8. Intrusion Detection Sensors

Abstract. *Intrusion detection sensors are divided into exterior or interior sensors depending upon their application. Sensor performance is described by the following characteristics: probability of detection, nuisance alarm rate, and vulnerability to defeat. The integration of individual exterior sensors into a perimeter sensor system must consider specific design goals, the effects of physical and environmental conditions, and the interaction of the perimeter system with a balanced and integrated physical protection system. The methods of classification of exterior sensors used in this session include passive or active; covert or visible; line of sight or terrain following; volumetric or line detection; and application—either buried-line, fence-associated, or freestanding sensors. Interior intrusion sensors can be active or passive, covert or visible, or volumetric or line detectors. The application classes of interior sensors discussed include boundary penetration sensors, interior motion sensors, and proximity sensors. An effective sensor system provides a continuous line of detection using multiple lines of complementary sensors located in an isolated clear zone, along with a variety of interior sensors to achieve protection-in-depth: at the boundary, within the room, and at the object to be protected. Topography, vegetation, wildlife, background noise, climate and weather, and soil conditions and pavement all affect the performance of exterior sensors. The designer of the perimeter sensor system must also consider its interaction with the video assessment system and the access delay system.*

8.1 Introduction

Overview

Intrusion detection systems consist of exterior and interior intrusion sensors, video alarm assessment, entry control, and alarm communication systems all working together. Exterior sensors are those used in an outdoor environment, and interior sensors are those used inside buildings.

Intrusion Detection Definition

Intrusion detection is defined as the detection of a person or vehicle attempting to gain unauthorized entry into an area that is being protected. The intrusion detection boundary is ideally a sphere enclosing the item being protected so that all intrusions, whether by surface, air, underwater, or underground, are detected. The development of intrusion detection technology has emphasized detection on or slightly above the ground surface with increasing emphasis being placed on airborne intrusion. This session will primarily cover ground-level perimeter intrusion detection systems.

Designers Need Knowledge of Facilities and Available Technology

The designer of an intrusion detection system should have a thorough knowledge of the operational, physical, and environmental characteristics of the facility to be protected. In addition, designers should be thoroughly familiar with the spectrum of sensors available, how the sensors interact with the adversary and the environment, and the physical principles on which each sensor classification depends for its operation. Figure 8-1 shows the example interior layout that will be used throughout the session.

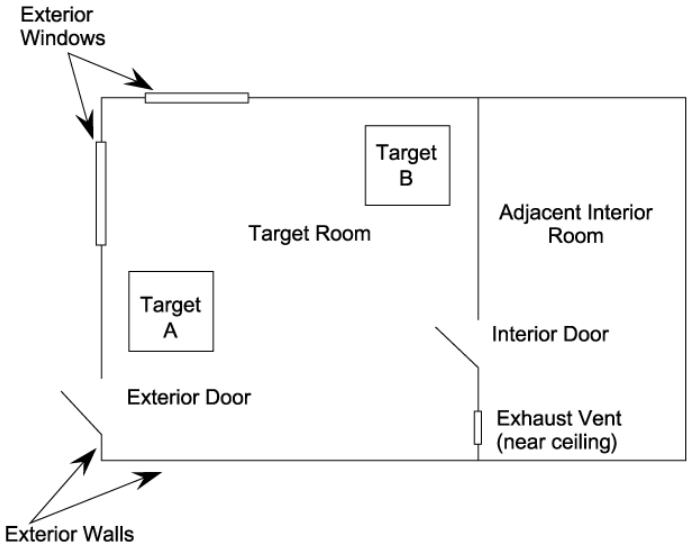

Figure 8-1. Example Interior Layout

Best Detection for Insider Activities

Interior intrusion sensors are the physical protection means that are most effective against the insider threat. Using interior intrusion sensors, an alarm can be generated by unauthorized acts or unauthorized presence of insiders as well as outsiders. INFCIRC225/Rev.5 states that inner areas should be under constant surveillance whenever persons are present. That surveillance and monitoring of interior areas is a primary mission of interior intrusion sensors.

8.2 Performance Characteristics

Fundamentals of Intrusion Sensor Performance

Intrusion sensor performance is described by three fundamental characteristics:

- probability of detection (P_D)
- nuisance and false alarm rates
- vulnerability to defeat

An understanding of these characteristics is essential for designing and operating an effective intrusion sensor system.

8.2.1 Probability of Detection (P_D)

Ideal Sensors Have 100% Success

For the ideal sensor, the P_D of an intrusion is one (1.0). That is, it has a 100% probability of detection. However, no sensor is ideal, and the P_D is therefore always less than 1.0. The way that P_D is calculated does not allow a P_D of 1. Even with thousands of tests, the P_D only approaches 1.

Factors that Affect the Probability of Detection

The probability of detection depends primarily upon:

- target to be detected (size, speed, method of attack, skill)
- sensor hardware design

- installation conditions
- sensitivity adjustment
- weather conditions
- condition of the equipment.

All of the above conditions can vary and, thus, despite the claims of some sensor manufacturers, a specific P_D cannot be assigned to one component or set of sensor hardware. For a P_D value to be meaningful, the conditions of the test must be carefully explained.

8.2.2 Nuisance Alarm Rate

Description

A nuisance alarm is any alarm that is not caused by an intrusion. In an ideal sensor system, the nuisance alarm rate would be zero (0.0). However, in the real world, all sensors interact with their environment and they cannot discriminate between intrusions and other events in their detection zone. Alarm assessment systems are needed because not all sensor alarms are caused by intrusions. The nuisance alarm rate is expressed as a number of nuisance alarms over a period of time, such as 1 alarm per day. Because nuisance alarms are caused by uncontrollable things, such as weather and animals, this number can be highly variable.

Sources of Nuisance Alarms

Usually nuisance alarms are further classified by source. Both natural and industrial environments can cause nuisance alarms. Common sources of natural nuisance alarms for exterior sensors are vegetation (trees and weeds), wildlife (animals and birds), and weather conditions (wind, rain, snow, fog, lightning). Interior sensors are affected by nuclear radiation, electromagnetic, acoustic, thermal, seismic, and optical effects. Industrial sources of noise include ground vibration, debris moved by wind, and electromagnetic interference.

False Alarms

False alarms are those nuisance alarms generated by the equipment itself (whether by poor design, inadequate maintenance, or component failure). Different types of intrusion sensors have different sensitivities to these nuisance or false alarm sources, as is discussed in detail later.

8.2.3 Vulnerability to Defeat

Sensor Defeat Methods

An ideal sensor could not be defeated; however, all existing sensors can be defeated by a knowledgeable adversary with the proper tools and enough time. The objective of the physical protection system designer is to make the system very difficult to defeat. There are two general ways to defeat the system:

- ***Bypass***—Because all intrusion sensors have a finite detection zone, any sensor can be defeated by going around its detection volume.

- ***Spoof***—Spoofing is any technique that allows the target to pass through the sensor's normal detection zone without generating an alarm.

Different types of sensors and sensor models have different vulnerabilities to defeat.

Intruders Trying to Defeat Sensors

Two general categories of intruders may try to defeat the sensor system: the "outsider" and the "insider."

Outsider Characteristics and Tactics

The outsider:

- does not have authorized access to a site.
- observes, from a distance, the site perimeter system (exterior sensors, CCTV cameras, layout, etc.), some daily operations, and possibly a limited amount of interior sensors (such as door switches when outside doors are opened and closed).
- may or may not have technical knowledge of sensors and other system components which he can observe.
- may, at first, try to bypass intrusion sensors such as exterior sensors in order to gain entry to the site.
- may attempt to spoof a sensor if the outsider can gain access to the sensor undetected.

Protecting against the Outsider

Tamper switches, complementary sensors, and other sensors covering a sensor's blind area can help protect against an outsider.

Insider Characteristics

An insider:

- has authorized access to a facility.
- poses a greater threat depending on that person's access levels, technical skills, and actions.

Vulnerabilities Insiders Can Exploit

Interior sensors are often placed in access mode during regular working hours, making them more susceptible to tampering. An insider among maintenance personnel probably has a greater opportunity than other employees and has the technical skills necessary to compromise sensors or the system. Vulnerabilities created by an insider include reducing sensor sensitivity, re-aiming a sensor's coverage area, or changing the characteristics of a zone area. These actions may not totally disable a sensor, but could create a hole in detection.

Protecting Against the Insider

To help protect against the insider, facilities can use:

- procedures such as two-person rules
- sensor effectiveness testing
- insider tracking
- supervised lines between sensor and host alarm system
- continuously monitored sensor tamper switches.

Perform Testing to Ensure Operational Effectiveness Periodically and After Maintenance or Upgrades

Use the follow testing methods to help ensure operational effectiveness:

- Use self-test mechanisms, whether part of a sensor or a separate device, and periodic walk testing, to allow frequent operational testing of the sensor and alarm communications. Self-testing should be activated on a random basis.
- Perform periodic as well as after-maintenance inspections of sensors and components to ensure that they conform to the required configuration and specifications.
- Use a sensitivity analysis or effectiveness test to confirm the performance of a sensor, verify sensor coverage, and to check for blind areas created by changes in room layout. Look for possible alterations and modifications to components during inspections. Effectiveness testing should be performed after repair or replacement of a sensor.
- Perform thorough inspections of spare parts before installation. Secure spare parts during storage to deter tampering.
- Perform walk tests on all sensors monitored by a data collection control panel after that control panel has undergone maintenance.

Two-Person Rule

Each person involved in a two-person rule task must be technically qualified to detect tampering by the other. The two-person rule is effective as long as the individuals involved do not relax the requirement because of long-term friendship or association.

8.3 Sensor Classification

General Classifications

In this discussion, five methods of classification are used:

- passive or active
- covert or visible
- line of sight or terrain following
- volumetric or line detection
- application.

8.3.1 Passive or Active

Passive Sensors Detect Energy

Passive sensors detect some type of energy that is emitted by the target of interest or detect the change of some natural field of energy caused by the target. Examples of the former are mechanical energy from a human walking on the soil or climbing on a fence. An example of the latter is a change in the local magnetic field caused by the presence of a metal.

Active Sensors Transmit Energy

Active sensors transmit some type of energy and detect a change in the received energy created by the presence or motion of the target.

Advantages and Disadvantages

The distinction of passive or active has a practical importance. The presence or location of a passive sensor is more difficult to determine than that of an active sensor; this puts the intruder at a disadvantage. Active sensors may be less affected by environmental conditions than passive sensors because they are transmitting signals selected to be compatible with those conditions. Because of this an active sensor typically may have fewer nuisance alarms than a passive sensor in the same environment.

8.3.2 Covert or Visible

Comparison of Sensor Types

Covert sensors are hidden from view, such as sensors that are buried in the ground or contained in walls. Covert sensors may have signal emanations that can be detected using electronic equipment. Covert sensors are more difficult for an intruder to detect and locate (than visible sensors), and thus they can be more effective. Also, they do not disturb the appearance of the environment.

Visible sensors are in plain view of an intruder, such as sensors that are attached to a fence or mounted on another support structure. Visible sensors may deter the intruder from acting. Visible sensors are typically simpler to install and easier to repair than covert ones.

8.3.3 Line of Sight or Terrain Following

LOS Sensors (exterior) require Specific Site Preparation

Line-of-sight (LOS) sensors perform acceptably only when installed with a clear LOS in the detection space. This usually means a clear LOS between the transmitter and receiver for active sensors. These sensors normally require a flat ground surface, or at least a clear LOS from each point on the ground surface to both the transmitter and receiver. The use of LOS sensors on sites without a flat terrain requires expensive site preparation to achieve acceptable performance.

Terrain-Following Sensors (exterior)

Terrain-following sensors detect equally well on flat and irregular terrain. The transducer elements and the radiated field follow the terrain and result in uniform detection throughout the detection zone. Some terrain-following sensors may require some leveling between fence posts to maintain a high probability of detection.

8.3.4 Volumetric or Line Detection

Factors that Affect Volumetric Detection

Volumetric sensors detect intrusion in a volume of space. An alarm is generated when an intruder enters the detection volume. The detection volume is generally not visible and is difficult for the intruder to precisely identify. The detection volume characteristics are based upon frequency, antenna properties, and other factors. Other factors, such as cable spacing, mounting height, sensitivity, and alignment, can make the exact detection volume difficult for an intruder to determine.

Line Detection Detects at a Specific Point

Line detection sensors detect along a line. For example, sensors that detect fence motion are mounted directly on the fence. The fence becomes a line of detection, since an intruder will not be detected while approaching the

fence; detection occurs only if the intruder moves the fence fabric where the sensor is attached. The detection zone of a line detection sensor is usually easy to identify.

8.3.5 Application

Modes of Sensors: Buried Line, Fence, and Freestanding (exterior)

In this classification method, the sensors are grouped by mode of application in the physical detection space. These modes are

- ***buried line***, in which the sensor is in the form of a line buried in the ground.
- ***fence-associated***, in which the sensor either is mounted on a fence or forms a sensor fence.
- ***freestanding***, being neither buried nor associated with a fence, but mounted on a support in free space.

Choose Sensors for their Needed Strengths (interior)

Interior sensors may be grouped by their application in the physical detection space. Some sensors may be applied in several ways. The application classes are

- Boundary-penetration sensors detect penetration of the boundary to an interior area
- Interior motion sensors detect motion of an intruder within a confined interior area
- Proximity sensors detect an intruder in the area immediately adjacent to an object in an interior area

8.4 Interior Sensor Technology

In the following discussion of interior sensor technologies, the sensors are grouped by their application.

8.4.1 Boundary-Penetration Sensors

Introduction

This class of sensors includes electromechanical, vibration, glass break, infrasonic, and capacitance proximity sensors. The interior area best protected by boundary penetration sensors is shown in Figure 8-2. This area includes ceilings and floors of rooms as well as walls and doors.

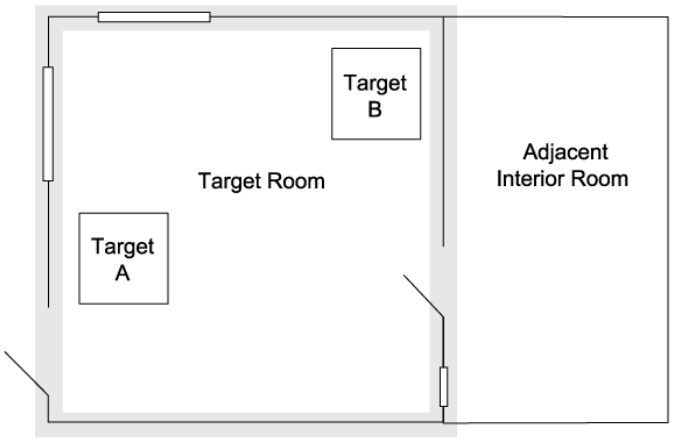

Figure 8-2. Boundary Penetration Areas

8.4.1.1 Electromechanical Sensors

Passive, Visible Line Sensors

Electromechanical sensors are passive, visible, line sensors. The most common type is a relatively simple switch generally used on doors and windows. Most of these switches are the magnetic switches, which consist of two units: a switch unit and a magnetic unit. Figure 8-3 shows the magnetic reed switch and its components in the closed and open positions.

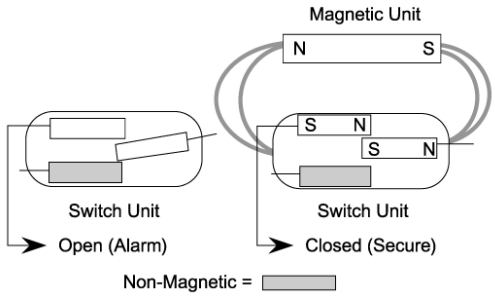

Figure 8-3. Magnetic Reed Switch Principle

Operation

The switch unit, which contains a magnetic reed switch, is mounted on the stationary part of the door or window. The magnetic unit, which contains a permanent magnet, is mounted on the movable part of the door or window, adjacent to the switch unit. With the door or window closed, the spacing between the switch unit and magnet unit is adjusted so that the magnetic field from the permanent magnet causes the reed switch to be in the closed (or secure) position. A subsequent opening of the door or window (removal of the magnet) results in the decrease of the magnet field and movement of the switch to the open (or alarm) position.

Balanced Magnetic Switches

In some of these units, an additional bias magnet that can be adjusted to help prevent defeat is also provided. Those with bias magnets are generally referred to as Balanced Magnetic Switches (BMS). Other variations are multiple reed switches and multiple magnets; fusing and voltage breakdown sensing devices; and shielded case construction. Some units incorporate internal electro-magnets, which have very complex interactions with the

movable magnets, increasing the complexity of the unit and decreasing its vulnerability to defeat. Features are available on some models to make them self-testing.

BMS Features

Balanced magnetic switches provide a higher level of protection for doors and windows than either magnetically or mechanically activated contacts or tilt switches. However, the protection is only as good as the penetration resistance of the door or window. These sensors are only adequate if the intruder opens the door or window for entry.

Hall Effect Switch

A Hall effect switch is electronic without mechanical-type reed switches. It contains active electronics and requires power. It is intended to provide a higher level of security than the balanced magnetic switches. Similar to other magnetic switches, it consists of a switch unit and a magnetic unit. Operation of the switch is based on Hall effect devices in the switch unit measuring and monitoring the magnetic field strength of the magnetic unit. If significant enough magnetic field changes occur, an alarm condition is generated. Both the BMS and Hall effect sensors provide better protection against insider tampering and defeat than does the simple magnetic switch.

Breakwire Sensor

The continuity (breakwire) sensor, is usually attached to, or enclosed in, walls, ceilings, or floors to detect penetration through many types of construction materials. The sensor consists of small electrically conductive wires and electronics to report an alarm when the conductor is broken. The wires can be formed in any pattern to protect areas of unusual shape. Printed circuit technology can be used to fabricate continuity sensors if desired.

Applications

Breakwire grids and screens can be used to detect forcible penetrations through vent openings, floors, walls, ceilings, locked storage cabinets, vaults, and skylights. Nuisance alarm rates for this class of sensor are very low since the wire must be broken to initiate an alarm. When an alarm occurs, the sensor must be repaired or replaced. Breakwire sensors should be continually supervised to decrease the chances of tampering.

9.4.1.2 Vibration Sensors

Description

Vibration sensors are passive, visible, and line sensors. They detect the movement of the surface to which they are fastened. A human blow or other sudden impact on a surface will cause that surface to vibrate at a specific frequency determined by its construction. The vibration frequencies are determined to a lesser extent by the impacting tool.

Vibration sensors may be as simple as mercury switches, or they may be as complex as inertial switches or piezoelectric sensors. In each case, they are designed to respond to frequencies associated with breaking and entering (usually greater than 4 kHz) and to ignore normal building vibrations such as air-conditioning or heating equipment noise.

Applications

The primary application advantage of vibration sensors is that they provide early warning of a forced entry. When applying vibration sensors, the

designer must be aware that the detector might generate nuisance alarms if mounted on the walls or structures that are exposed to external vibrations. If the structures are subject to severe vibrations caused by external sources such as rotating machinery, vibration sensors should not be used. However, if the structures are subject to occasional impacts, vibration sensors with a pulse accumulator or count circuit might be effective.

8.4.1.3 Glass Break Sensors

Description: Vibration or Acoustic Technology

Glass break sensors are passive, visible, and line sensors. They employ either vibration or acoustic technology.

The vibration types are mounted directly on glass and are designed to generate an alarm when the frequencies associated with breaking glass are present within the glass or when an initial impact on the glass is extremely hard. These frequencies are normally above 20 kHz. The vibration type can employ piezoelectric sensor or jiggle switch technology. Acoustic glass break sensors process the sounds of breaking glass. In order to generate an alarm, most of these sensors need to sense the initial low frequency impact followed immediately by the higher glass breaking frequencies.

Acoustic glass break sensors are typically mounted on a ceiling or wall within a specified distance from the window(s) being protected.

Operating Parameters and Nuisance Alarms

Manufacturers usually specify parameters for dependable detection and environmental performance tests to verify that the sensors will operate without excessive nuisance alarms. These parameters include glass thickness, type, and maximum mounting distance from protected windows. Window coverings (curtains, blinds, laminates, and other large objects that may deaden the sound of the glass) affect performance.

Vibrations in glass due to machinery or objects striking glass with sources that generate the higher frequencies of breaking glass can cause nuisance alarms. ***Nuisance alarm sources*** include items such as keys, tape measures, glass objects dropped or struck against other objects and machinery (vehicles, dishwasher, clothes dryer, noisy and loud air handlers).

High-Security Applications

Vibration glass break sensors that are mounted directly on the glass are likely to provide better performance in higher security applications. Direct contact with the glass provides better glass break detection, with some of these devices having magnetic contacts to detect the removal of the glass from the frame.

Glass Break Sensors Do NOT Detect Cutting or Small Holes

Glass break sensors should *not* be depended on for detection of glass cutting or small penetrations in the glass, such as bullet holes.

8.4.1.4 Capacitance Sensors

Description

Capacitance sensors are most commonly proximity-type sensors; however,

they can be applied for boundary penetration detection. They establish a resonant electrical circuit between a protected metal object and a control unit making them active sensors. The capacitance between the protected metal object and ground becomes a part of the total capacitance of a tuned circuit in an oscillator. The tuned circuit may have a fixed frequency of oscillation or the oscillator frequency may vary.

How They Work

Oscillators whose frequency is fixed have an internally adjustable capacitance which is used to compensate for different capacitive loads. A loop of wire, known as the protection loop, is connected between the conductive object or objects to be protected and the control unit which contains the tuned circuit. Once the connection is made, the circuit is adjusted to resonance using a tuning meter for an indicator. Then any change in capacitance between the protection loop (which now includes the metal objects to be protected) and ground will disturb the resonance condition, thereby causing an alarm.

Variable Frequency Oscillators

Variable frequency oscillators use a phase locked loop and use the correction voltage for sensing. This type of capacitance proximity sensor generally balances itself in a short time (usually less than two minutes) after being connected to the conductive metal object to be protected. Once the sensor is balanced, any change in capacitance between the object to be protected and ground will disturb the balance condition, thereby causing an alarm.

Capacitance Proximity Sensors

Capacitance proximity sensors are operated at frequencies below 100 kHz and can often be set to detect capacitance changes of a few picofarads. The object to be protected is normally not grounded. This type of sensor is used to detect boundary penetration through existing openings such as grills and ventilation ducts or metal window frames and doors.

8.4.1.5 Active Infrared Sensors

Description

Active infrared sensors are active, visible, and line sensors. These sensors establish a beam of infrared light using an infrared light source or sources (mated with appropriate lenses) as the transmitters and photodetectors for receivers. Several transmitters and receivers are usually employed to provide a system with multiple beams, and the beams are usually configured into a vertical infrared fence, as shown in Figure 8-4. A pulsed synchronous technique may be used to reduce interference and the possibility of defeat by other sources of light.

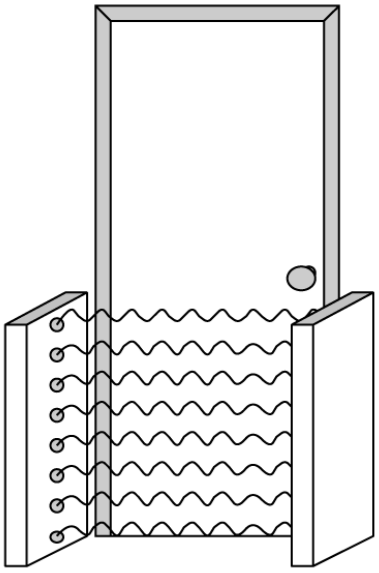

Figure 8-4. Active Infrared System Using Multiple Beams

Applications

The narrow vertical plane in which this sensor operates does not provide any significant volume coverage, and the PPS designer must carefully consider its installation in order to avoid easy defeat or bypass. These sensors can also be used over short ranges for applications for filling gaps, such as for gates, doors, and portals. They may also be used in applications with long ranges up to about 100 m. Infrared light is invisible to the human eye.

Preventing Defeat

To reduce the vulnerability of an intruder bypassing the active IR sensor:

- install at least two detectors to form a barrier.
- install mirrors to reflect the IR beam back and forth to form a fence-like pattern across an entrance.

Nuisance Alarms

IR sensors are susceptible to several nuisance alarm sources, including:

- **Smoke and dust** in the air that can scatter the beam until, depending on the density of the particles, the energy at the receiver is reduced to a level that causes the sensor to initiate an alarm.
- **Falling objects**, small animals, or anything that could interrupt the IR beam long enough can cause an alarm.

8.4.1.6 Fiber Optic Cable Sensors

Description

These passive, line detectors can be either visible or covert. They can be applied as either a boundary penetration or a proximity sensor. A fiber optic sensor typically consists of a length of fiber optic sensing cable and an alarm processor unit. Both ends of the fiber are usually connected to the processor unit which has a light source, a light receiver, and signal alarm

processing electronics. Figure 8-5 shows a block diagram of a fiber optic sensor.

Advantages

One of the major advantages of a fiber optic cable is its immunity to radio and electromagnetic frequencies, and changes in temperature and humidity.

Categories of Fiber Optic Sensors

Fiber optic sensors can be separated into two major categories:

- continuity type sensors and
- microbend type sensors.

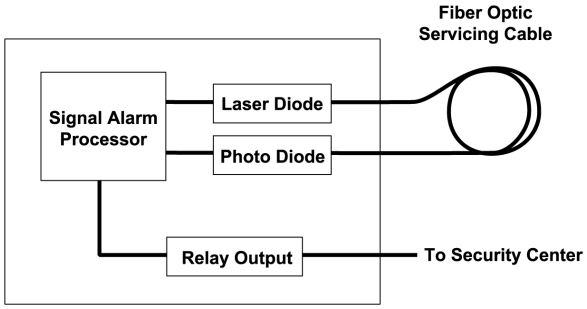

Figure 8-5. Block Diagram of Fiber Optic Sensor

How Fiber Optic Cable Sensors Work

A fiber optic continuity sensor is primarily sensitive to damage or breaks in the fiber loop, which causes a severe loss of signal amplitude at the receiver. The signal alarm processor detects the loss of signal and then initiates an alarm. Schemes such as time-of-flight techniques and synchronous detection, which are based on injecting pulses of light into the fiber, may recognize attempts to splice or bridge portions of the optical fiber.

Microbend Fiber Optic Sensors

A microbend fiber optic sensor is sensitive to both pressure applied and movement of the cable. Pressure and movement causes microbends in the fiber cable, which are detected. Techniques used to detect microbending include:

- ***speckle pattern***—This technique uses a multimode fiber optic cable through which light travels in many different paths. As a result, light at the end of the cable appears as a speckle pattern of light and dark patches when focused onto a detector surface. When the cable is stationary, the pattern is stationary. When microbending occurs, the speckle pattern changes. The photo diode detector converts the changes to electrical signals.

- ***interferometry***—This technique uses a single mode fiber. Wavelength-division multiplexing is employed using a beam splitter that generates multiple light signals at different wavelengths to travel down the same fiber in opposite directions. When pressure is applied to the fiber cable, changes to the interference between the signals occur. These changes are detected and converted to electrical signals for processing.

Electrical Signal Processing Occurs

With either technique, the alarm processor performs electrical signal processing of the microbending events that occur along a fiber sensor cable.

The processing is aimed at detecting intruder movement and rejecting nuisance alarm sources. The amount of processing varies among the different models. Examples of the processing are sensitivity and threshold levels, event counting, event timing, low and high pass frequency filtering.

Sensing Area

The sensing area covered by a fiber optic sensor depends on how the cable is laid out or arranged and the maximum length of cable supported by the fiber processor. Systems currently being offered can support in the ranges of 1000 to 2000 meters of sensor cable, depending on the system.

Continuity Sensors vs. Microbend Sensors

Fiber optic continuity sensors, when properly installed, are a reliable means of intrusion detection for structural boundary penetration such as breaking through walls or ceilings. Fiber optic microbend sensors can be applied as vibration or pressure sensors. Interior detection applications include installation within or on walls, ceilings, or doors, or under carpets. One advantage of using a fiber optic microbend sensor over a continuity sensor is that a microbend sensor can give earlier warning that an intrusion is being attempted. In the case of a wall protection application, the sensor can detect vibrations caused by a penetration attempt.

Nuisance Alarms

Nuisance alarm sources for microbend fiber optic sensors are similar to sources for vibration sensors. Vibrations caused by external sources such as rotating machinery, low flying aircraft, nearby trains, or large vehicles can cause nuisance alarms. Some nuisance alarm sources can be filtered out by adjusting the sensitivity, frequency filtering, event counting, and event timing. Caution must be exercised against decreasing sensitivity to intrusion detection when adjusting to reduce nuisance alarms.

8.4.2 Interior Motion Sensors

Figure 8-6 shows the interior areas best suited to motion sensors.

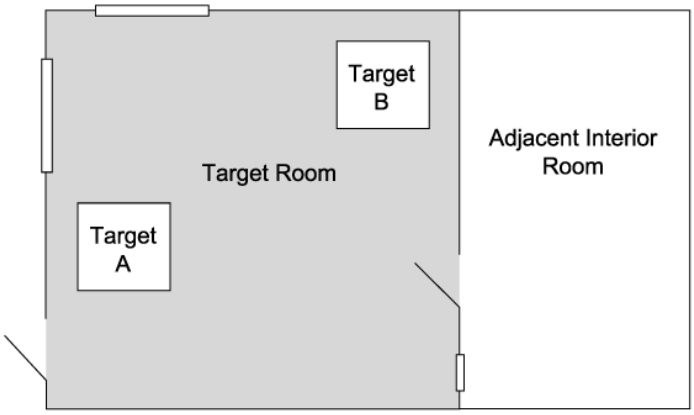

Figure 8-6. Interior Motion Area

8.4.2.1 Microwave Sensors

Description

Microwave sensors are active, visible, and volumetric sensors. They establish an energy field using energy in the electromagnetic spectrum,

usually at frequencies on the order of 10 GHz. Interior microwave motion sensors are nearly always in the monostatic configuration with a single antenna being used to both transmit and receive. Intrusion detection is based on the Doppler frequency shift between the transmitted and received signal caused by a moving object within the energy field. Microwave sensors are most sensitive with motion directly towards or away from the sensor. This is because the largest amount of Doppler frequency shift is created with motion towards or away from the sensor. This needs to be kept in mind when determining a location for the sensor. To the extent possible, the sensor should be located so that an intruder's movement in the direction of protected items from likely points of entry will have a considerable vector of movement towards the sensor.

Antenna Design and Detection Zone

The shape of the detection zone is governed by the design of the antenna and is roughly similar to an elongated balloon. The antenna is typically a microwave horn but may be a printed circuit planar or phased array. Figure 8-7 shows a typical relationship between antenna angle and pattern shape. A manufacturer may show a representation of a full and a half pattern based on the sensitivity settings of the sensor and assuming the same size target. A large target may be detected at a greater distance, even at lower sensitivity settings unless the sensor is range-gated.

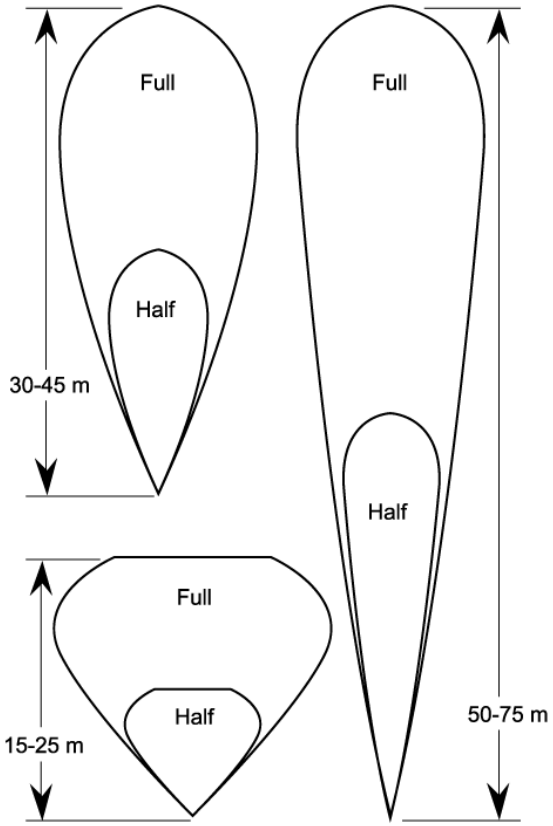

Figure 8-7. Typical Microwave Detection Patterns

Range Gating—Recognizing Return

Monostatic microwave sensors can be range-gated. Range gating is an electronic technique that only allows the sensor to recognize return echoes

Echoes

that occur within a specified period. Return echoes that occur at other times are ignored. The return time of the echo is determined by the distance from the sensor to the intruder (or other target). Range gating is usually used to prevent detection beyond a maximum desired range.

Applications

Range gating is desirable if the sensor is to be used at a location where the microwave energy can penetrate beyond the walls of the area or room being protected. Microwave energy will readily penetrate most glass, as well as plaster, gypsum, plywood, and many other materials used in normal wall construction. Such penetration can cause unwanted interference with effective sensor operation. Metal objects, such as large bookcases or desks and screens or fencing within the protected area, will cause shadow zones and incomplete coverage.

Advantages and Disadvantages of Microwave Sensors

The fact that microwave energy can penetrate walls has both advantages and disadvantages. An advantage occurs when an intruder is detected by the microwave energy penetrating partitions within a protected volume; but detecting someone or something moving outside the protected area, or even outside the building, is then a disadvantage and would cause a nuisance alarm. Plastic drain pipes inside a wall can also be a hard to determine cause of nuisance alarms. Because microwave energy is difficult to contain, special care should be taken when locating and directing the energy within the area requiring protection.

Point Sensors for Limited Coverage

Monostatic microwave devices can also be used as point sensors to provide limited coverage of a point or area in which other sensors may provide inadequate coverage or may be vulnerable to tampering. A common commercial application of monostatic microwave sensors is automatic door openers used in supermarkets and airports.

Placement

Microwave detectors should be mounted high, near the ceiling of the area being protected. They should be aimed in the direction of desired coverage, yet pointed away from metal objects that might reflect microwave energy and cause nuisance alarms.

8.4.2.2 Passive Infrared Sensors

Description

Passive infrared sensors are passive, visible, and volumetric. This sensor responds to changes in the energy emitted by a human intruder, which is approximately equal to the heat from a 50-W light bulb. They also detect changes in the background thermal energy caused by someone moving through the detector field of view and shadowing the energy emanating from the objects in the background. These systems typically employ special optical and electronic techniques that limit their detection primarily to an energy source in motion.

Characteristics of Infrared Radiation

The major characteristics of infrared radiation (IR) are:

- IR is emitted by all objects. The intensity of the infrared is related to the object's temperature.

- IR energy is transmitted without physical contact between the emitting and receiving surfaces.
- IR warms the receiving surface and can be detected by any device capable of sensing a change in temperature.
- IR is invisible to the human eye. Passive infrared (PIR) sensors respond to infrared energy in the wavelength band between 7 and 14 nm.

Technical Considerations

The passive infrared sensor is a thermopile or pyroelectric detector that receives radiation from the intruder and converts changes in this radiation into an electrical signal. The signal is then amplified and processed through logic circuits. Special lenses focus the IR energy onto the detector and create a specific detection field of view. The field of view can be changed by changing lenses. The lenses also segment the field of view into sensitive and non-sensitive areas. When a source of radiation (such as an intruder) moves within the field of view, changes in the radiation received at the pyroelectric detector occur (due to the segmented lens), resulting in an electrical signal output of the detector. Simple processing of the signal includes intensity measurement, pulse counting (number of sensitive segments an intruder moved through) and timing of the pulses. Once a predetermined set of signal parameters are present, an alarm is generated. Current PIR sensors usually employ more sophisticated and proprietary signal processing. The probability of detecting someone moving through a varying background will generally be higher than detecting the same person moving through a constant background.

Applications

Many passive infrared sensors are available with multiple lenses that can be changed in the field. These vary from a short distance, wide angle field of view to a longer distance, narrow field of view. The wide angle lenses provide volumetric detection, such as within a room, while the long narrow lenses can be used to protect a corridor.

Nuisance Alarms

Sources of nuisance alarms include:

- An ***insect*** crawling on the lens can cause a large enough temperature change, creating a nuisance alarm.
- ***Other sources of infrared energy***. Infrared energy does not penetrate most building materials (including glass) and therefore sources of infrared energy that are located outside buildings will not typically generate nuisance alarms. Nuisance alarms can be generated indirectly, however, from sources outside the buildings due to local heating effects. For example, while glass and Plexiglas™ window materials are effective filters for infrared energy in the wavelength region of interest (7 to 14 nm), sunlight passing through windows can produce locally heated surfaces that can radiate energy in this band. If changes in these locally heated surfaces are fast enough, an alarm can be generated.
- ***Heat sources***. Place infrared sensors away from any heat sources that could produce thermal gradients in front of the sensor's lens. Heat

sources within the sensor's field of view should be avoided. For instance, an infrared sensor should never be mounted over or near radiators, heaters, hot pipes, etc. Radiant energy from these sources can produce thermal gradients in the view of the detector's lens that might change the background energy pattern. Depending on the intensity of the heat source, the thermal gradients might cause nuisance alarms. An unshielded incandescent light that is within 3-5 m of the sensor might also cause an alarm if it burns out or goes out due to loss of power.

Detection Pattern

The detection pattern for a typical passive infrared sensor is shown in Figure 8-8. Subdivision of the field of view into the solid angular segments shown is accomplished with the segmented lens. PIR lenses are either a fresnel type lens located in front of the pyroelectric detector, or a segmented mirror type lens that reflects energy onto the detector.

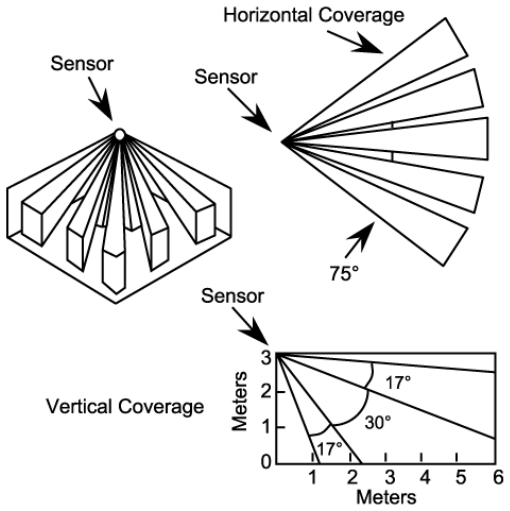

Figure 8-8. Passive Infrared Sensor Pattern

PIR Sensitivities

An important characteristic of PIR sensors that the physical protection designer needs to be aware of is that PIR sensors are most sensitive with motion across the field of view, and least sensitive directly toward or away from the sensor. (This is the opposite of microwave and ultrasonic sensors). Motion through the field of view will result with more segments being entered in a shorter distance. This characteristic plays an important role in determining where to mount the sensor with regards to the most likely ways of intruder entry. Keeping in mind also the location of any nuisance alarm sources.

8.4.2.3 Dual Technology Sensors

Description

This sensor is both active and passive, visible, and volumetric. This sensor attempts to achieve absolute alarm confirmation while maintaining a high probability of detection. Absolute alarm confirmation is achieved ideally by combining two technologies that individually have a high probability of detection and no nuisance alarms in common. Currently available dual technology motion detectors combine a microwave sensor with a passive infrared sensor. Dual technology sensors use different combinations of

sensor technologies. While traditional dual technology sensors incorporate a combination of passive infrared and microwave technologies, some sensors use passive infrared/micro impulse radar and passive infrared/glass break technologies. When used in combination, alarms from the microwave sensor are logically combined with the alarms from the infrared sensor in an AND gate logic configuration. The AND gate logic requires nearly simultaneous alarms from both the active and passive sensors to produce a valid alarm. Some dual technology sensors allow the technologies to be selectable in either the logical AND or logical OR combination. In addition, some dual technology sensors use different logic schemes. As an example, one dual technology sensor uses pattern recognition algorithms to identify conditions to switch between the PIR/microwave modes to a microwave mode only.

Nuisance Alarm Rate

Dual technology sensors usually have a lower nuisance alarm rate than single technology sensors when the detectors are properly applied and assuming each has a low nuisance alarm rate.

Probability of Detection

However, when two sensors are logically combined with AND, the probability of detection of the combined detectors will be less than the probability of detection of the individual detectors. For instance, if one sensor has a probability of detection of 0.95 and it is combined with an infrared detector that also has a probability of detection of 0.95, the dual sensor has the product of the individual probabilities of detection, or only 0.90. Also, microwave detectors have the highest probability of detecting motion directly toward or away from the sensor, but infrared sensors have the highest probability of detecting someone moving across the field of view. Therefore, the probability of detection of the combined sensors in a single unit will be less than if the individual detectors are mounted perpendicular to each other with overlapping energy patterns and field of view. Therefore, if a higher probability of detection is needed for the application, separately mounted logically combined sensors are recommended. To achieve the highest probability of detection, the individual sensors should be separately annunciated.

8.4.3 Proximity Sensors

This class of sensors includes capacitance and pressure sensors. Figure 8-9 shows the interior areas best protected by proximity sensors.

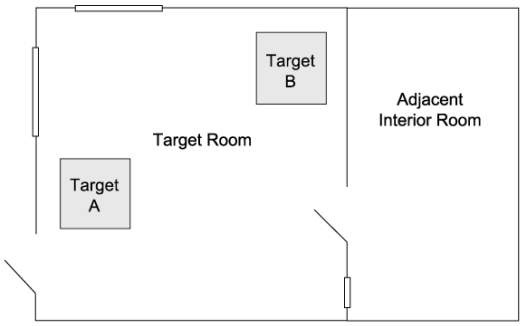

Figure 8-9. Proximity Area

8.4.3.1 Capacitance Proximity Sensors

Definition

Capacitance proximity sensors are active, covert, and line sensors. They can detect anyone either approaching or touching metal items or containers that the sensors are protecting. These sensors operate on the same principle as electrical capacitors. A capacitor is an electronic component that consists of two conductor plates separated by a dielectric medium. A change in the electrical charge or dielectric medium results in a change in the capacitance between the two plates. In the case of the capacitance proximity sensor, one plate is the metal item being protected, and the second plate is an electrical reference ground plate under and around the protected item. The metal item in this application is isolated from ground by insulating blocks. This leaves only air around and between the metal object and ground. Therefore, air is the dielectric medium.

How They Work

During operation, the metal object is electrically charged to a potential that creates an electrostatic field between the object and reference ground. The electrical conductivity of an intruder's body alters the dielectric characteristic as the intruder approaches or touches the object. The dielectric change results in a change in the capacitance between the protected item and the reference ground. When the net capacitance charge satisfies the alarm criteria, an alarm is activated. Figure 8-10 illustrates a typical arrangement for connecting a capacitance proximity sensor to a safe or file.

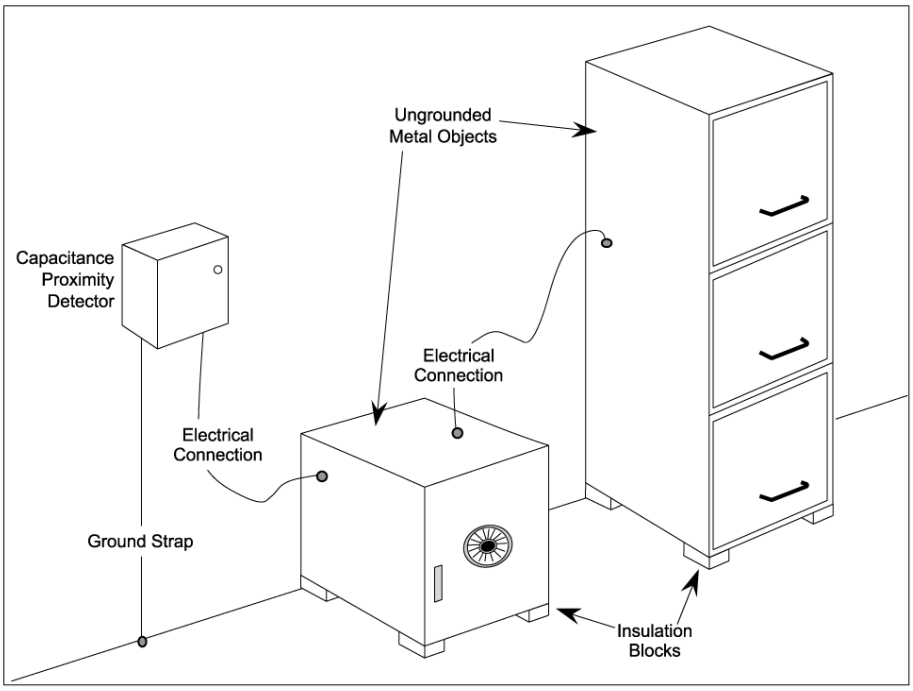

Figure 8-10. Typical Connections of Capacitance Proximity Sensor

Capacitance Blanket

For applications where the object to be protected must be grounded, the object can be considered the ground plane. This requires the fabrication of a capacitance blanket for draping over the protected object as shown in Figure 8-11. If the blanket is made large enough to cover the object

entirely, any access attempts will cause blanket movement, capacitance change, and alarm.

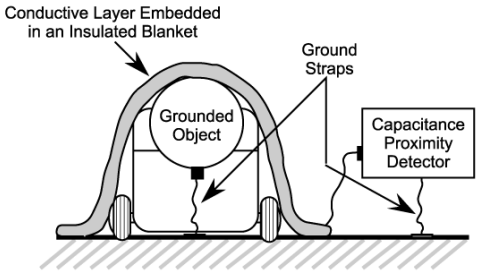

Figure 8-11. Grounded Object Protected by a Capacitive Blanket

Sensitivity Affected By Humidity and Metal Objects

The sensitivity of capacitance sensors is affected by changes in relative humidity and the relocation of other metal objects closer to or away from the protected item. Changes in the relative humidity vary the dielectric characteristics which can either increase or decrease the air conductivity. If the sensor's sensitivity is adjusted to detect an intruder several meters from the object, this change in conductivity could be enough to initiate a nuisance alarm.

Capacitance sensors using a self-balancing circuit adjust automatically to the change in relative humidity and relocation of metal objects close to the protected object.

Grounding Conditions

Sometimes objects requiring protection are located in areas with poor grounding conditions. In such places, a reference or ground plane can be established by installing a metal sheet or screen under the object.

Avoid using wooden blocks to isolate the protected metal object from the ground plane. Wooden blocks might absorb enough moisture over a period of time to change the dielectric enough that the protective object is no longer isolated from ground, resulting in nuisance alarms.

8.4.3.2 Pressure Sensors

Description

These sensors are passive, covert, and line detectors. Pressure sensors, often in the form of mats, can be placed around or underneath an object. Pressure mats consist of a series of ribbon switches positioned parallel to each other along the length of the mat. Ribbon switches are constructed from two strips of metal in the form of a ribbon separated by an insulating material. They are constructed so that when an adequate amount of pressure, depending on the application, is exerted anywhere along the ribbon, the metal strips make electrical contact and initiate an alarm.

Placement

When using pressure mats in security applications, the mats should be well concealed under carpets or even under tile or linoleum floor coverings. If the intruder is aware of their existence, however he can just step over or bridge over the mat. Pressure mats alone should be used only to detect low-skill intruders. However, pressure mats can be used along with other sensors in a system designed to provide a higher level of protection.

Classification Summary of Interior Sensors

Table 8-1 provides a summary of classifications for interior sensors.

Table 8-1. Typical Classifications of Interior Sensors

	Passive or Active	Covert or Visible	Volumetric or Line
Boundary Penetration Sensors			
Electromechanical	P	C	L
Infrared	B*	V	L
Vibration	P	C	L
Capacitance	P	C	L
Fiber Optic	P	E*	L
Interior Motion Sensors			
Microwave	A	V	V
Infrared	P	V	V
Proximity Sensors			
Capacitance	P	C	L
Pressure	P	C	L
Fiber Optic	P	E*	L

B* - Both active and passive types exist

E* - Can be either covert or visible

8.4.4 Wireless Sensors

Description

The most common wireless sensors are the radio frequency (RF) transmission type. In the United States these systems typically operate in the 300 MHz or 900 MHz bands. Some systems utilize spread spectrum techniques for transmission.

Typical Operation

A typical RF wireless sensor system consists of sensor/transmitter units and a receiver. The sensor/transmitter unit has both the sensor and transmitter electronics integrated into one package and are battery powered. Advertised battery life is 2 to 5 years, depending on the number of alarms and transmissions. Each sensor/transmitter unit is programmed with a unique identification code. The number of individual sensors that can transmit to one receiver and the transmission range varies with the system. In order to conserve battery power, the transmitters are in a "sleep" mode until an event requires a transmission. Events consist of alarms, tampers, and state-of-health messages. Alarms and tampers are transmitted when they occur. State-of-health messages verify that the sensor is still present and operating. They typically consist of battery status, alarm status, and tamper status and are transmitted to the receiver at user specified intervals. The receiver is programmed to expect state-of-health messages at the specified intervals. If they are not received, the receiver will indicate a fault condition.

Sensor Types Associated with Wireless Systems

Most wireless systems have PIR, microwave, dual-technology, and magnetic switch as sensor types. They also typically have what is known as a universal transmitter. The universal transmitter allows interfacing to other sensors or controls by monitoring the alarm contacts of the separate sensor.

RF Sensor System Limitations

Some of the concerns when considering the use of an RF sensor system include:

- ***Collisions***—Collisions occur when two or more signals, such as state-of-health, are received simultaneously, resulting with neither message being read by the receiver.
- ***Signal fade***—Fading can occur when the path between the transmitter and receiver is too far or is blocked by too much material which shields the RF signal, such as large metal objects, metallic building siding, etc.
- ***Interference***—Interference occurs when other RF sources transmitting in the same frequency range overpowers the signal sent by the sensor/ transmitter unit.
- ***Jamming***—Jamming is similar to interference and can be attempted by an intruder so that alarm signals do not get through to the receiver.

Techniques such as spread spectrum transmission and dithering the state-of-health timing can help reduce these problems. Testing to verify a good transmission path and possible interference sources prior to final location and installation of transmitters and receivers is recommended and can also help reduce problems. For high security applications, hardwired systems provide higher protection for alarm signal transmission. Aside from signal jamming, an intruder can also attempt to intercept alarm transmissions or mimic a secure state to the receiver.

8.4.5 Miscellaneous Technologies

Light and Electric Sensors

Any quantity or parameter in a volume or area that changes when an intrusion takes place can be used to detect the intrusion. The most common ones have already been discussed. Other technologies that have been exploited include:

- ***Light sensors*** monitor the average light level within their field of view. If the light level changes by a predetermined amount, the possibility of an intrusion exists. The light sensor is designed to produce an alarm when such a change occurs.
- ***Electric field sensors*** are similar to capacitance proximity sensors except they may cover larger areas. They consist of sets of wires that alarm when a human approaches or touches the wires, for example, along a wall.

8.5 Effects of Environmental Conditions on Interior Sensors

Environmental Conditions Can Affect Sensor Performance

Many environmental conditions can produce signals (also called "noise") in the same energy spectra that the intrusion sensors are designed to detect. These outside sources can degrade sensor performance and may cause the sensor to generate an alarm even when an intruder is not present. The following paragraphs discuss several factors that can degrade sensor performance. Environmental conditions that can affect interior sensors include:

- electromagnetic energy
- nuclear radiation
- acoustic
- thermal
- optical
- seismic
- meteorological

8.5.1 Electromagnetic Energy

Electromagnetic Energy Can Adversely Affect Performance

Sources of electromagnetic energy that could affect the performance of a particular type of interior detection system include:

- lightning
- power lines and power distribution equipment
- transmission of radio frequency
- telephone lines and equipment
- lighting
- computer and data processing equipment
- various electric-powered vehicles such as forklifts and elevators
- television equipment
- automotive ignition
- electrical machinery or equipment
- intercom and paging equipment
- aircraft

Construction Affects Electromagnetic Energy

Construction of the building or room to be monitored will play an important role in determining the nature of the electromagnetic energy that is present. If the structure is made primarily of wood or concrete, neither of which provides electromagnetic shielding, then a high background of electromagnetic energy generated by sources outside the building or room is possible.

How to Minimize Electromagnetic Energy

The best way to minimize the effects of stray electromagnetic energy is:

- to provide electromagnetic shielding to all system components (including all data transmission links), and
- to ensure that all the components have a common, adequate electrical ground.

8.5.2 Nuclear Radiation Environment

Nuclear Radiation Degrades Performance

Nuclear radiation can damage various components within the sensor. The most susceptible elements are semiconductors. Research has shown that current systems cannot be made totally invulnerable to the effects caused by some radiation environments. System vulnerability can, however, be reduced by the appropriate design and choice of components. Generally speaking, neutrons will degrade the performance of semiconductor devices and integrated circuits. The degradation primarily depends on the total dose.

8.5.3 Acoustic Environment

Sources of Acoustic Energy

Acoustic energy is generated by many sources within an internal area. Also, energy generated by outside sources can be transmitted into an area to be protected. Some of the forms of acoustic energy that can affect the performance of interior sensors are noise from meteorological phenomena; ventilating, air-conditioning and heat equipment; television equipment; telephone electronic equipment; and exterior sources such as aircraft, vehicles, and trains.

8.5.4 Thermal Environment

Sources of Thermal Stimuli

Changes in the thermal environment can result in stimuli that affect the performance of interior intrusion sensors. These stimuli include uneven temperature distribution that causes air movement within the area and expansion and contraction of buildings. Causes of changes in the thermal environment include weather, heating and air-conditioning equipment, machinery that produces heat, interior lighting, chemical and radioactive reactions producing thermal outputs, and fluctuations of sunlight through windows and skylights.

8.5.5 Optical Effects

Light Affects Sensor Performance

The sources of optical phenomena that affect interior intrusion sensors include light energy from sunlight, interior lighting, highly reflective surfaces, and infrared and ultraviolet energy from other equipment.

8.5.6 Seismic Effects

Seismic Phenomena Produce Vibrations

Seismic phenomena affect interior intrusion devices by producing undesirable vibrations in interior areas. Seismic phenomena include earth tremors, machine equipment, vehicular traffic, trains, thunder, and high winds.

8.5.7 Meteorological Effects

Weather Affects Sensors Adversely

Meteorological phenomena, such as lightning, thunder, rain, hail, temperature, wind, earth tremors, high relative humidity, and sunlight, that adversely affect interior intrusion sensors have already been discussed within the individual sensor sections.

8.6 Interior Sensor Selection

Factors to Consider in Sensor Selection

Sensor selection consists of identification of the equipment and installation methods that best meet the intrusion detection system objectives for a given facility. A consideration of the interaction among equipment, environment, and potential intruders is integral to the selection of the proper technological type of equipment necessary to ensure the desired intrusion detection functions. Two important physical conditions that affect sensor performance are the building or room construction and the various equipment or objects that occupy the same area or room to be monitored.

The major characteristics of several types of interior sensors suitable for fixed site applications are shown in Table 8-2.

Table 8-2. Interior Sensors Suitable for Fixed-Site Applications

Application	Operating Principle	Detection					Factors That Cause Unreliable Detection	Typical Defeat Methods	Major Causes of Nuisance Alarms									
		Portal Opening	Break through Wall/Floor\Ceiling	Radial Motion	Transverse Motion	Touching Object			Humidity/Temp/ Velocity (wind)	Localized Heating (sunlight)	Movement Greater than 0.025 m/sec	Movement Outside Area (Vibration)	Fluorescent Lights	Loose-Fitting Doors	Mount Vibration	Ambient Acoustic Noise (lightning/thunder)	Animals	RFI-radio transmitter
Boundary Penetration	Balanced Magnetic	X					Improper installation	Stay behind intruder or enter through unprotect-ted area						X				
	Vibration		X									X			X			
	Continuity		X															
Motion	Microwave	X		X			RFI	Cover when sensor is in access			X	X	X		X		X	X
	Infrared				X		Unstable thermal background			X					X		X	X
Proximity	Capacitance					X	Gross changes in relative humidity, temperature, or pressure	Disable electronics	X								X	
	Strain					X											X	
	Pressure Pad					X											X	

Understand the Environment and Possible Sources of Nuisance Alarms When Selecting Sensors

It is usually possible to identify appropriate sensors that will perform acceptably in the environment in question since the environment associated with interior areas is normally controlled and is usually predictable and measurable. However, correct sensor choice requires that the particular nuisance alarm stimuli to which it is susceptible be known, as well as whether these stimuli are contained in the environment in question. This is particularly true of the motion detectors (microwave and infrared), all of which can be installed to provide acceptable detection coverage and which typically have nuisance alarms from different stimuli. Figure 8-12 shows a possible arrangement of interior sensors for the example layout.

Optimum performance of an interior intrusion detection system can be achieved by an appropriate combination of sensors and sensor technologies.

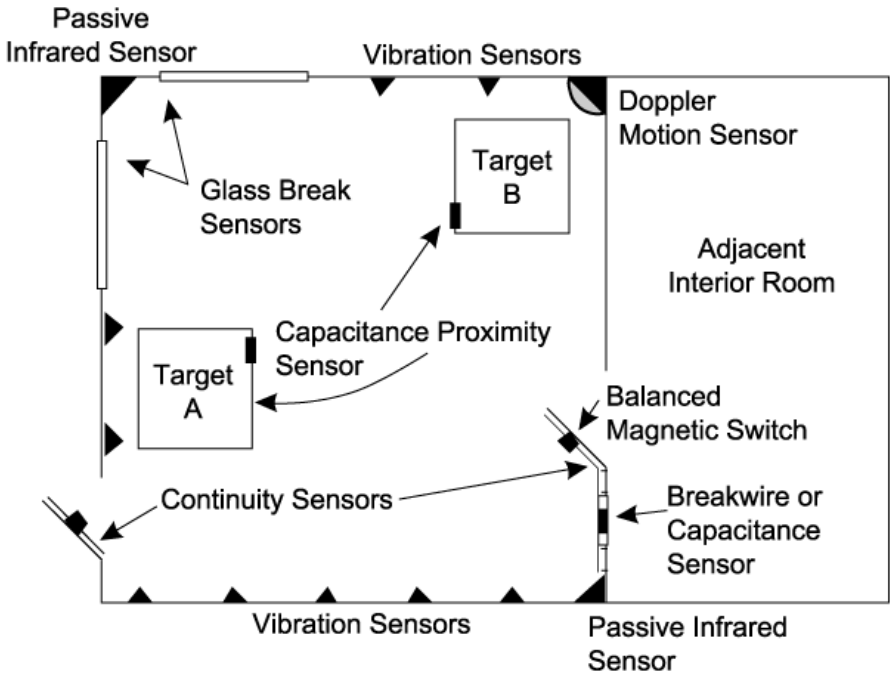

Figure 8-12. Example Layout of Interior Sensors

8.7 Exterior Sensor Technology

Types of Perimeter Sensors

In this discussion, the exterior sensors are grouped by their modes of application. Table 8-3 summarizes the different exterior intrusion sensor technologies according to the different sensor classification schemes.

Table 8-3. Types of Perimeter Sensors

	Passive or Active Detection	Covert (C) or Visible (V)	Line of Sight (LOS) or Terrain Following (TF)	Volumetric (V) or Line (L)
Buried Line				
Seismic Pressure	P	C	TF	L
Magnetic Field	P	C	TF	VOL
Ported Coax	A	C	TF	VOL
Fiber Optic Cables	P	C	TF	L
Fence-Associated				
Fence Disturbance	P	V	TF	L
Sensor Fence	P	V	TF	L
Electric Field	A	V	TF	VOL
Freestanding				
Active Infrared	A	V	LOS	L/VOL*
Passive Infrared	P	V	LOS	VOL
Bistatic Microwave	A	V	LOS	VOL
Dual Technology	A	V	LOS	VOL
Video Motion	P	C	LOS	VOL

8.7.1 Buried-Line Sensors

Types of Buried Line Sensors

Types of buried-line sensors that depend on different sensing phenomena include:

- pressure or seismic sensors,
- magnetic field sensors,
- ported coaxial cable sensor, and
- fiber optic sensors.

8.7.1.1 Pressure or Seismic

Description and Applications

Seismic sensors are passive, covert, terrain-following sensors that are buried in the ground. They respond to disturbances of the soil caused by an intruder walking, running, jumping, or crawling on the ground.

Seismic Sensor Technology

A typical seismic sensor consists of a string of geophones. A geophone consists of a conducting coil and a permanent magnet. Either the coil or the magnet is fixed in position, and the other is free to vibrate during a seismic disturbance; in both cases an electrical current is generated in the coil. Far-field effects in seismic sensors can be somewhat reduced by alternating the polarity of the coils in the geophone string.

Sensitivity and Burial Depth

The sensitivity of this type of sensor is very dependent on the type of soil in which it is buried. The best burial depth is also dependent on the soil. The trade-off is high probability of detection with narrow detection width at a shallow depth versus lower probability of detection with wider detection width at a greater depth. A test conducted on site with short test sections of the sensor buried at different depths is recommended to determine the optimum depth. A typical detection width for walking intruders is in the range of 1–2 m.

Effects of Winter Weather

Pressure and seismic sensors tend to lose sensitivity in frozen soil. Thus, at sites where the soil freezes in winter, either a reduced winter sensitivity must be accepted, or a semiannual adjustment to pressure and seismic sensors must be made to obtain equivalent sensitivity throughout the year.

Nuisance Alarms for Seismic Sensors

Many sources of seismic noise may affect these sensors and cause nuisance alarms. The primary natural source of nuisance alarms is wind energy that is transmitted into the ground by fences, poles, and trees. Seismic sources made by man include vehicular traffic (cars, trucks, trains) and heavy industrial machinery. Because it is difficult to distinguish between footsteps close to the sensor and vehicle traffic much farther away with these types of sensors, they are seldom used in perimeter applications and are more frequently used in battlefield or border applications.

Defeat Methods

Because these sensors are passive and buried, movement above the ground is not detected. If the location of the buried-line sensor is known, an adversary may defeat this sensor by forming a low bridge over the transducer line.

8.7.1.2 Magnetic Field

Detect Vehicles and Intruders with Metal Weapons

Magnetic field sensors are passive, covert, terrain-following sensors that are buried in the ground. They respond to a change in the local magnetic field caused by the movement of nearby metallic material. Thus magnetic field sensors are effective for detecting vehicles or intruders with weapons.

Technology Description, Nuisance Alarms, Defeat Method

This type of sensor consists of a series of wire loops or coils buried in the ground. Movement of metallic material near the loop or coil changes the local magnetic field and induces a current. Magnetic field sensors can be susceptible to local electromagnetic disturbances such as lightning. Intruders who are not wearing or carrying any metal may be able to defeat this type of sensor. Because of the passive nature of the magnetic sensor it is difficult to tell whether the alarm was caused by an intruder with a small weapon close to the sensor or a large vehicle outside of the perimeter. Like the seismic sensors, magnetic sensors are not commonly used in perimeter applications.

8.7.1.3 Ported Coaxial Cables

Description

Ported coaxial cable sensors are active, covert, terrain-following sensors that are buried in the ground. They are also known as leaky coax or radiating cable sensors. This type of sensor responds to motion of a material with a high dielectric constant or high conductivity near the cables. These materials include both the human body and metal vehicles.

Technology

The name of this sensor is derived from the construction of the transducer cable. The outer conductor of this coaxial cable does not provide complete shielding for the center conductor, and thus some of the radiated signal leaks through the ports of the outer conductor. The detection volume of ported coax sensors extends significantly above the ground: about 0.5 to 1.0 m above the surface and about 1 to 2 m wider than the cable separation. The sensitivity of this type of sensor in frozen soil actually increases slightly relative to thawed conditions. This is because some of the field energy is absorbed by conductive soil, and the conductivity of frozen ground is less than that of thawed ground.

Installation

Some ported coaxial cables use a foil shield with a slot instead of actual ports. A semiconductive inner jacket allows the combination of the two cables into a single outer jacket. This allows the sensor to be installed more easily because only a single trench is required and cable spacing is no longer an issue. The disadvantage is that the detection volume is slightly smaller than for a dual cable system with a wider cable spacing. Older versions of this technology provided a single alarm indication for a single zone, typically 100 meters, and also allowed only a single alarm threshold for each zone. Newer versions can provide additional location of where the alarm occurred along the cables within a few meters of resolution. In addition, the alarm thresholds may also be varied along the length of the cables, allowing more even sensitivity settings as the sensor cables pass through different burial mediums.

Nuisance Alarms

Metal or water in the ported coax detection zone can cause two types of sensor problems. Moving metal objects and moving water are large targets for ported coax sensors and thus are a major potential source of nuisance alarms. Both flowing water and standing water contribute to this problem. The second problem is that fixed metal objects and standing water distort the radiated field, possibly to the extent of creating insensitive areas with no detection. Nearby metal objects or utility lines should be excluded from the detection volume. This includes above ground fences and poles and underground water lines and electrical cables.

8.7.1.4 Fiber Optic Cables

Description

Optical fibers are long, hair-like strands of transparent glass or plastic. Fiber optics is the class of optical technology that uses these transparent fibers to guide light from one end to the other. A fiber optic cable consists of an inner core of pure material and a cladding material that is usually the same material as the core with additional "doping" material added. Because the cladding is designed to have a different refraction of light, the light ray is bent back towards the center of the core. Thus, the fiber becomes a "lightpipe" (Figure 8-13). A fiber can either be multi-mode or single-mode depending upon the thickness of the core of the fiber. Single-mode fibers are so thin that only a single light path is possible through the core.

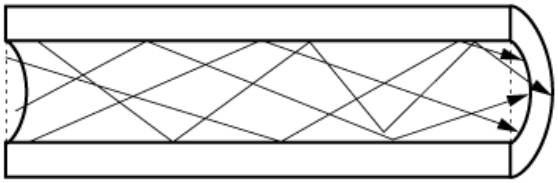

Figure 8-13. Optical Fiber Guides Light

Fiber Optic Cable Technology

The fiber does not have to be straight because of the characteristics of the fiber, the light tries to remain in the core of the fiber. The light diffraction (speckle) pattern and the light intensity at the end of the multi-mode fiber is a function of the shape of the fiber over its entire length. Even the slightest change in the shape of the fiber can be sensed using sophisticated sensors and computer signal processing at the far end (100 m or more). A single mode fiber can also be used as a sensor by splitting the light source and sending it both directions around a loop. If the fiber is disturbed, the two light sources come back in a different phase. The change in phasing relates to the amount of disturbance. Thus a single strand of fiber optic cable, buried in the ground at the depth of a few centimeters, can very effectively give an alarm when an intruder steps on the ground above the fiber. To ensure that an intruder steps above the fiber, it is usually woven into a grid and buried just beneath the surface. Fiber optic cables are most commonly used as fence disturbance sensors.

8.7.2 Fence-Associated Sensors

General Types

Three types of intrusion sensors either mount on or attach to a fence or form a fence using the transducer material:

- fence disturbance sensors
- sensor fences
- electric field or capacitance sensors.

8.7.2.1 Fence Disturbance Sensors

Description

Fence disturbance sensors are passive, visible, terrain-following sensors designed for installation on a security fence, typically constructed with chain-link mesh. These sensors are considered terrain following because the chain-link mesh is supported every 3 m with a galvanized steel post, and thus the fence itself is terrain following.

Mechanical Disturbances

Fence disturbance sensors respond to mechanical disturbances of the fence. Thus, they are intended to detect primarily an intruder who climbs on or cuts through the fence fabric. Several kinds of transducers are used to detect the movement or vibration of the fence. These include switches, electromechanical transducers, fiber optic cables, and strain sensitive cables.

Nuisance Alarms

Fence disturbance sensors respond to all mechanical disturbances of the fence, not just intruders. Common disturbances include strong winds, debris blown by wind, rain driven by wind, hail, and seismic activity from nearby traffic and machinery. Good fence construction, specifically rigid fence posts and tight fence fabric, is important to minimize nuisance alarms.

Defeat Methods

Fence disturbance sensors can be defeated by digging under the fence or bridging over the fence without touching the fence itself. Digging can be deterred by putting concrete under the fence. The bottom edge of the fabric can also be placed in the concrete, although this may be undesirable for corrosive environments where the fabric must be replaced frequently.

8.7.2.2 Sensor Fences

Description

Sensor fences are passive, visible, terrain-following sensors that make use of the transducer elements to form a fence itself. These sensor fences are designed primarily to detect climbing or cutting on the fence. Sensor fences tend to be much less susceptible to nuisance alarms than fence disturbance sensors. However, because sensor fences also have a plane of detection that is well defined, they are vulnerable to the same defeat methods as fence disturbance sensors.

Taut Wire Sensor Fences

Taut wire sensor fences consist of many parallel, horizontal wires with high tensile strength that are connected under tension to transducers near the midpoint of the wire span. These transducers detect deflection of the wires caused by an intruder cutting the wires, climbing on the wires to get over the fence, or separating the wires to climb through the fence. The wire is typically barbed wire, and the transducers are mechanical switches, strain

gages, or piezoelectric elements. Taut wire sensor fences can either be mounted on an existing set of fence posts or installed on an independent row of posts.

Fiber Optic, Mesh Fences

Fiber optics can be woven into a mesh that can be installed on a fence to create a sensor fence. These mesh fences usually use some type of continuity detection to determine when an intruder has cut through the fence. The upper portion of the fence is usually configured mechanically in such a manner that the fiber is crimped when an intruder attempts to climb over the fence. The crimp of the fiber reduces the amount of light passed through the fiber causing an alarm.

8.7.2.3 Electric Field or Capacitance

Description

Electric field or capacitance sensors are active, visible, terrain-following sensors that are designed to detect a change in capacitive coupling among a set of wires attached to, but electrically isolated from, a fence.

Sensitivity and Nuisance Alarms

The sensitivity of some electric field sensors can be adjusted to extend up to 1 m beyond the wire or plane of wires. A high sensitivity typically has a trade-off of more nuisance alarms. Electric field and capacitance sensors may be susceptible to lightning, rain, fence motion, and small animals. Ice storms may cause substantial breakage and damage to the wires and the standoff insulators. Good electrical grounding of electric field sensors is important to reduce nuisance alarms. Other metal objects (such as the chain-link fence) in the sensor field must also be well grounded; poor or intermittent grounds will cause nuisance alarms.

Defeat Methods

Because the detection volume extends beyond the fence plane, electric field sensors are more difficult than other fence-associated sensors to defeat by digging under or bridging over the fence.

Performance

Electric field or capacitance sensors can be mounted on their own set of posts. This results in two areas of improved performance: a wider detection volume for the sensitive electric field sensor, and a lower nuisance alarm rate by eliminating extraneous motion from the chain-link fence. For the freestanding version of electric field sensors, some electronic signal processing techniques employ additional wires in the horizontal plane to reduce the effects of distant lightning and alarms due to small animals.

8.7.3 Freestanding Sensors

General Types

The types of freestanding sensors currently used for exterior intrusion detection are

- active infrared (IR),
- bistatic microwave, and
- video motion detection sensors.

8.7.3.1 Active Infrared

Characteristics of Exterior IR Sensors

The infrared sensors used for exterior intrusion detection are active, visible, line of sight, and freestanding sensors.

How IR Sensors Work

An infrared beam is transmitted from an IR light-emitting diode through a collimating lens. This beam is received at the other end of the detection zone by a collecting lens that focuses the energy onto a photodiode. The IR sensor detects the loss of the received infrared energy when an opaque object blocks the beam. These sensors operate at a wavelength of about 0.9 microns, which is not visible to the human eye.

Although single-beam IR sensors are available, multiple-beam sensors are normally used for high-level security applications because a single IR beam is too easy to defeat or bypass. A multiple-beam IR sensor system typically consists of two vertical arrays of IR transmitter and receiver modules. The specific number and configuration of modules depends on the manufacturer. Thus the IR sensor creates an IR fence of multiple beams but detects a single beam break. Multiple beam sensors usually incorporate some type of logic that will detect if an intruder attempts to capture a receiver with an infrared source.

Nuisance Alarms

Conditions that reduce atmospheric visibility have the potential to block the IR beams and cause nuisance alarms. If the visibility between the two arrays is less than the distance between the two arrays, the system will probably produce a nuisance alarm. These conditions sometimes exist in fog, snow, and dust storms.

Defeat Methods

The detection volume cross section of a multiple-beam IR sensor is typically 5 cm wide and 2 m high. Thus IR sensors have a narrow plane of detection similar in dimensions to fence sensors: IR sensors are considered line of sight sensors and require a flat ground surface because the IR beam travels in a straight line. A convex ground surface will block the beam, and a concave surface will permit passing under the beam without detection. Digging under the bottom beam is possible unless a concrete sill or paved surface has been installed.

8.7.3.2 Passive Infrared

How PIR Sensors Work

Humans emit energy because of the warmth of their body. On the average, each active human emits the equivalent energy of a 50-watt light bulb, and passive infrared (PIR) detectors sense the presence of this energy and cause an alarm to be generated. For years this technology was only usable in an interior application because the changes in heat, emitted by the ground as clouds passed overhead, caused too many false alarms. Current models, however, as shown in Figure 8-14, compare the received thermal energy from two curtain-shaped sensing patterns. A human moving into one area and then the other would cause an imbalance. Weather changes should affect both areas equally and would not cause an alarm.

Nuisance Alarms and Detection Ranges

The passive infrared sensors should be mounted such that the motion of the intruder will most likely be across the line of sight, since that is the most sensitive direction. Nuisance alarms could be caused by blowing debris, animals, and birds. A phenomenon known as a "dust devil" can also cause nuisance alarms that are sometimes difficult to assess. A dust devil occurs in desert climates when the surface air becomes warmer than the air above and rises creating a whirlwind of air that can trap and carry dust and debris. The passive infrared detector is most sensitive when the background is at a much different temperature than an intruder. Detection ranges can exceed 100 m. Because these are optical devices, the only way to limit the maximum range is to aim the detector at a solid object, such as the ground, at the end of the desired detection zone. Detection may also be reduced during periods of heavy rain.

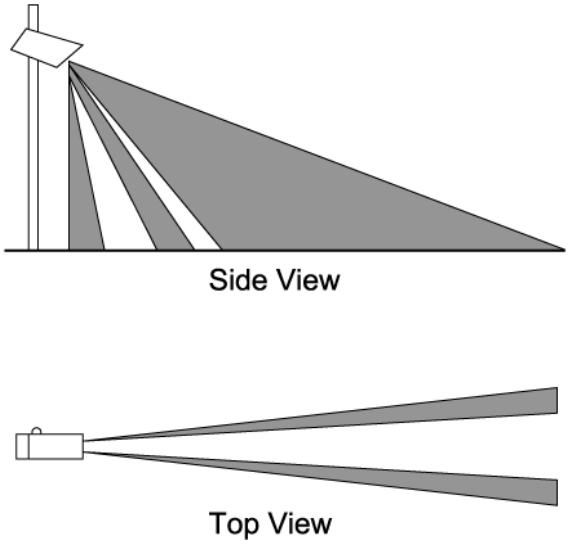

Figure 8-14. Passive Infrared Sensor

8.7.3.3 Bistatic Microwave

Description

Bistatic microwave sensors are active, visible, line of sight, freestanding sensors. Typically, two identical microwave antennas are installed at opposite ends of the detection zone. One is connected to a microwave transmitter that operates near 10 GHz or 24 GHz. Other frequencies may be available outside of the United States to comply with local regulations. The other is connected to a microwave receiver that detects the received microwave energy. This energy is the vector sum of the direct beam between the antennas and the microwave signals reflected from the ground surface and other objects in the transmitted beam. Microwave sensors respond to changes in the vector sum caused by objects moving in that portion of the transmitted beam that is within the viewing field of the receiver. This vector sum may actually increase or decrease, as the reflected signal may add in phase or out of phase.

How Microwave Sensors Work

Bistatic microwave sensors are often installed to detect a human crawling or rolling on the ground across the microwave beam, keeping the body parallel

to the beam. From this aspect the human body presents the smallest effective object to the bistatic microwave sensor. This has the following important consequences for the installation of microwave sensors:

- ***The ground surface must be flat*** so that the object is not shadowed from the microwave beam, precluding detection. The surface flatness specification for this case is +0, –15 cm. Even with this flatness, crawlers may not be detected if the distance between antennas is much greater than 120 m.

- ***A zone of no detection exists*** in the first few meters in front of the antennas. This distance from the antennae to the point of first crawler detection is called the "offset distance." Because of this offset distance, long perimeters where microwave sensors are configured to achieve a continuous line of detection require that the antennas overlap one another, rather than being adjacent to each other. An offset of 10 m is typically assumed for design purposes, thus adjacent sectors must overlap twice the offset distance of 20 m.

Detection Volume

The detection volume for bistatic microwave sensors varies with the manufacturer's antenna design but is large compared to most other intrusion sensors. The largest detection cross section is at midrange between the two antennas and is approximately 4 m wide and 3 m high.

Nuisance Alarms

Microwave sensors tolerate a wide range of environmental conditions without producing nuisance alarms. However, nuisance alarms can be produced by the following conditions:

- A nearby parallel ***chain-link fence with loose mesh that flexes in the wind*** will appear to the sensor as a large moving target.

- ***Surface water from rain or melting snow*** appears to the microwave sensor as a moving reflector; therefore, the flat plane required for crawler detection should have a cross slope for water drainage.

- ***Heavy blowing snow*** may produce nuisance alarms; snow accumulation will reduce the P_D, especially for the crawler; and complete burial of the antenna in snow will produce a constant alarm. The water content of the snow increases snow effects: dry light snow has less effect than heavy wet snow.

Defeat Methods

Defeats by bridging or digging under are not simply due to the extent of the detection volume. More sophisticated defeat methods involve the use of secondary transmitters.

Monostatic Microwave Detectors

Monostatic microwave detectors are also available. In this configuration, the transmitter and receiver are in the same unit. Radio frequency energy is pulsed from the transmitter and the receiver looks for a change in the reflected energy. Motion by an intruder causes the reflected energy to change and thus causes an alarm. These sensors are "range-gated" meaning

that the site can set the range beyond which motion can occur without an alarm. Monostatic microwave sensors have similar characteristics to bistatic sensors, although they are more affected by cross fences than parallel fences, and they are susceptible to re-aiming.

8.7.3.4 Dual Technology Sensors

Combine Sensors to Reduce Nuisance Alarms

In an effort to reduce nuisance alarms, dual technology sensors are becoming more popular for security use. An example of dual technology would be to place both a passive infrared and a monostatic microwave in the same housing. The device would not give an alarm until both sensors alarmed, thus avoiding common nuisance alarms from each of the technologies and only alarming on an actual intruder. In this mode the sensitivity of each sensor could be set very high without the associated nuisance alarms.

The detection probability of these sensors is lower than some of the other sensors since an intruder must only defeat one sensor technology to prevent an alarm from reporting and to bypass the detector.

8.7.3.5 Video Motion Detection

Description

Video motion detectors (VMDs) are passive, covert, line of sight sensors that process the video signal from closed-circuit television (CCTV) cameras. These cameras are generally installed on towers to view the scene of interest and may be jointly used for detection, surveillance, and alarm assessment. Lighting is required for continuous 24-hour operation.

How VMD Works

VMDs sense a change in the video signal level for some defined portion of the viewed scene. Depending on the application, this portion may be a large rectangle, a set of discrete points, or a rectangular grid. Some newer versions may do analysis on individual pixels. Detection of human body movement is reliable except during conditions of reduced visibility, such as fog, snow, and heavy rain.

Nuisance Alarms

Potential sources of nuisance alarms for VMD used outdoors include:

- apparent scene motion due to unstable camera mounts,
- changes in scene illumination caused by such things as cloud shadows, shiny reflectors, and vehicle headlights, and
- moving objects in the scene such as birds, animals, blowing debris, and precipitation on or near the camera.

Defeat Tactics

Defeat tactics include taking advantage of poor visibility conditions and camouflaging the target into the background.

8.7 Perimeter Sensor Systems

Integrating Sensors

This section discusses the integration of individual sensors into a perimeter

into a System

sensor system and considers the interaction of the perimeter system or subsystem with a balanced integrated physical protection system. Before the detailed design and implementation of a perimeter sensor system are considered, some basic design philosophy and concepts for perimeter sensor systems should be understood.

8.7.1 Design Concepts and Goals

Continuous Line of Detection

By definition, a perimeter is a closed line around some area that needs protection. A design goal is to have uniform detection around the entire length of the perimeter. This requires that sensors form a continuous line of detection around the perimeter. In practice this means configuring the sensor hardware so that the detection zone from one perimeter sector overlaps with the detection zones for the two adjacent sectors. Also, in areas where the primary sensor cannot be deployed properly, such as a gate, an alternate sensor is used to cover that gap.

Protection-in-Depth

As applied to perimeter sensor systems, the concept of protection-in-depth means the use of multiple lines of detection. Thus a minimum of two continuous lines of detection are used in high security systems. Many perimeter sensor systems have been installed with three sensor lines, and a few have four. For example, a perimeter sensor system might include a buried-line sensor, a fence-associated sensor, and a freestanding sensor. Multiple sensor lines provide duplicated detection, increased reliability, and in case of hardware failure, will fail safe. In this scheme, any single sensor can fail without jeopardizing the overall security of the facility being protected.

Complementary Sensors

Significantly better performance by the perimeter sensor system can be achieved by selecting different and complementary types of sensors for the multiple lines of detection. Complementary sensors enhance the overall system performance, expressed in terms of the three fundamental sensor characteristics:

- probability of detection,
- nuisance alarm rate, and
- vulnerability to defeat.

This implies that no two sensor lines will use the same technology. This design philosophy results in detection of a wider spectrum of targets, allows operation of at least one sensor line during any conceivable environmental disturbance, and increases the difficulty of the task for the covert intruder attempting to defeat the system.

8.7.1.1 Priority Schemes

Processing Nuisance Alarms

One disadvantage of multiple sensor lines is that more nuisance alarms will have to be processed. System effectiveness has not been increased if the system operator is overwhelmed with nuisance alarms. As discussed in the

session "Alarm Communication and Display," the probability of detection decreases as the time to assess alarms increases. The assessment subsystem should aid the operator in evaluating alarm information.

Using Computer Software to Prioritize Alarms

A recommended method for handling alarms requires the system operator to assess all alarms with the aid of a computer that establishes the time order of assessment for multiple simultaneous alarms. The computer sets a priority for each alarm based on the probability that an alarm event corresponds to a real intrusion. The alarms are displayed to the operator in order of decreasing priority; all alarms are eventually assessed. The alarm priority is established typically by taking into account the following:

- the number of sensors in alarm in a given sector,
- the time between alarms in the sector,
- the order in which the alarms occur in relation to the physical configuration of the sensors, and
- alarms in the two adjacent sectors.

8.7.1.2 Combination of Sensors

Strive to Improve Detection and Reduce Nuisance Alarms

It is desirable that a sensor or sensor system have

- a high probability of detection (P_D) for all expected types of intrusion, and
- a low nuisance alarm rate (NAR) for all expected environmental conditions.

No single exterior sensor presently available meets both of these criteria; all are limited in their detection capability and all have high NARs under certain environmental conditions.

Basic Techniques

The two basic techniques for combining sensors are

- OR combinations
- AND combinations

OR Combination

A system can consist of two or more sensors with their outputs combined by an OR gate so that an alarm would be generated when any sensor is activated. This combination is useful for sensors which make up for the deficiencies of each other; each sensor is intended to detect particular types of intrusions. Thus, sensors that detect above ground, overhead, and tunneling intrusions should be combined by an OR gate.

The nuisance alarm rate of the OR combination (NAR (OR)) will be the sum of the NAR of each sensor.

AND Combination

The nuisance alarm rate can be significantly reduced by combining sensors with an AND gate if the nuisance alarms of the sensors are not correlated. A seismic sensor and an electric field sensor do not give correlated alarms, for example, because they respond to different things. If both are activated at about the same time, it is probable that they have detected an intrusion. Since a single intrusion attempt will not activate two or more sensors simultaneously, a system can be designed to generate an alarm if two or more sensors are all activated within a preselected time interval. A long time interval is desirable to assure detection of intruders moving slowly, but if the interval is too long, the NAR may not be reduced enough. By installing sensors so they cover the same general area, thereby providing redundant coverage, the time interval can be kept small.

AND Combination and Vulnerability to Defeat

Detection probability of the AND combination (P_D(AND)) will be lower than the detection probability of each sensor. If an intruder can successfully defeat one sensor than the entire combination is defeated and will not alarm. To assure a reasonable detection probability for the system, the detection probability of the individual sensors must be high. AND combinations are seldom used in the exterior environment at high security facilities because of the vulnerability to defeat.

8.7.1.3 Clear Zone

Definition and Purpose

A clear zone is defined usually by two parallel fences extending the entire length of the perimeter. The fences are intended to keep people, animals, and vehicles out of the detection zone. The area between the fences is usually cleared of all above ground structures, including overhead utility lines; vegetation in this area is also removed. After the zone between the fences is cleared, only the detection and assessment hardware and associated power and data lines are installed in the area.

The purpose of the clear zone is to improve performance of the perimeter sensor system by:

- increasing detection probability,
- reducing nuisance alarms, and
- preventing defeat.

The clear zone also promotes good visual assessment of the causes of sensor alarms. A perimeter intrusion detection system performs better when it is located in an isolated clear zone.

8.7.1.4 Sensor Configuration

Combine Sensors to Improve Coverage

The configuration of the multiple sensors within the clear zone also affects the system performance. Overlapping the detection volumes of two different sensors within each sector enhances performance by creating a larger overall detection volume. Thus, defeat of the sensor pair is less probable because a larger volume must be bypassed or two different

technologies must be defeated simultaneously. A third sensor can even further enhance performance, not by overlapping with the first two, but by forming a separate line of detection. Physically separate lines of detection can reveal information useful for determining alarm priority during multiple simultaneous alarms. In particular, the order of alarms in a sector (or adjacent sectors) may correspond to the logical sequence for an intrusion.

8.7.1.5 Site-Specific System

Each Site Is Unique

Each site requiring physical protection has a unique combination of configuration and physical environment. Thus, a physical protection system designed for one site cannot be transferred to another.

Factors that Help Determine Which Sensors Will be Appropriate

The following factors generally help determine the appropriate set of sensors:

- ***the physical environment*** will influence the selection of types of sensors for perimeter sensor systems.
- ***the natural and industrial environments*** provide the nuisance alarm sources for the specific site.
- ***the topography of the perimeter*** determines the shapes and sizes of the space available for detection, specifically the clear zone width and the existence of flat or irregular terrain.

Although the understanding of the interaction between intrusion sensors and the environment has increased significantly in recent years, it is still advisable to set up a demonstration sector on site using the possible sensors before making a commitment to a complete system. This test sector located on site is intended to confirm sensor selection and to help refine the final system design.

8.7.1.6 Tamper Indication

Features of Tamper Indication

The hardware and system design should incorporate features that detect or indicate tampering, as follows:

- Sensor electronics and junction box enclosures should have tamper switches that alarm if opened.
- Aboveground power and signal cables should be installed inside metal conduit. Signal boxes containing important equipment should be metal rather than plastic.
- Alarm communication lines should use some type of line supervision that detects lines that have been cut, disconnected, short-circuited, or bypassed.
- To reduce vulnerability to defeat, place bistatic sensors so that an intruder must be in or pass through the detection volume to approach the receiver.

8.7.1.7 Self-Test

Manual and Remote Testing Capabilities

To verify normal operation of a perimeter sensor system, its ability to detect must be tested regularly. Although manual testing is recommended, man-power requirements are usually restrictive. A capability for remote testing of trigger signals can be provided and initiated by the alarm communication and control system. Typically this is just a switch closure or opening. In an automatic remote test procedure, the central computer control system generates at a random time a test trigger to a given sensor. The sensor must then respond with an alarm. The control system checks that an alarm occurred within a specified time and cleared within another specified time. Failure to pass the test indicates a hardware failure or tampering and produces an alarm message. Current self-test techniques may identify that the sensor is still working, but do not test the sensor thoroughly enough to verify the calibration or aiming, so remote self-test should supplement, not replace, performance testing.

8.7.2 Effects of Physical and Environmental Conditions

Types of Physical and Environmental Conditions That Affect Sensors

The physical and environmental conditions that can affect exterior detection systems include

- topography
- vegetation
- wildlife
- background noise
- climate and weather
- soil and pavement.

These conditions are different at every site.

Topography

Topographic features such as gullies, slopes, lakes, rivers and swamps must be considered when designing an exterior detection system. Grading may be required to reduce hills and slopes. Draining may also be required to reduce water flow through gullies and ditches to prevent seismic disturbances caused by running water. The perimeter system should avoid lakes, rivers, and swamps, since there are few commercial sensors suitable for use in water.

Vegetation

Sensor performance can be affected by vegetation in two ways: underground and above ground. Motion of trees or plants caused by wind may be transmitted to their root systems and cause a seismic sensor to generate a nuisance alarm. Above ground, large plants and trees can be used as cover by an intruder. If vegetation is a problem, it must be controlled by mowing, removal, soil sterilization or surfacing.

Wildlife

In some locations, wildlife may cause some problems. Large animals may

damage equipment by collision and burrowing animals may eat through cable insulation material. Small animals, burrowing animals, birds, and insects also cause nuisance alarms that may be difficult to assess. Dual chain-link fences and chemical controls may be used to control wildlife; however, local regulations should be observed with regard to poisons and repellents. Removing vegetation from fence lines has been found to discourage some smaller animals.

Background Noise

A site survey along with information obtained from utility companies and plant engineering organizations on site may reveal many sources of background noise. These sources may include wind, traffic, electromagnetic interference, and seismic sources:

1. ***Wind***. Disturbances related to wind are caused by the transfer of energy to the ground by trees, power and light poles, fences, etc. High winds and wind-blown debris can also cause nuisance alarms from sensors mounted on fences by disturbing the fence.

2. ***Traffic*** from nearby roadways, railways, and airports creates nuisance alarms from seismic sensors. Roads should be kept smooth and the speed limit at a minimum to reduce the nuisance alarm rate. Seismic sensors are not practical near heavy air or railway traffic, because this type of traffic causes seismic disturbances even at long distances.

3. Examples of sources of ***electromagnetic interference*** include lightning, radio transmitters, welding, and electrical transients. Shielding of the sources or the sensors can reduce nuisance alarms.

Climate and Weather

Specific data about the climate and the weather conditions should be obtained for the site. Information such as frequency, velocity, accumulation and duration should be obtained about hail, electrical storms, rainfall, and wind. Mean minimum and maximum temperatures should also be noted as well as other weather and environmental conditions.

Soil and Pavement

Soil and pavement conditions can affect the operation of buried seismic sensors. The seismic conductivity of the medium is the determining factor. It should be high enough to make seismic sensors effective, but not so high that it causes nuisance alarms. Wet soil tends to have exceptionally good seismic conduction. However, wet soil tends to respond strongly to distant sources of seismic activity and thus cause excessive nuisance alarms. Buried systems of seismic magnetic sensors and seismic sensors may have to be embedded in or installed under areas paved with concrete or asphalt. The sensitivity of a sensor embedded in the pavement is increased if the sensor is adequately coupled to the medium. If the sensor is not adequately coupled to the medium, its sensitivity may be much lower than when it is installed in soil or buried under the pavement.

Reducing Lightning Damage

Because exterior sensors are installed outdoors, they are exposed to electrical storms at most sites. Lightning can easily disable, damage, or destroy the sensitive electronics used in sensor equipment. There are three primary precautions for reducing lightning damage. First, all signal cables

should be shielded, either by the internal cable construction or by using metal conduit. Second, a good ground system is required. This means eliminating ground loops and using grounds at a single point. Third, passive transient suppression devices can be installed at the ends of the cables. Fiber-optic transmission cables are not affected by lightning and have thus become very popular for transmitting signals long distances outside a building.

8.7.3 Integration With Video Assessment System

Compatibility

Many perimeter security systems use a CCTV system to perform alarm assessment. For both the sensor and video systems to perform well, care must be taken to ensure that the designs of the two systems or subsystems are compatible.

Clear Zone

One consideration is the width of the clear zone. Sensor engineers desire a wide area for installing their sensors to reduce nuisance alarms. Video engineers desire a narrow area to assess so that they can achieve better resolution from the cameras. A compromise clear zone width is in the range of 10 to 15 m.

Location of Camera Towers

Another trade-off is the location of the camera tower within the clear zone. The camera must be positioned to view the entire area being assessed. The sensors must be placed far enough away from the camera towers to prevent distortion of the detection volume and nuisance alarms. Frequently the camera towers are located 1 to 2 m inside the outer fence of the clear zone.

8.7.4 Integration With Barrier Delay System

Delay Time Allows Video Assessment

Balanced integrated physical protection systems usually incorporate some type of barrier or access denial systems to provide delay time for video assessment of the alarm source and for the response force to respond to an intrusion. In many cases, this includes some type of barrier installed at the perimeter; however, the barrier should not degrade the performance of the sensors.

Barrier Placement

Perimeter barriers are usually installed on or near the inner clear zone fence so that an intruder cannot tamper with or defeat the barrier without first passing through the detection zone. This placement is important to ensure that the response action is initiated before the delay occurs. Barriers should not distort the sensors' detection volume, cause nuisance alarms, or obscure part of the camera's view.

8.9 Extended Detection or Early Warning Sensors

Early Warning Systems Development

Sensors being investigated as early warning systems have been, primarily, developed for quickly deployable, tactical, applications. In a battlefield environment, early warning of an adversary's approach has obvious advantages. As the threat to domestic facilities has increased, the desire to become aware of the presence of an intruder sooner has increased. Early

detection of the adversary provides the protective force more time to preposition themselves or to engage the potential threat prior to reaching the area of interest.

There are a variety of exterior intrusion sensors and sensor combinations that have been deployed in tactical environments and are now being evaluated for application in a fixed location. These technologies include long and short range ground surveillance radar, scanning thermal imaging, and laser radar. The effective range of these systems varies from hundreds of meters to tens of kilometers.

"Sensor Fusion" is a technology capability that is being developed to improve intrusion detection in remote areas. This concept uses existing sensor technologies (IR, seismic, magnatometer, etc.) "fused" to each other using software that either requires multiple sensors to be activated in a logical sequence or uses a predefined weighted sum of the reporting sensors to help reduce nuisance sources while maintaining effective detection. The deployment locations would include areas outside the facility not within line-of-site of other sensors and assessment systems. The devices are designed to be covert and totally self-contained requiring minimal or no maintenance for long periods of time. The sensor nodes will communicate with the monitoring station via wireless link using a self-healing network scheme.

Effectiveness Criteria

In order to be effective, early warning systems should have similar performance measures as those required for traditional exterior sensors. These performance measures include probability of detection, nuisance alarm rates, degradation factors, vulnerability to defeat and manning requirements. Objectively determining these performance measures is a challenge given the nature of these systems and the large areas they can potentially cover. Performance can be expected to vary depending on site specific factors such as environment and topography. Specific criteria for detection and nuisance alarm rates are still being determined for these types of sensors.

Specific Challenges for EWS

Most of these systems require a line of site from the sensor to the target and operate most effectively in open areas with minimum vegetation. The systems will detect wildlife and wind-induced movement of vegetation within its field of view. In areas where wildlife activity is high and/or vegetation is abundant, the nuisance alarm rate can be high. To be most effective, the system itself should have detection range-limiting settings and functions, or masking capabilities, in order to ignore alarms from movement in populated areas outside the desired detection area.

Most of the systems require a dedicated operator to monitor the display to look for target data that can be interpreted by the operator to indicate purposeful movement within the scanned area. The addition of this operator can add significant expense to the operations budget of the facility. For systems that operate using multiple "Early Warning" technologies, issues arise with assessing and determining intent of multiple targets without over-committing response forces.

Assessment cameras (both visible light and thermal imagers) have been integrated with some of the systems; however, reliable assessment remains a challenge, particularly for targets detected at greater distances. To address this issue, there have been numerous developments and improvements in systems to assess a target at these distances. The developments have largely been in the areas of high resolution cameras using infrared or laser illuminator devices for nighttime assessment and thermal imagers. Evaluation of these systems is ongoing.

When compared to traditional perimeter security systems, the purchase price of these devices can be quite high, ranging from $40K to $250K per unit. In addition, the cost of maintenance, training, and operation must also be considered. These issues, and the fact that their expansion into this market has been fairly recent, means that the systems have not been thoroughly tested for performance capabilities and effectiveness in fixed site applications.

8.10 Summary

Create a Balanced PPS

Interior intrusion detection sensors have been discussed in terms of application, probability of detection, nuisance alarm rate, and vulnerability to defeat. The integration of individual sensors into an interior sensor system must consider the skill level of the intruder, the design goals, the effects of environmental conditions, as well as the interaction of the interior system with a balanced and integrated physical protection system.

Exterior intrusion detection sensors have been discussed in terms of application, probability of detection, nuisance alarm rate, and vulnerability to defeat. The designer integrating individual sensors into a perimeter sensor system must consider specific design goals, the effects of physical and environmental conditions, and the interaction of the perimeter system with a balanced and integrated physical protection system.