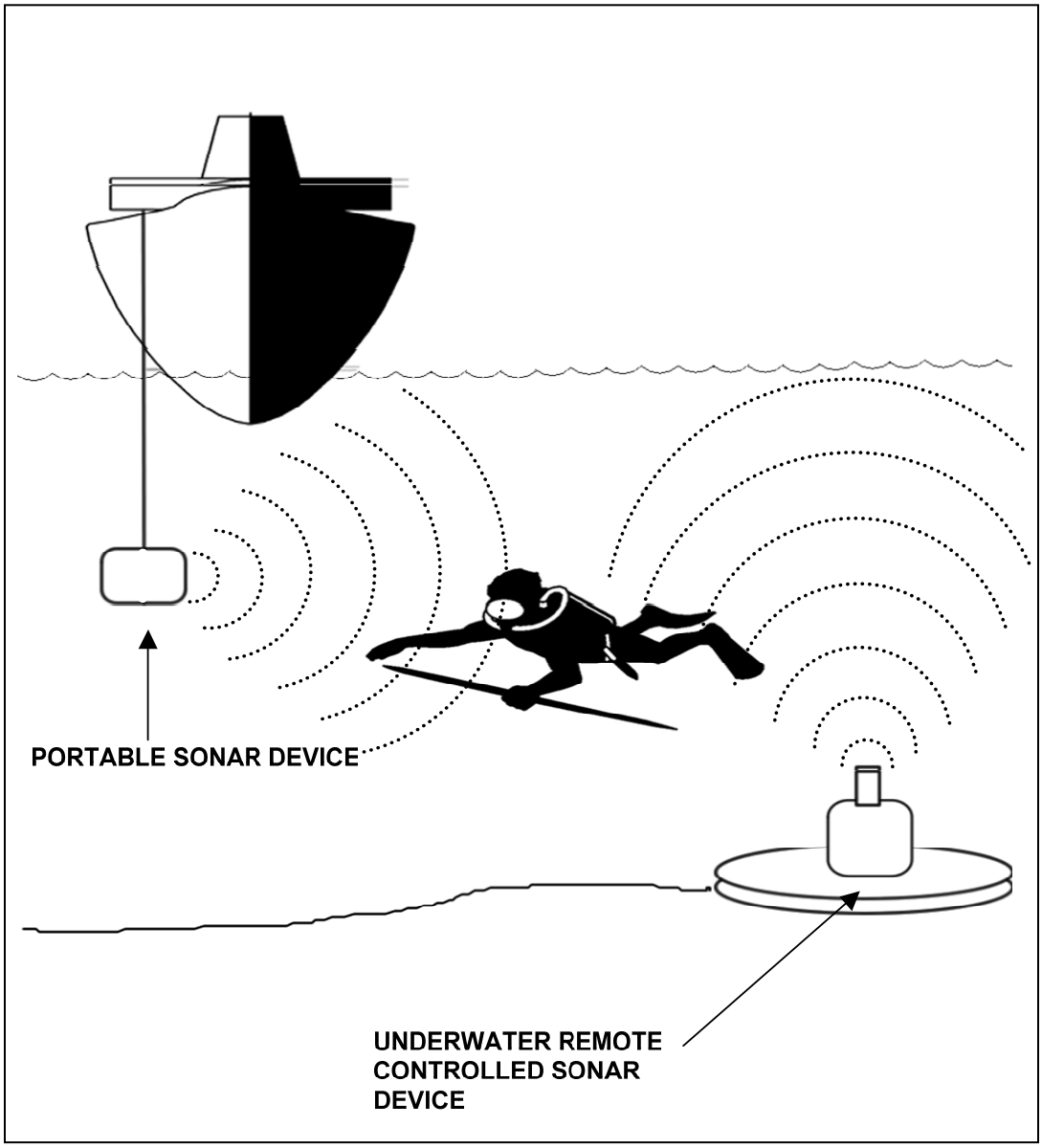
4. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Bottom topography, large construction features, and large vessels can create dead zones or shadows that divers can use to avoid detection. The quantity and variety of background noise in the waters of a port complicates signal processing and the discrimination of intruders. The salinity, temperature, turbidity, and other water quality parameters, as well as the geologic features of the bottom can all affect the propagation of sound in the water and reduce the performance of sonar detection systems. Variations in salinity and temperature can prevent acoustic energy at some depths from reaching a transducer altogether.

a. Causes of Nuisance Alarms: Nuisance alarms can be generated by acoustic energy from man-made, marine, or environmental sources.

c. Typical Defeat Measures: Bottom topography, large construction features, bridge abutments, vessels, or other obstructions in the water create dead zones and can cause spurious reflections that can mask the presence of an intruder. Knowledge of the sound-velocity profile of the water column and the depth of the sonar heads may allow an intruder to avoid detection. A supporting sensor technology, such as a fiber optic barrier, could be employed with a sonar detection system to improve the probability of detecting an intruder.

SONAR


PORTABLE SONAR DEVICE
UNDERWATER REMOTE CONTROLLED SONAR DEVICE

LIDAR

1. Introduction: LIDAR is an acronym for Light Detection and Ranging. LIDAR systems use a laser to reflect a beam of light from a target. LIDAR systems are used to detect ground-level intrusions by personnel and vehicles at relatively short ranges; they are not designed to detect air intrusions. The reflected beam is used to identify a target's presence, range, bearing, speed, and direction of motion. Perimeter security systems using LIDAR technology are available in deployable configurations and can interface easily with other detection technologies, such as video motion detection.

2. Operating Principles: LIDAR systems use one or two eye safe laser range finders mounted on a rotating arm that sweeps a circle with a radius of up to 150 meters. The sweep frequency is about one revolution per minute. The results of each sweep are used to build up a digital map of the monitored area, which is then compared to previous sweeps. Small or slow changes, such as from windblown debris, update the digital map. Larger changes, such as the presence of a human-sized shape, trigger an alarm.

3. Applications:

a. Interior: LIDAR systems can be used indoors; however, more cost effective alternatives are available.

b. Exterior: LIDAR systems are used primarily in exterior security applications, to provide coverage for protected areas, approaches, and high value assets that must remain outdoors. LIDAR sensors consist of an electro-optical assembly mounted in a weatherproof enclosure, which may be mounted permanently on a building, fence pole, tower, or mounted temporarily on a tripod or parked vehicle. LIDAR systems interface through RS485 communication ports to a computer control system. The RS485 standard specifies a maximum cable length of 4,000 feet, but it also includes a wireless technology option. LIDAR should be used in conjunction with video surveillance or a volumetric intrusion detection system to enhance detection probabilities and allow security personnel to assess alarms.

Several LIDARs can be networked to provide overlapping coverage of complete perimeters.

c. Portable: LIDAR systems are available in portable configurations for rapid deployment and can be mounted on tripods, vehicles, or other suitable bases. LIDAR systems are marketed in wired or wireless communications configurations with a variety of power options.

d. Aquatic: An independent security specialist should be consulted on the feasibility of using LIDAR for overwater applications.

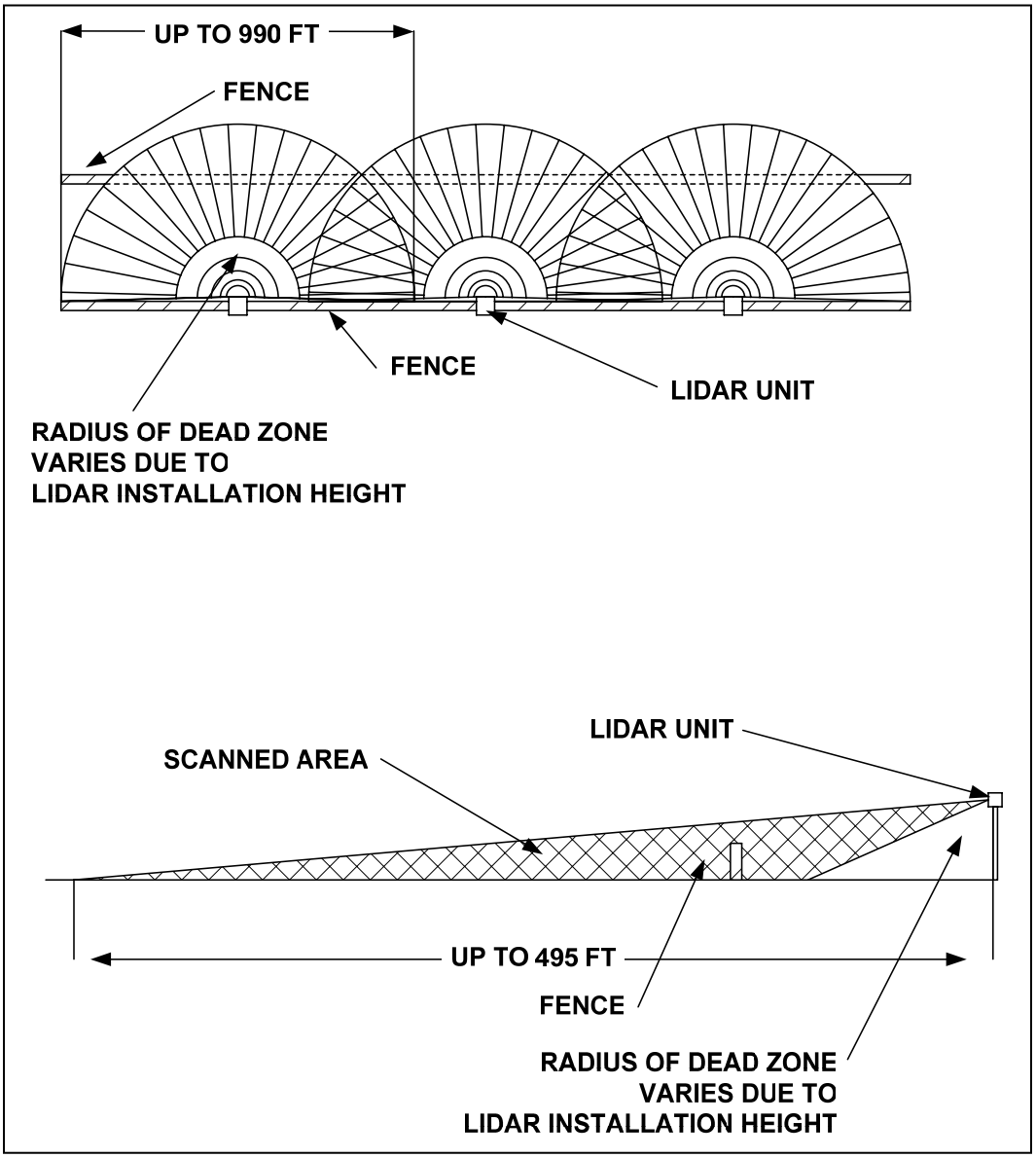
4. Reliability Considerations:

a. Conditions that Reduce Detection Probability: Extreme weather conditions can cause unreliable detection. Failure to mount the sensor in accordance with the manufacturer's directions can result in reduced sensitivity. If poor sensor placement cannot be avoided, consult the vendor to determine if mechanical adjustments to the sensor or software changes to the processing algorithm are necessary to compensate.

b. Causes for Nuisance Alarms: Animals may cause nuisance alarms. These can be rapidly assessed if the integrated security system has video surveillance or video motion detection capability.

c. Vulnerabilities: Intruders may attempt to approach under the cover of heavy rain or heavy fog. Objects or ground surface irregularities may cause shadows in a LIDAR system's field of view that potential intruders could exploit. The system may be vulnerable to tunneling and is not intended to detect intrusions from the air.

LIDAR FENCE


UP TO 990 FT
FENCE
FENCE
LIDAR UNIT
RADIUS OF DEAD ZONE
VARIES DUE TO
LIDAR INSTALLATION HEIGHT
LIDAR UNIT
SCANNED AREA
UP TO 495 FT
FENCE
RADIUS OF DEAD ZONE
VARIES DUE TO
LIDAR INSTALLATION HEIGHT

This page intentionally left blank.

4

VENDORS

This section contains a list of the vendors who responded to the Federal Business Opportunities Journal request for information and a cross-referenced matrix of the responding vendors with appropriate products.

Arkonia Systems Limited
214 Des Bois Dr.
Russell, Ontario K4R 1C4
613-445-3977
www.arkonia.co.uk

BEI Security
15424 Merrifields Ln.
Silver Springs, MD 20906
240-305-1159
www.beicomm.com

DeTekion Security Systems, Inc.
3209 Vestal Pkwy East
Vestal, NY 13850
607-729-7179
www.detekion.com

Diversified Optical Products, Inc.
282 Main Street
Salem, NH 3079
603-898-1880
www.diop.com

DUCOM, Inc.
850 Sligo Ave., Suite 700
Silver Springs, MD 20910
301-585-0900
www.ducominc.com

EMX, Inc.
315 Stan Dr., Suites 5&6
Melbourne, FL 32904
407-568-9767
www.emx-inc.com

Fiber SenSys, Inc.
9640 SW Herman Road
Tualatin, OR 97062, USA
(503) 692-4430
www.fibersensys.com

I**ntegrated Security Corporation**
2550 Oakley Park Rd., Suite 100
Walled Lake, MI 48390
248-624-0700
www.integratedsecuritycorp.com

L3 Communicatons Klein Associates
11 Klein Dr.
Salem, NH 30791
603-893-6131
www.kleinsonar.com

Object Video
11600 Sunrise Valley Dr., Suite 290
Reston, VA 20191
703-654-9300
www.objectvideo.com

Ocean Marine Industries Inc.
206 Research Dr., Suite 101
Chesapeake, VA 23320
757-382-7616
www.oceanmarineinc.com

Perimeter Products
43180 Osgood Rd.
Fremont, CA 94539
510-249-1450
www.perimeterproducts.com

QinetiQ
1215 Jefferson Davis Hwy
Arlington, VA 22202
215-242-6356
www.qinetiq.com

RBtec
55 Hanevi'im St., POB 1877,
Ramat Hasharon, Israel 47117
+972-3-5493387

SAIC
3990 Old Town Ave., 304C
San Diego, CA 92110
619-686-5641
www.saic.com

Senstar Stellar
43184 Osgood Rd.
Fremont, CA 94539
800-676-3300
www.senstarstellar.com

Sparton Technology, Inc.
4901 Rockaway Blvd., SE
Rio Rancho, NM 87124
505-892-5300
www.sparton.com

Systems & Electronics, Inc
201 Evans Ln.
St. Louis, MO 63121
314-553-4187
www.seistl.com

Matrix of Intrusion Detection Sensor Vendors

Sensor Technology / Vendors	Arkonia Systems Ltd.	B.E.I.	DeTekion Security Systems Inc.	Diversified Optical Products Inc.	Ducom Inc.	E.M.X.	Fiber Sensys Inc.	Integrated Security Corp.	L3 Comm Klein Assoc.	Object video	Ocean Marine Industries	Perimeter Products	QinetiQ	Rbtec Electronic Security	SAIC	Senstar-Stellar	Southwest Microwave	Systems & Electronic Inc.
Balanced Magnetic Switch																		
Glassbreak																		
Microwave												X				X	X	
Structural Vibration																		
Audio																		
Passive Infrared	X		X			X		X		X					X	X		
Active Infrared																X		
Dual Technology (PIR/MW)	X		X	X		X		X							X	X		
Fence Vibration								X						X		X	X	
Electrostatic Field			X													X		
Strain Sensitive Cable			X													X		
Fiber Optics		X			X		X							X		X	X	
Taut Wire			X					X						X				
Ported Coax Buried Line			X															
Balanced Buried Pressure																		
Geophone																		
Magnetic Sensors														X				
Video Motion Detection	X									X					X			
Radar	X								X				X					X
Sonar											X		X		X			
Laser Radar (LIDAR)																		

This page intentionally left blank.

ACRONYM GLOSSARY

ATM	Automatic Teller Machine
CBD	Commerce Business Daily
CCTV	Closed Circuit Television
CD	Compact Disc
COTS	Commercial Off The Shelf
DTMF	Dual Tone Multi Frequency
EMI	Electromagnetic Interference
FAR	False Alarm Rate
FedBizOps	Federal Business Opportunities
FSK	Frequency Shift Keying
GHz	Gigahertz
IDS	Intrusion Detection System
IR	Infrared
KHz	Kilohertz
LED	Light Emitting Diode
LIDAR	Light Detection and Ranging

MAD	Magnetic Anomaly Detection
MHz	Megahertz
MW	Microwave
NAR	Nuisance Alarm Rate
Pd	Probability of Detection
PIR	Passive Infrared
PIR/MW	Passive Infrared / Microwave
Radar	Radio Detection and Ranging
RCO	Receiver Cut Off
RF	Radio Frequency
RFI	Radio Frequency Interference
Sonar	Sound Navigation and Ranging
UV	Ultraviolet
VMD	Video Motion Detection