NUREG/CR–5722
SAND91–0948

Interior Intrusion Detection Systems

Received by OSTI
NOV 21 1991

Prepared by
J. R. Rodriguez/SNL
B. Dry/BEI
J. C. Matter/SNL

Sandia National Laboratories

BE Inc.

Prepared for
U.S. Nuclear Regulatory Commission

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555

2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082

3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC bulletins, circulars, information notices, inspection and investigation notices; licensee event reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grant publications, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG-series reports and technical reports prepared by other Federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions. *Federal Register* notices, Federal and State legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

DISCLAIMER NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability of responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

NUREG/CR--5722

TI92 003139

Interior Intrusion Detection Systems

Manuscript Completed: September 1991
Date Published: October 1991

Prepared by
J. R. Rodriguez, Sandia National Laboratories
B. Dry, BE Inc.
J. C. Matter, Sandia National Laboratories

Sandia National Laboratories
Albuquerque, NM 87185

Subcontractor:
BE Inc.
P.O. Box 381
Hwy. 278, Airport Industrial Park
Barnwell, SC 29812

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Prepared for
Division of Safeguards and Transportation
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555
NRC FIN L1387

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

ABSTRACT

The purpose of this NUREG is to present technical information that should be useful to NRC licensees in designing interior intrusion detection systems. Interior intrusion sensors are discussed according to their primary application: boundary-penetration detection, volumetric detection, and point protection. Information necessary for implementation of an effective interior intrusion detection system is presented, including principles of operation, performance characteristics and guidelines for design, procurement, installation, testing, and maintenance. A glossary of sensor terms is included.

CONTENTS

FIGURES

TABLES

INTRODUCTION

U.S. Nuclear Regulatory Commission (NRC) regulations under Part 73 "Physical Protection of Plants and Material" of Title 10, Code of Federal Regulations, specify performance requirements for the physical protection of special nuclear materials and associated facilities. For fuel cycle facilities using or possessing a formula quantity of strategic special nuclear material, paragraph 73.45(c)(1)(iii) calls for the use of detection and surveillance subsystems and procedures to discover and assess unauthorized activities and conditions and communicate them so that response can stop the activity or correct the conditions. For these facilities, an example reference system is outlined in paragraph 73.46. Paragraph 73.46(e)(3), in part, calls for all unoccupied vital areas and material access areas to be locked and protected by an intrusion alarm subsystem which will alarm upon the entry of a person anywhere into the area, upon exit from the area, and upon movement of an individual within the area, except that for process material access areas only the location of the strategic special nuclear material within the area is required to be so alarmed.

The purpose of this NUREG is to present technical information that may be of use to a licensee in assembling an interior intrusion detection system. By virtue of the nature of a NUREG document, the discussion of equipment or systems, herein, does not constitute acceptance or endorsement by the NRC.

1 INTERIOR INTRUSION AND PHYSICAL PROTECTION

The objective of a physical protection system (PPS) is to deter or prevent intrusion into a sensitive fixed-site facility through detection, delay, and response. Interior intrusion detection is part of the detection function of a PPS. The specific objective of interior intrusion detection, as addressed in this NUREG, is to detect an unauthorized intrusion into a building or a room within a fixed-site facility.

The report begins with an overview of PPS concepts. Interior intrusion sensors are then discussed according to their primary applications: boundary-penetration detection, volumetric detection, and point protection. Finally, information necessary for implementation of an effective interior intrusion detection system (IIDS) is presented, including guidelines for sensor procurement, installation, and maintenance and principles of system design.

Technical terms and words having specialized meanings for the purpose of the NUREG have been included in the glossary. The glossary also includes acronyms, initialisms, and abbreviations found in the body of the report.

2 THE PHYSICAL PROTECTION SYSTEM

Section 2 addresses the basic design concepts of a PPS (physical protection system) and shows how an IIDS (interior intrusion detection subsystem) relates to its other physical protection subsystems.

2.1 Physical Protection System Concepts

A fixed-site safeguards system provides physical protection against hostile acts, such as theft of special nuclear material (SNM). Three elements, which should interact in a timely manner, form the foundation for an effective PPS:

- *Detection* systems detect and verify unauthorized intrusion attempts by individuals or serious malevolent acts by insiders or outsiders.
- *Delay* systems impede adversary penetration into or exit from the area under protection.
- *Response* systems or forces counteract adversary activity and contain the threat.

These elements are equally important, and none of them can be eliminated or compromised in an effective PPS. Detection, which encompasses not only intrusion detection and assessment but also entry control, is an important element because any delay system can eventually be penetrated; and without detection the response force would not be alerted. Delay elements should provide sufficient time after detection to allow the response force to arrive before the intruder's mission can be completed. Finally, the response force should be adequately prepared to contain the adversary actions.

Intrusion detection system (IDS) hardware consists of sensors, alarm assessment systems, and alarm reporting systems, including alarm communication and display equipment. The factors that should be considered along with the hardware to produce an effective IDS are shown in Figure 2-1. The performance of the sensing and assessment equipment is heavily influenced by the physical environment in which it operates and by installation and maintenance practices. To determine correlation between a sensor's operation and the physical environment, on-site evaluation may be required before, during, and after installation. The type of facility or material to be protected and the most likely threat, including intruder attributes, should be considered along with the hardware to produce an effective IDS. Regulations, procedures, and personnel should be evaluated in order to establish an operationally effective IDS.

Intrusion detection systems can be associated with a barrier system so that attempts to penetrate the barrier result in an alarm. An interface with entry control systems to allow authorized activity at a facility is also necessary. Perimeter subsystems are used to detect penetration of barriers and isolation zones that form the perimeter of an area under protection, a protected building, or a fixed-site facility. An interior intrusion detection system, shown diagrammatically in Figure 2-2, detects penetration into a structure, detects movement within a structure, or provides knowledge of contact with a critical or sensitive item.

2.2 Intrusion Detection System Integration

Intrusion detection system integration is the process of interfacing the various individual elements, procedures, and personnel into one system for providing intrusion detection at a facility. The expression "operationally effective" is used to describe systems that have achieved a reasonable balance between being understood, accepted, and efficiently used by security personnel and providing a sufficient degree of detection capability at the facility.

Careful planning and analysis of a new or to-be-improved IDS ensures that it will perform reliably and that the system's strengths and weaknesses are identified and understood. To this end, it is important to have a firm understanding of the total PPS.

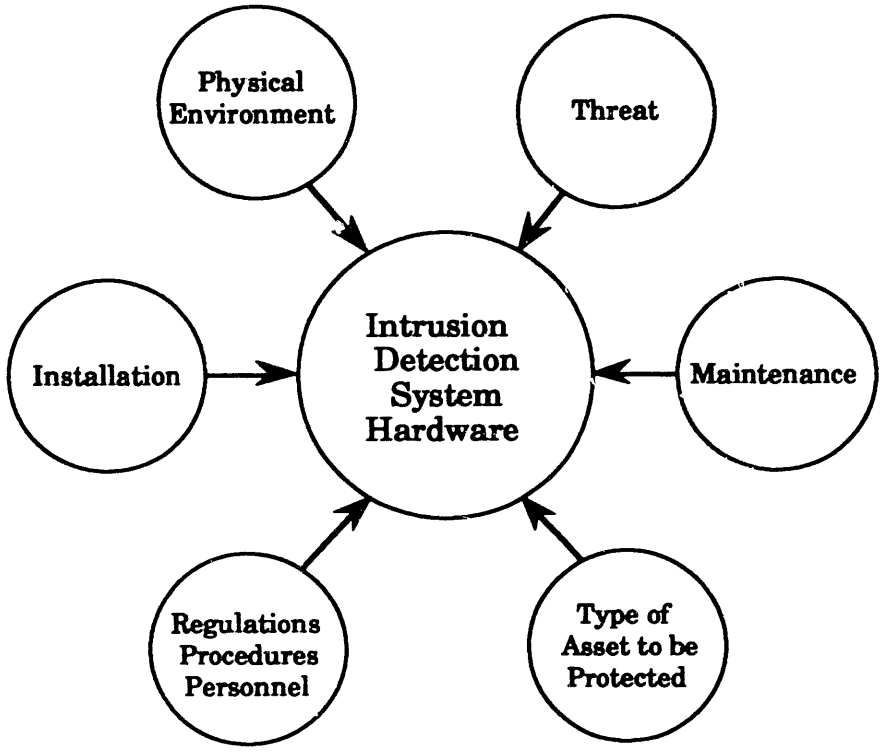


Figure 2-1. Factors that influence intrusion detection system design

Physical security requires a balance among hardware, personnel, and operating procedures. An efficient PPS exercises this balance and does not use hardware to solve security problems that could be more efficiently solved by simple operational procedures.

Applicable security regulations should be obtained and thoroughly understood before planning the PPS upgrade or installation. The threat to the site should be well defined. The functions of the various elements of the planned security system should be examined to see how well the defined threats are countered. Such examination requires an iterative design process.

A balanced and effective IDS has many elements that should be properly integrated with each other, with any new security procedures, and with the facility operation. Figure 2-3 shows some of the equipment that should be integrated. The sensors comprising the first block should be selected and configured so that they form a complementary and effective detection system. The need for power, alarm- and tamper-communication, and self-test implementation calls for careful consideration of the power distribution system and of the alarm processing and communication system. The assessment devices in the second block should be selected and installed with consideration for each other. Integrating the IDS subsystem smoothly with the communication subsystem involves selection of signal routing media and signal conditioning media. The IDS should also be integrated with the display and control subsystem, with the entry-control subsystem, with the barriers, and with other elements. Many details should be designed to accommodate the various subsystems.

2.3 Physical Protection System Design Philosophy

Section 2.3 addresses a design philosophy for a total PPS. In designing a PPS, the general concepts to be addressed include

- target identification
- characterization of threat

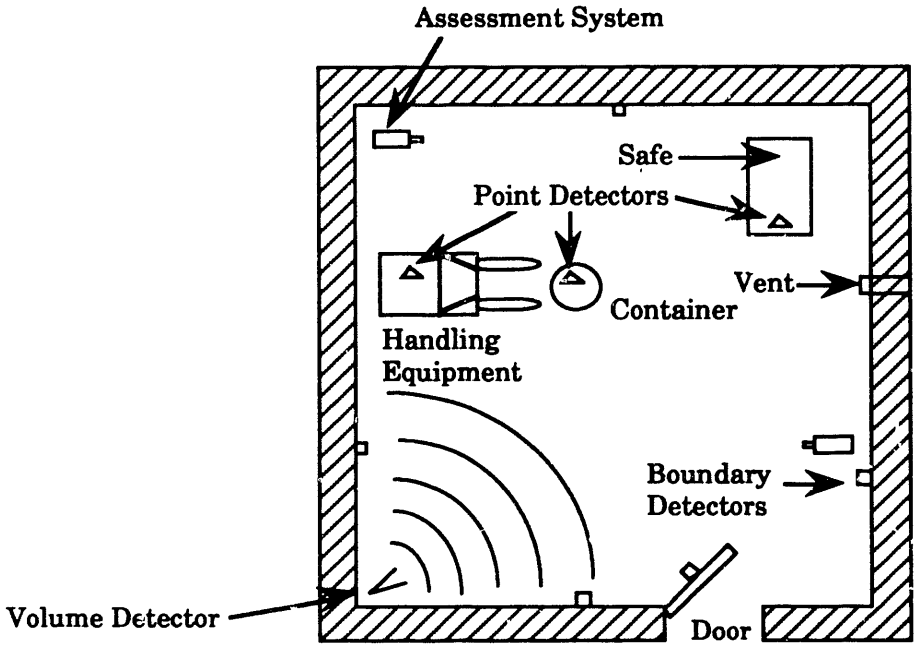


Figure 2-2. Typical relationship of an interior intrusion detection system with barriers

- interaction of detection, delay, and response
- concept of protection in depth

2.3.1 Target Identification

The target identification process can be very simple or complicated depending on the nature of the facility and the materials in the facility. If the theft targets are discrete items, then a simple listing of the locations to protect may be all that is needed. In these cases, the targets are often obvious to the security analyst.

When a facility is complex and the sensitive material is dispersed, such as bulk material in process, much more complicated analytical techniques are required to identify targets. For facilities of a standard design, most of the analytical work often exists; however, for unique, large, complex facilities, this step in the overall physical protection system design can be a major effort.

2.3.2 Threat Characterization

The NRC's design basis threat statement for fuel cycle facilities using or possessing a formula quantity of strategic special nuclear material is contained in paragraph (a)(2) of 10 CFR 73.1. The postulated threat is described as:

A. A determined violent, external assault; attack by stealth; or deceptive actions by a small group with the following attributes, assistance, and equipment:
   1. Well-trained (including military training and skills) and dedicated individuals;
   2. Inside assistance that may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both;
   3. Suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and effective long-range accuracy;

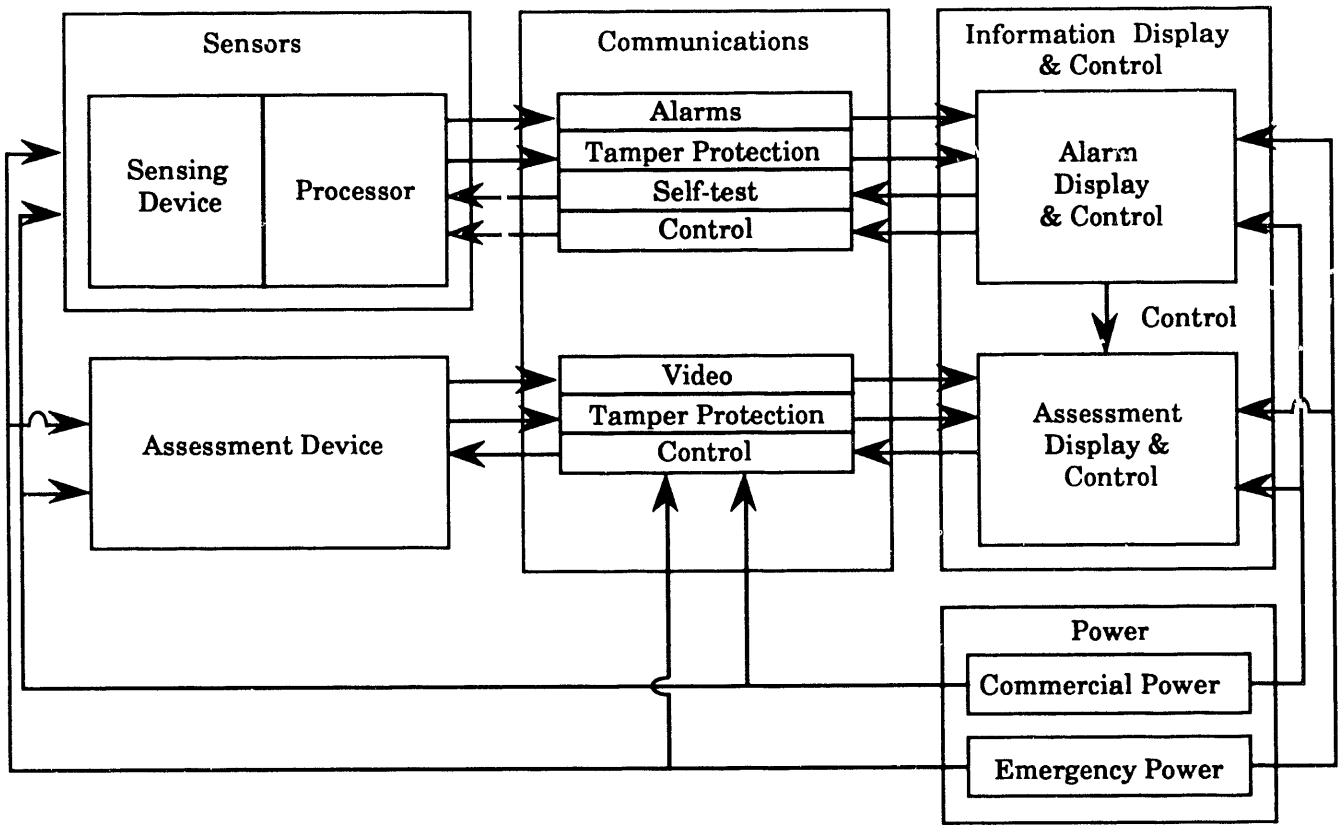


Figure 2-3. Intrusion detection system hardware

4. Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system;
5. Land vehicles used for transporting personnel and their hand-carried equipment; and
6. the ability to operate as two or more teams

B. An individual, including an employee (in any position), and

C. A conspiracy between individuals in any position who may have:
1. Access to and detailed knowledge of nuclear power plants or the facilities referred to in section 73.20(a), or
2. Items that could facilitate theft of special nuclear material (e.g., small tools, substitute material, false documents, etc.), or both.

2.3.3 Detection, Delay, and Response

In designing an effective physical protection system, balance among detection, delay, and response is essential. The best detection system is worthless without delay and response. Likewise, the best response force will be ineffective if, once detected, the adversary is not delayed sufficiently for the arrival of the force. In the same vein, an effective detection system, coupled with adequate barriers, may result in an overall poor system if the response force consists of only a few persons who have a long response time.

2.3.4 Protection in Depth

Protection in depth is a concept involving a number of distinct protection measures that the adversary should defeat in sequence in order to be successful. Protection in depth can be achieved by surrounding the critical item or facility with layers or zones containing detection systems and delay barriers as shown in Figure 2-4. It may be desirable to make these zones more difficult to defeat as they are located closer to the critical item or facility.

Other considerations that should be included in the system to provide protection in depth are the backup systems, including the fail-soft concept and the redundancy, or fail-safe, concept. Fail soft refers to the capability of the physical protection system to operate, perhaps in a reduced capacity, during a failure of some element in the system. Redundancy, as the name implies, refers to the use of more than one of each type of critical element. Therefore, if one of these essential elements fails, there is a backup to keep the system operational. Associated with this is the need to eliminate or at least to recognize and take appropriate measures to protect single points of failure or defeat; for example, it is necessary to avoid routing sensor communication cables through unsecured portions of the building, such as utility rooms, where construction or an intruder could cut the cables at a single location, resulting in the total loss of alarm communication.

2.4 Physical Protection System Design Methodology

PPS design is an iterative process that can be divided into several phases. All phases include the following activities:

- characterization of a facility
- identification of zones in the facility that require protection

In the various phases, these activities differ only in degree. In early conceptual phases, facility descriptions lack detail, and PPS definition and effectiveness estimates are consequently limited. As more facility details are considered in later phases, PPS definitions are more complete, and cost and

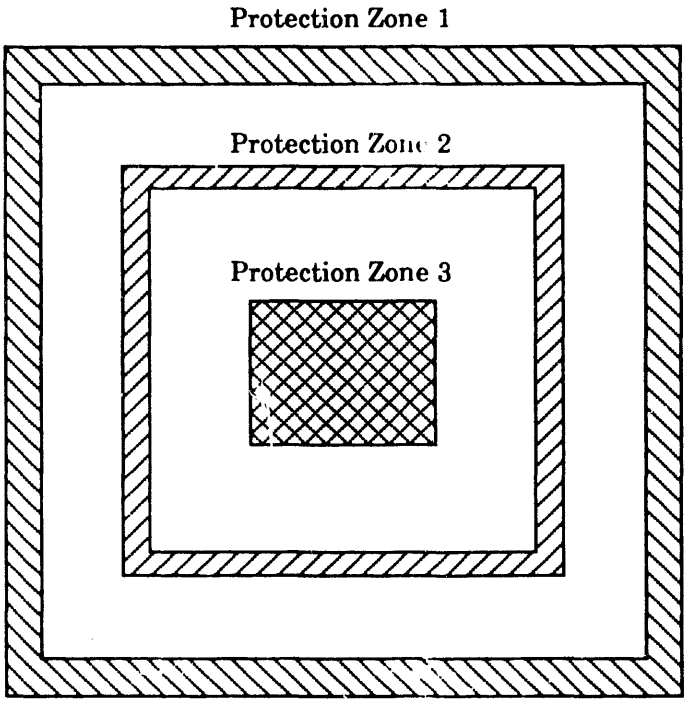


Figure 2-4. Protection in depth concept

effectiveness estimates can be more precise. After a limited, initial examination of many options, less attractive options can be discarded before moving to the more detailed, time-consuming design phases.

2.4.1 Facility Characterization

The first step in the development of a PPS is facility characterization. Building plans are required showing the details of exterior and interior building construction, including basement and roof, plus all types of doors, other openings such as windows and ventilation ducts, utility rooms and passages, and elevators and stairways. Details of facility operations are also required. These details include

- nuclear material input, location, output, and flow rates
- personnel staffing levels, shift patterns, and access requirements
- existing procedures for normal operations, security, material control and accountability, maintenance, and emergency management

2.4.2 Protection Zone Definition

The facility characterization is reviewed to identify areas that require protection, to identify protection concerns within those areas, and to determine potential consequences of adversary activity within the identified areas. Protection concerns include actions that would result in loss of SNM, long-term diversion of small amounts of SNM, and theft of large amounts of SNM. The identification of areas within the facility that require protection is an essential task. Protection zones can be defined as contiguous areas having common protection requirements. For example, areas in which SNM is equally accessible could be combined into one zone. Other protection zones might include areas containing only critical equipment.

Physical protection techniques and associated procedures are selected to protect all identified zones. Design requirements include

- isolating SNM and critical equipment from unauthorized people, with a minimum operational impact
- requiring unauthorized people to pass through several barriers and detectors to reach SNM or vital systems in the protection zones
- controlling all authorized activity in order to detect and stop employee actions that could pose a threat
- providing protection during emergency and maintenance situations

Each protection measure is reviewed to assure compatibility with health, safety, material accounting, and operational requirements. Alternatives are pursued until all requirements can be met. It may be necessary to revise the protection zones or to modify the facility. For example, in some facilities a completely controlled emergency evacuation system is necessary to protect adequately against the threat of theft by an insider and to still meet safety requirements.

3 INTERIOR INTRUSION SENSORS

The design of an effective IIDS (interior intrusion detection system) calls for a thorough knowledge of the operational, physical, and environmental characteristics of the facility to be protected. In addition the designer should be familiar with the broad spectrum of sensors available, the physical principles by which each sensor operates, their strengths and weaknesses, and the means by which the sensors interact with the intruder and with the environment.

Section 3 addresses the basic principles that apply to all interior intrusion sensors. The following sections address specific sensors, grouped according to their applications. Boundary penetration sensors (Section 4) are designed to detect intruder-penetration of the area under protection boundary; volumetric sensors (Section 5) detect the motion of an intruder within a confined interior volume; and point sensors (Section 6) detect the presence of an intruder at the protected object itself.

3.1 Performance Characteristics

Individual sensor performance can be described by three basic characteristics:

1. probability of detection (P_d)
2. nuisance alarm rate (NAR)
3. vulnerability to defeat

All three characteristics are highly dependent on the distinctive features of the specific sensor, the methods of installation and adjustment, the manner in which the equipment is interconnected with the system, and the environment in which the equipment is operated.

3.1.1 Probability of Detection (P_d)

The probability of detection (P_d) is defined as the likelihood of detecting an adversary within the zone covered by an intrusion sensor. The ideal P_d is 1.0, representing 100 percent probability of detection. Many factors contribute to a less than ideal P_d, including the behavior and physical characteristics of the target intruder; the sensor's basic design, installation method, sensitivity adjustments, and equipment condition; and the characteristics of the sensor's ambient environment. The inability to standardize such factors makes impossible assigning a single P_d to a specific sensor.

3.1.2 Nuisance Alarm Rate (NAR)

Nonadversary-related sensor alarms can be categorized as nuisance alarms, unknown alarms, and false alarms. Nuisance alarms are produced by sensors in response to a known stimulus unrelated to an intrusion attempt. Such alarms may be generated by authorized personnel, vehicles, or activities in the sensor vicinity. Thermal, acoustic, and electromagnetic interference also cause nuisance alarms. Unknown alarms are alarms for which the cause is unidentified. Expending a reasonable effort to identify the causes of all alarms keeps the number of unknown alarms low. False alarms, alarms caused by internal equipment malfunction, have no readily assessable cause, so they are actually unknown alarms. In this report nuisance alarms, unknown alarms, and false alarms are all included in the term "nuisance alarm."

The NAR for a sensor is coupled to its P_d. A trade-off should be made between an acceptably high Pd and a tolerably high NAR. An acceptable nuisance alarm rate (NAR), expressed as number of alarms per unit of time, depends heavily on the system's ability to identify the source of each alarm. Since a high NAR undermines confidence in the system, the system design should eliminate as many sources of nuisance alarms as possible.

3.1.3 Vulnerability to Defeat

Probability of detection, nuisance alarm rate, and vulnerability to defeat are all measures of the quality of a sensor. A sensor exhibiting an acceptable NAR and P_d is not suitable for application in a situation where it is vulnerable to defeat.

Two basic modes of defeating a sensor are spoof and bypass. Spoof refers to defeat methods that employ equipment and actions to mask the intruder's signal or to inhibit the electronics from producing an alarm during an intrusion through the sensor's detection zone. Bypass refers to an intruder's ability to avoid the sensor's detection zone.

Vulnerability to defeat can be diminished by the use of tamper alarms, anticapture circuitry, line supervision, and full end-to-end self-test capability. The intrusion-detection system design can contribute to a reduced vulnerability to defeat through such features as overlapping detection zones to provide mutual protection and by employing point sensors to enhance marginal detection locations in the sensor zone.

3.2 Sensor Classification

Interior intrusion sensors are discussed in this report according to three methods of classification:

- passive/active
- mode of application
- covert or visible

Table 7-1 in Section 7 tabulates these classifications for the sensors described in this NUREG.

3.2.1 Active versus Passive Sensors

An interior intrusion sensor may be classified as active or passive relative to its interaction with the environment, as illustrated in Figure 3-1. An active sensor emits a signal from a transmitter and employs a receiver to detect changes in the signal caused by the presence or motion of an intruder. If the transmitter and the receiver are situated in separate locations, the installation is called bistatic. If they are collocated, the installation is called monostatic.

A passive sensor produces no signal but simply detects energy emitted in the proximity of the sensor or detects the perturbation of a natural field of energy. The detected energy may be vibrational, from a man walking or from a truck; infrared, from a man or an animal or from the sun; acoustic, sounds from a destructive boundary penetration; or it may be the result of a change in the mechanical configuration of the sensor, such as occurs in the simple electromechanical sensors. Multiple passive sensors may be placed in a volume without interaction, since no signals are emitted.

The distinction between passive and active sensors has practical importance in some applications. The presence and/or location of a passive sensor is more difficult to ascertain than that of an active sensor, thus putting an intruder at a disadvantage. In environments containing explosive vapors or materials, passive sensors are safer than active sensors because no potentially explosion-initiating energy is emitted. However, signal processing techniques for active sensors are generally more effective at discriminating against nuisance alarm sources than are such techniques for passive sensors.

3.2.2 Mode of Application

The application of an interior intrusion sensor usually occurs in one of three categories:

- boundary-penetration detection
- volumetric detection
- point protection

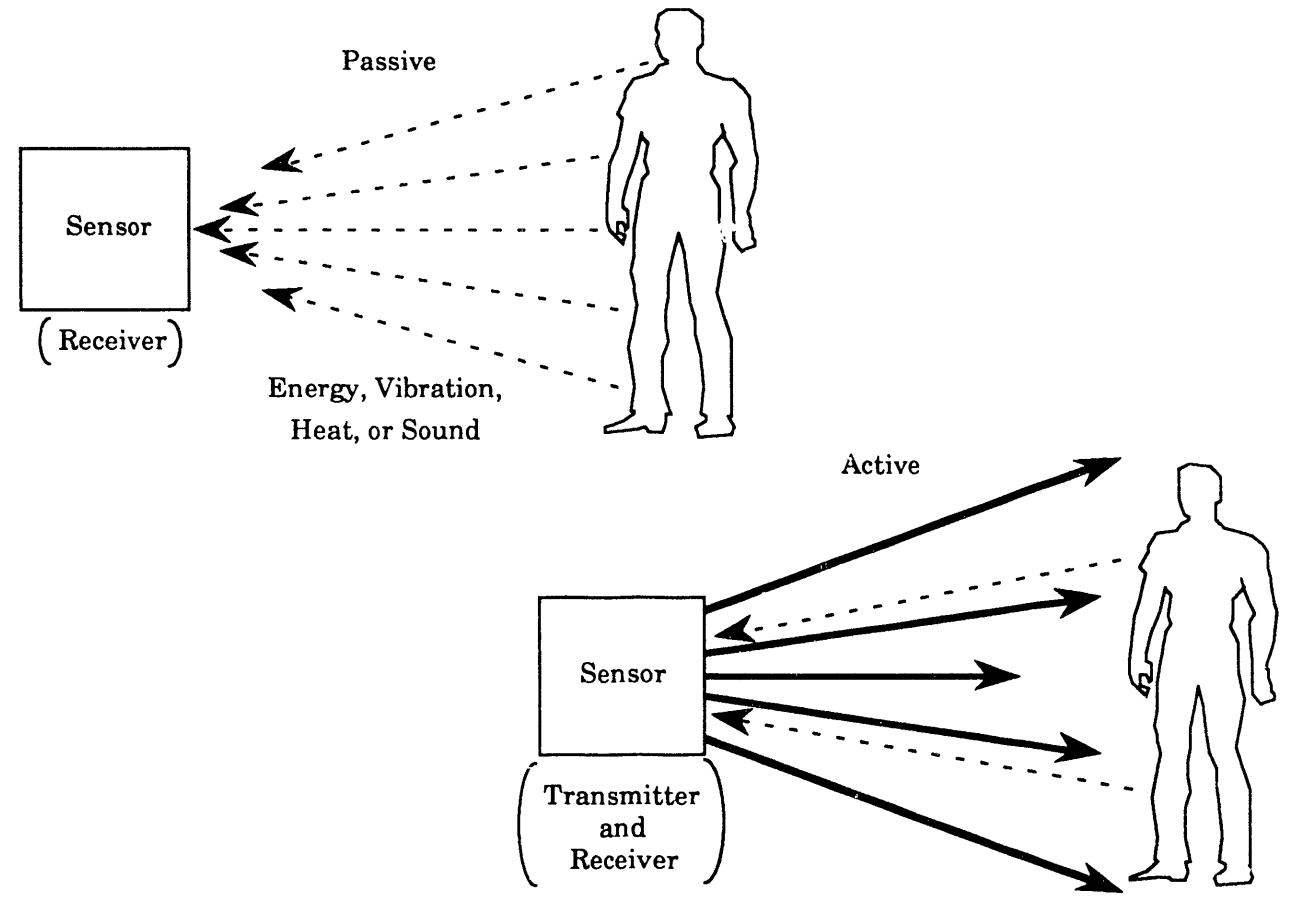


Figure 3-1. Active versus passive sensors

The three basic modes of application provide three layers of protection as illustrated in Figure 3-2.

The first layer of protection, provided by boundary-penetration sensors, detects the breaching of a wall, door, window, roof, or ventilation duct. Sensors that provide boundary-penetration detection include balanced magnetic switches, glass-break detectors, vibration sensors, and light-beam sensors.

The second layer of protection is provided by volumetric sensors, which detect motion within a specified volume of a structure. Examples of volumetric sensors are the active ultrasonic sensor, the microwave sensor, and the passive infrared sensor.

The third layer of protection is established by utilizing point sensors, which detect activity in the immediate vicinity of the protected object. Examples of point sensors are the capacitance proximity sensor and the pressure switch.

3.2.3 Covert or Visible

A sensor may be covert or visible according to its method of installation. A covert sensor, such as one located in a wall or under a floor, is hidden from view. A sensor attached to a door or mounted on a support

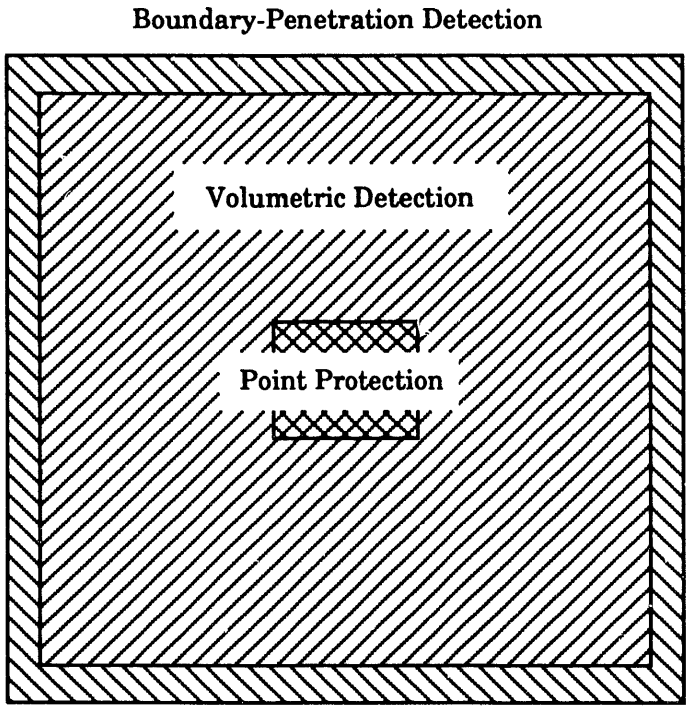


Figure 3-2. Interior intrusion protection in depth

structure is a visible sensor, in clear view of an intruder. Covert sensors can be more effective than visible sensors because they are more difficult for an intruder to detect and locate. In addition the concealment of covert sensors contributes to the aesthetics of the surroundings. However, visible sensors may deter an intruder from acting and are typically simpler to install and easier to repair than covert sensors.

Some manufacturers provide sensors with camouflaged housings that are not usually associated with intrusion detection sensors. Such covert sensors are useful in offices and homes where aesthetics are a factor as well as in areas where a desired element of surprise is provided by such concealment. Examples of such concealed sensors are light-beam sensors resembling wall outlets, passive infrared sensors resembling thermostats, and magnetic switches concealed in hinges. Installing a microwave sensor behind a curtain is another example of concealment.

3.3 Effects Of Physical Surroundings

Building and room construction should be taken into consideration before choosing the sensor appropriate for the area to be protected. A stable installation site is essential for reliability of detection from every sensor but most especially for the balanced magnetic switch. Detection is not possible through glass or other common solid objects for infrared or ultrasonic sensors; however, microwave energy from the microwave sensor easily penetrates glass, wood, and wallboard. Microwave energy is contained by metal and masonry construction.

Large objects, such as bookcases, desks, and partial wall partitions, may create shadow zones in the area under protection for sensors such as the microwave and the ultrasonic. Large objects placed nearby may also change the capacitance to ground of an object protected by a capacitance proximity sensor. Moving objects such as curtains and hanging signs may cause nuisance alarms. The effects of physical surroundings as they apply to specific sensors are discussed in greater detail in the following sections.

3.4 Effects Of Environmental Conditions

Natural and man-made phenomena in an interior intrusion sensor's environment may affect the ability of the sensor to detect an intrusion by producing signals in the same energy spectrum the sensor is designed to detect or by degrading sensor performance. Such phenomena may be characterized as electromagnetic interference (EMI), nuclear radiation, acoustic energy, thermal radiation, humidity, optical phenomena, seismic activity, and meteorological conditions.

Sources of electromagnetic energy which could interfere with the performance of an IIDS include lightning, power lines and power distribution equipment, transmission of radio frequency (including linked remote control), telephone lines and equipment, lighting, computer and data processing equipment, various electrically powered vehicles such as forklifts and elevators, television equipment, automotive ignition, electrical machinery and equipment, intercom and paging equipment, and aircraft. If the structure of the protected building or room is primarily of wood or concrete, neither of which provides electromagnetic shielding, then a high background of electromagnetic energy generated by exterior sources is possible. Providing electromagnetic shielding for all system components, including all data transmission links, and equipping all components with a common, adequate electrical ground minimizes the effects of stray electromagnetic energy.

Nuclear radiation can damage various components within a sensor, the most susceptible elements being semiconductors. Alpha particles and beta particles are not usually of concern because alpha particles are readily shielded and beta particles are not usually contained in a radiation environment in significant quantity. Gamma rays and x-rays can cause sensor damage through energy deposition or by charge displacement that results in generation of undesirable electrical transients. The performance degradation of semiconductor devices and integrated circuits caused by neutrons is dependent upon the total dose. Although current systems cannot be made totally invulnerable to a radiation environment, system vulnerability can be reduced by choosing radiation-tolerant components.

Acoustic energy which interferes with the performance of an interior intrusion detector may be generated within an area under protection or transmitted into the area from exterior sources. Some sources of undesirable noise are meteorological phenomena; heating, ventilating, and air-conditioning (HVAC) equipment; television equipment; telephone and electronic equipment; and vehicles, such as aircraft, trucks, and trains. Acoustic energy may cause a sensor to be less sensitive to motion within its detection zone; or the energy may even be within the sensor's detection bandpass, generating a nuisance alarm. Acoustic energy may even cause thermal air currents which cause the problems discussed in the next paragraph. The adverse effects of acoustic energy can be reduced by identifying and shielding the energy source, by reducing the number of hard surfaces from which the acoustic energy can be reflected, and by filtering out unwanted frequencies at the sensor. In all cases, care should be taken to ensure that sensitivity to intrusion is maintained.

The thermal environment in an area under protection can affect the performance of an interior intrusion sensor: The ambient temperature may be outside the range in which the sensor components were designed to operate. Uneven temperature distribution may cause air movement within the area which can be detected by a passive infrared sensor. Thermal expansion and contraction of structural materials may be detected by boundary-penetration sensors. An uncontrolled thermal environment may also reduce the detection sensitivity of some interior intrusion sensors. Contributors to an unstable thermal environment include weather, HVAC equipment, heat-producing machinery, interior lighting, heat-producing chemical and radioactive reactions, and fluctuating sunlight through windows and skylights. Specifying that all sensor components should operate between 0 and 50 °C, reduces the likelihood that sensors will be required to operate outside the desired range. Thermal expansion and contraction of structural components and unstable convection currents can be reduced by proper maintenance of the HVAC system, by shielding thermal sources, and by reorientation of the sensors.

High relative humidity may cause water vapor to condense on electronic and electromechanical sensor components. The presence of the water vapor may degrade the performance and reliability of the system. For sensors in a high-humidity environment, specifications requiring proper operation at 85 percent

relative humidity at 30 °C are adequate for most applications. A water-resistant, conforming coating for all components and circuit boards should be required. Desiccants may be placed in all enclosures to reduce the possibility of condensation.

Optical phenomena which reduce the effectiveness of an interior intrusion detector may be produced by sunlight, interior lighting, highly reflective surfaces, and infrared and ultraviolet energy from other equipment. Infrared sensors and video motion detectors are sensitive to incident or reflected light and to its movement within the field of view of the lens. Other sensors are affected by the heat generated when light is focused either on the sensor or on a nearby object. The adverse effects can be reduced by repositioning the affected sensor, by eliminating reflective surfaces, and by shielding sources of optical energy.

Seismic activity produces vibrations or structural movement which might be detected by interior intrusion devices. Undesirable vibrations result from earth tremors, machinery, vehicular traffic, thunder, and high winds. The seismic effects can be reduced by shock-mounting the sensors and by securely fastening or storing objects that might easily be moved.

Meteorological phenomena have been mentioned as part of each of the environmental conditions discussed in this section. These and other phenomena which may produce undesirable effects include lightning, thunder, rain, hail, temperature, wind, earth tremors, high relative humidity, and sunlight.

4 BOUNDARY-PENETRATION DETECTION

Boundary-penetration detection employs sensors to detect violation of the perimeter of a building or a room. Boundary-penetration sensors generally detect a penetration into an area under protection by an intruder through a door, a window, a wall, or another feature of the perimeter. Windows and doors may be opened without being damaged, and the appropriate sensors to detect such actions are usually position indicators. Walls, on the other hand, should be broken through, so the sensors utilized for detecting destructive intrusions are designed to detect activities such as impacts, sawing, and breaking of surfaces. It is desirable to detect an intrusion at the earliest possible moment, therefore some boundary-penetration sensors are actually designed to detect the approach of an intruder before an attempt is made to breach the perimeter.

Sensors that have some application to boundary-penetration detection but which are not discussed in this section include driveway sensors to detect vehicles brought close to the area under protection, cameras having video motion detectors to sense intrusions into an area under protection, passive infrared sensors used to detect human movement in an area adjacent to a boundary, and induction loops used to detect the presence of metallic masses.

4.1 Electromechanical Sensors

Electromechanical sensors are passive detectors which may be visible position indicators or covert continuity sensors. Position indicators, which are commonly used on doors and windows, range from simple mechanical switches to more intricate balanced magnetic switches. A continuity sensor consists of a fiber-optic or conductive wire grid enclosed in a wall, a ceiling, or a floor and the electronics for reporting an alarm when the grid is broken.

4.1.1 Mechanical Switches

Mechanical switches are employed as intrusion detectors on doors and windows and as tamper switches on many sensors. Such switches are commonly called microswitches. The feature of the switch that is most useful in such applications is that while the amount of travel of the switch actuator can be quite large, the amount of travel required for actuation is quite small. Therefore switch adjustment is not very critical for installation on doors which may not close to exactly the same position each time.

4.1.1.1 Principles of Operation

The mechanical switch is a simple snap action, single-pole single-throw or single-pole double-throw switch with a long throw actuator. The actuator may be a plunger with a movement range of about ½ inch, or it may be a spring leaf lever, with or without a roller, with a similar or even greater movement range. The switch is wired into the intrusion alarm system just as any switch is connected into a circuit. If the switch is used with a transistor, a logic-level output may be provided; but the switch is more likely to be connected directly to the associated processor.

A mechanical switch used as a tamper switch usually has a feature such that pulling the plunger out closes the switch and permits working on the usually tamper-protected sensor with the enclosure open. When the enclosure is closed, the plunger is returned to its normal state automatically. This feature is especially useful when the tamper and alarm indications are returned to the processor on the same wiring loop.

4.1.1.2 Performance Characteristics

Since the mechanical switch is not a very sophisticated device, it is vulnerable to both mechanical and electrical tampering. If the switch is inside a protected volume, that volume provides protection from an outsider. Enclosing a mechanical door switch in a tamper-protected box prevents bridging of the switch terminals by an insider. Additional insider protection is provided by configuring the switch mounting and the actuation mechanism so that the switch cannot easily be mechanically bypassed.

4.1.1.3 Installation Guidelines

A mechanical switch is mounted on the frame surrounding the protected door or window, positioned in a manner that will cause the switch to activate when the door or window is opened. In order to preclude bypassing the switch from the inside, a well may be fabricated on the door for the switch to move into when the door or window is closed. The well should be deep enough to prevent insertion of an object between the door and the switch plunger for the purpose of holding the switch closed when the door is opened. Frequent door operation, especially slamming, can cause parts of the sensor installation to move out of alignment over a period of time.

4.1.2 Magnetic Switches

Magnetic switches are commonly employed to detect the opening of doors or windows. Two types of magnetic switches are commercially available: simple and balanced. The simple magnetic switch is used as a tamper switch as well as in door-contact installations. The balanced magnetic switch (BMS) is especially useful for high-security applications.

4.1.2.1 Principles of Operation

Simple Magnetic Switch

A simple magnetic switch consists of two parts, a magnet unit and a switch unit. The magnet unit is a permanent magnet in a housing that permits mounting on a door or a window. The switch unit, which is mounted on the frame, employs a steel armature connected to an electrical contact. When the steel armature is near the magnet unit, the armature is attracted to the magnet. When the magnet is removed by opening the door or window, motion of the armature causes the switch contact to be transferred from one position to another. Some magnetic contacts employ a small magnetic reed switch in place of the steel armature. As illustrated in Figure 4-1, the reed switch changes state between its rest condition and the condition under the influence of a magnet, resulting in the same output as that provided by the armature: a switch actuation when the associated door or window is opened.

Balanced Magnetic Switch

A balanced magnetic switch (BMS), the most commonly used door sensor, employs a magnet in both the switch unit and the magnet unit (See Figure 4-2.). The switch unit, which contains a magnetic reed switch, a bias magnet, and tamper/supervisory circuitry, is mounted on the stationary part of the door or window. The magnet unit, which contains the larger 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 magnetic fields are adjusted to create a magnetic loop such that the reed switch experiences a magnetic field of

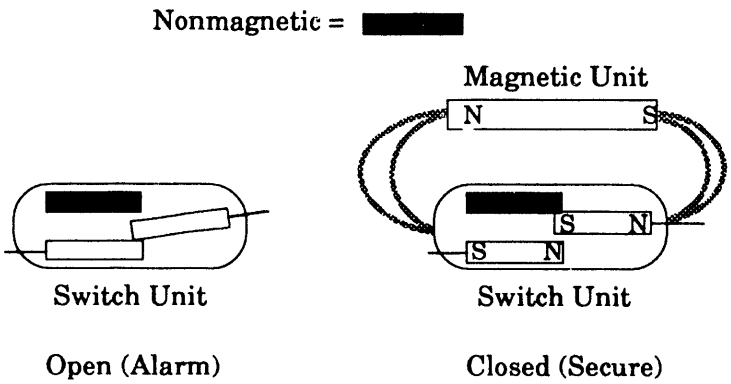


Figure 4-1. Magnetic reed switch

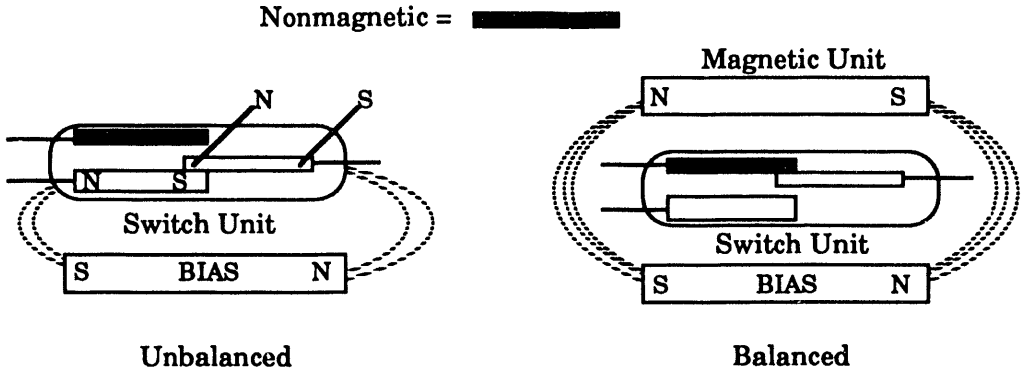


Figure 4-2. Balanced magnetic switch

essentially zero. In some models, this adjustment is accomplished by adjusting the bias magnet; while in other models the adjustment is made by varying the position of the magnetic unit with respect to the switch unit. Any action which causes the magnetic field to become unbalanced, such as opening the door or window, results in the transfer of the reed switch and an alarm output. A similar result is obtained if an external magnet is brought into the vicinity of the BMS, thus changing the magnetic field. Since the BMS is the most commonly used magnetic switch, the following performance characteristics, installation guidelines, and maintenance guidelines specifically address the BMS.

4.1.2.2 Performance Characteristics

The sensitivity of a BMS can be decreased by an externally introduced magnetic field. It is also possible to physically bypass, or shunt, the switch. Manufacturers reduce the vulnerability of magnetic switches to external magnetic fields by employing multiple magnets, various magnetic orientations, and magnetic shielding such as Mumetal; by creating standoff distances; and by adding magnetic tamper indicators. The newest switches on the market have very narrowly defined magnetic field paths to make them immune to external magnets.

4.1.2.3 Installation Guidelines

Site Preparation

Satisfactory operation of a BMS calls for a stable installation site. Doors, windows, or gates on which the switches are mounted should have well-fitting hardware which is properly maintained so that the balanced switch position is repeated consistently. If the mounting surface is ferrous material, spacers of Lucite™ or other nonferrous material prevent interference with switch operation. For the same reason, mounting brackets should be made of aluminum instead of steel. Conduits for connections can be installed prior to installation of the switches. Recessing the switch assembly into the door/window jamb is preferable to surface mounting to make tampering more difficult. Consult the manufacturer's manuals for specific site-preparation information for the switch selected.

Modifications

Modifications to the commercially available equipment improve the security afforded by the BMS. Since modifications may change performance characteristics, experimenting with the BMS before it is installed helps to determine any modifications which may be necessary. The following alterations have been used with success.

Pinning the Cover

Installing a pin, so that the cover on the switch assembly engages the pin, forces an intruder to manipulate the cover with greater certainty in order to prevent exposing the internal components and generating a tamper indication.

Magnetic Tamper Protection

Utilization of a foreign magnetic field to tamper with a BMS may be detected by installing additional reed switches in a supervisory loop. The switches are able to detect a foreign field before it is of sufficient magnitude to be a problem.

Shielding

The principle of operation employed in a BMS is the creation of a balanced or null magnetic field in the vicinity of a reed switch. Any externally introduced magnetic field which maintains a balanced field can make the switch less sensitive to opening of the protected door or window. Encasing the switch in a magnetically permeable material, excluding the side facing the field magnet, shunts an external field from the switch. Experimentation may determine that shielding is only necessary in certain areas, rather than encasing the entire switch. Materials with high magnetic permeability, such as Mumetal, are preferable for such shielding, although steel can be used.

Installation

Locating the switch within the area under protection reduces the opportunity for tampering. The switch assembly is mounted on the fixed surface, and the magnetic assembly is mounted on the movable surface at the top near the edge opposite the hinge for maximum detection of door or window movement, as illustrated in Figure 4-3. A rigid mount maintains switch alignment and prevents a high NAR. To minimize induced residual magnetism, the switch and magnet assemblies should not be allowed any closer to steel parts than they will be in the final mounting position. Final mounting position is determined by moving one unit with respect to the other or by internal adjustments, according to manufacturer's instructions.

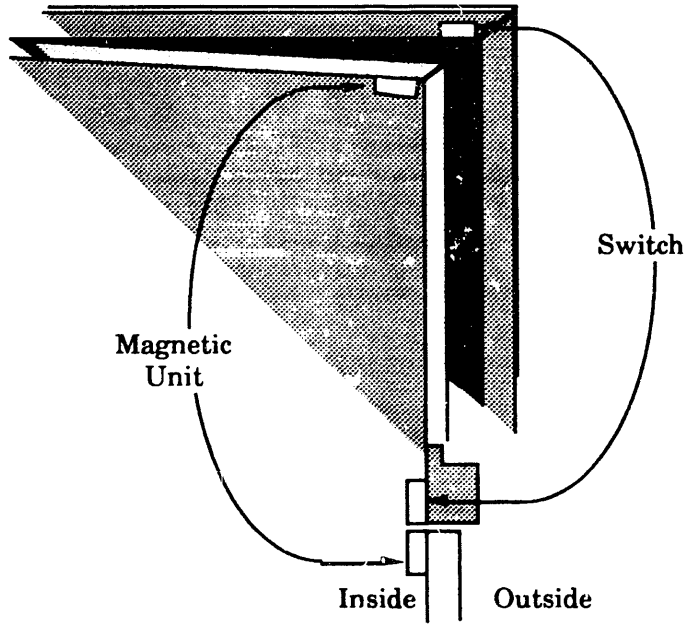


Figure 4-3. Installation of a magnetic switch

After the switch is mounted, open and close the door, window, gate, or other protected object to assure that the switch is operating properly. If not, further alignment and adjustment may be necessary.

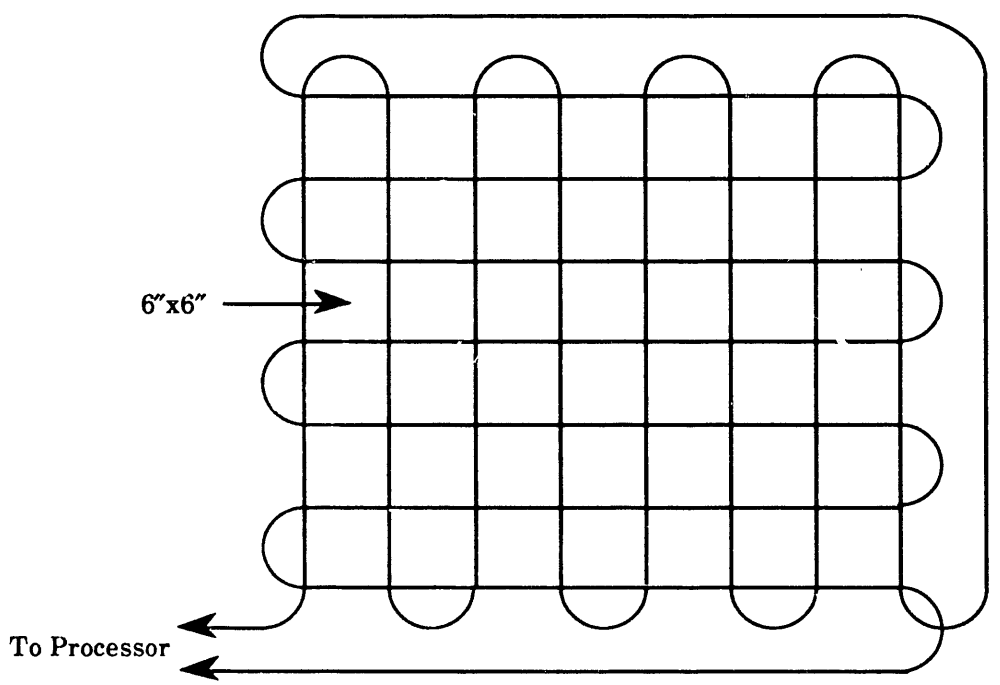
Loose bolts and screws and worn hinges cause misalignment of the switch. Frequent shock due to door closing causes wiring and connection failures and intermittent signals.

4.1.3 Continuity Sensor

A continuity sensor is an electromechanical sensor which is usually attached to or enclosed in a wall, a ceiling, or a floor to detect penetration. The continuity sensor, which is effective for many types of construction materials, consists of an optical-fiber or electrically conductive wire grid, arranged as in Figure 4-4, and the electronics required to report an alarm when the grid is broken. Any pattern can be formed to protect surfaces of unusual shape. Continuity sensors can be employed to detect forcible penetrations through vent openings, floors, walls, ceilings, locked storage cabinets, vaults, and skylights.

4.1.3.1 Wire Grid

A wire grid, also known as a breakwire sensor, is one of the simplest boundary penetration sensors. A loop of wire is attached to or enclosed in a wall or a window, and the continuity of the wire is monitored. As long as the wire remains unbroken, it is assumed that the boundary surface has not been penetrated. Breaking the loop of wire anywhere causes an intrusion alarm to be generated. Systems utilizing multiple closely spaced grids of wire and large printed-circuit panels with multiple conductors have been used successfully.



NOTE: The grid is composed of a single conductor NOT connected at the crossover points

Figure 4-4. Arrangement of a typical continuity sensor

Principles of Operation

To an alarm processor, the loop of wire forming a wire grid looks like a closed switch contact. If the loop is broken, an intrusion alarm is generated. By using a transistor to excite the loop, a logic level can be generated; but more commonly the loop itself is the reporting device with no intermediate processing.

Performance Characteristics

The NAR for a wire grid is very low because the wire should be broken to initiate an alarm. The wire grid is vulnerable to being taken apart by an intruder if the intruder has enough time. The loop cannot sense being touched, only being broken; therefore, it may be handled and still not detect an intrusion. It may also be bridged by soldering or clipping a jumper wire across the two ends of the wire. If no broken wire occurs during the handling and bridging, no detection occurs.

A grid that is more difficult to bridge is created by using multiple conductors. Not all the conductors should be used to make the task of picking through the grid of wires more difficult. If multiple conductors are employed, the conductors are made separate arms of a sensitive resistance bridge which can be coupled with electronics to detect bridging and tampering of the conductors. The electronics required are a bridge amplifier and a power supply with an output that may be a logic level or a relay actuation.

Installation Guidelines

The wire-grid sensor is installed by placing a grid of small diameter wire on or in a wall that is part of the boundary of an area under protection. The wire is installed in a serpentine fashion with about 6-inch spacing horizontally and vertically. In a new installation the wire grid may be installed in the walls at the time of construction, whereas in an older building it may be stapled to the walls and covered with protective paneling. Kits are manufactured containing spools of #26 enameled wire and a staple gun which dispenses the wire and staples it to the wall surface in one operation. The installation of a multiconductor wire grid requires that the individual conductors remain separated from each other. Large multiconductor flexible printed-circuit panels are often manufactured to be glued in place with a contact adhesive.

Combining the wire-grid sensor with proximity detection or video surveillance provides the means for detecting an attack on the sensor. Installing the grid in a fashion that makes understanding the serpentine pattern difficult should make finding the bridging points more difficult.

4.1.3.2 Fiber-Optic Grid

An optical fiber embedded in the walls of a structure acts as a boundary-penetration sensor. An intrusion attempted by breaking through the wall would result in breaking the fiber. Any interruption in the transmission of light through the optical fiber would indicate that the fiber had broken. Sophisticated measurements of the pattern of reflections within the fiber can distinguish between an intrusion attempt and a normal stressing of the wall containing the fiber. Such pattern measurements have not been used extensively but have been demonstrated in the laboratory. A fiber-optic grid provides covert protection of windows, because an optical fiber embedded in glass would be very difficult to detect.

Principles of Operation

In operation as a boundary-penetration sensor, an optical fiber is monitored to verify that the fiber is continuously passing light. A light source such as an LED or a laser is coupled to one end of the fiber to inject visible or infrared light into the fiber. A receiver in the form of a phototransistor or similar device receives the light passed through the optical fiber. Breaking of the fiber results in loss or reduction of the signal received at the far end of the fiber; the processed receiver output causes a relay actuation or a change in logic level. Schemes have been developed which inject pulses of light into each end of the optical fiber and observe the pulses coming out of both ends. Time-of-flight techniques and synchronous detection may detect attempts to splice or bridge portions of the optical fiber.

Performance Characteristics

An optical fiber is difficult, but not impossible, to tap into while it is in operation. By observing the amplitude of the light transmitted down the fiber, tapping or bridging the fiber may be detected; however, sensitive measurements are required because the associated changes are usually small. An attempted breakthrough of the boundary of a structure should break a properly installed, embedded fiber. Detection of the presence of light in the fiber from measurements taken near the fiber is difficult, unlike similar measurements for wire conductors.

Installation Guidelines

An optical fiber sensor installed in the boundary of a structure at the time of construction is an integral part of the structure. Such a sensor is difficult to detect and defeat and is easily broken during an attempted intrusion. In existing construction the fiber can be installed on the inside surface of the boundary and covered with a protective surface to prevent accidental breakage. Since the sensor is designed to be fragile, the most difficult part of installation is prevention of breaking the fiber.

4.2 Sound-Wave Detectors

In addition to sonic waves, infrasonic, seismic, and ultrasonic waves may all be called sound waves. Sound waves are defined as longitudinal pressure waves in any material medium, regardless of whether they constitute audible sound. The sensors discussed in this section detect such pressure waves generated by attempts to penetrate a protected boundary.

4.2.1 Infrasonic Sensor

An infrasonic sensor may be considered a volumetric sensor as well as a boundary-penetration sensor because it detects pressure changes in a volume of space; any enclosed volume ranging in size from a large building to an automobile is appropriate. When the pressure within the volume has stabilized, opening any hinged door leading into or out of the volume creates a slight but detectable negative or positive pressure change for a short time, as illustrated in Figure 4-5. Opening or closing windows, sliding doors, or roll-up doors generally does not cause a detectable pressure change. The pressure change manifests itself as infrasonic waves, sound waves occurring at such a low frequency, below 2 Hz, that they are inaudible. The infrasonic sensor consists of a microphone exhibiting very sensitive low-frequency response coupled to processing circuitry.

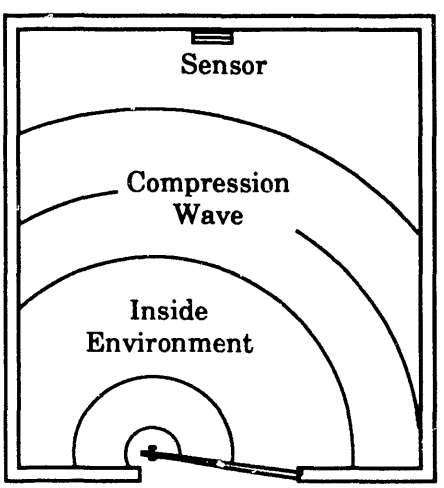


Figure 4-5. Pressure change to which infrasonic sensor responds

4.2.1.1 Principles of Operation

The infrasonic sensor is an ultralow-frequency-sound listening device employing an electret microphone as the sensor. An electret microphone is employed because it produces good response to very low frequencies. The output of the electret microphone is routed to amplifiers and filters to increase the signal amplitude and to remove all frequency components above a few hertz. The filtered signal is applied to logic circuits or pulse stretchers and then to a relay driver or another output device that indicates when the sensor has detected an intrusion. A time window is designated within which the pressure change should occur to avoid detection of atmospheric pressure changes.

4.2.1.2 Performance Characteristics

An infrasonic sensor is sensitive to any stimulus which causes a quick pressure change within the protected volume, such as drafts caused by winds gusting through vents, chimneys, and open doors and windows. In a building with openings to the outside of the volume, the sensor may be unusable on very windy days. Forced-air heating can pressurize a volume temporarily when it starts up, causing a sensor response. An infrasonic sensor may also respond to the opening of doors in rooms outside the area under protection or to thunder and other stimuli which cause the walls of a lightly constructed building to flex.

4.2.1.3 Installation Guidelines

An infrasonic sensor mounted on a surface, such as a wall, near the center of the protected volume provides the most consistent and sensitive detection. Making the monitored structure airtight by minimizing cracks and openings to the outside of the area under protection eliminates many nuisance alarms generated by air blowing into the closed volume. To avoid coupling of infrasonic pressure waves, heating and air conditioning ducts should not connect many rooms of a building. Positioning the sensor to avoid blasts of air from furnace or air conditioning vents reduces the occurrence of nuisance alarms. If one sensor is insufficient to cover all parts of a structure, several may be used without interaction among them.

To detect entry into an area or a room of the structure without detecting entry into the structure as a whole, installation of tight fitting doors is recommended between areas under protection and areas not under protection as well as restriction of the number of openings connecting the two areas. In the area where detection is not desired, the use of sliding doors or a revolving door would prevent sensor response.

4.2.2 Passive Sonic Sensor

The passive sonic sensor, also called a sound discriminator, is a covert listening device that employs a microphone to detect sounds generated by breaking and entering. Such a sensor is useful in many security applications and is generally of low cost because of its simplicity. However, if the area to be protected is noisy, the passive sonic sensor may not be applicable.

4.2.2.1 Principles of Operation

A passive sonic sensor, which may be hardwired or wireless, comprises a microphone, signal conditioners, and an amplifier. The signal conditioning may consist of filtering, pulse counting, and integration of pulses and noise. The filter selects high frequency audio components of the composite signal from the microphone, the portion of the audio spectrum associated with breaking and entering, usually frequencies above 4 kHz. The harder the material that is broken or impacted, the higher are the frequency components generated by a break-in. For example, breaking concrete generates higher frequencies than breaking wood. Passbands are selected based on the type of break-in expected. A gain control is often provided for sensitivity selection. Figure 4-6 illustrates the frequency response of a typical passive sonic sensor.

Logic circuitry is employed to integrate and analyze the filtered signal. When a signal of sufficient amplitude is detected, the sensor produces an output signal. In order to reduce nuisance alarms, a

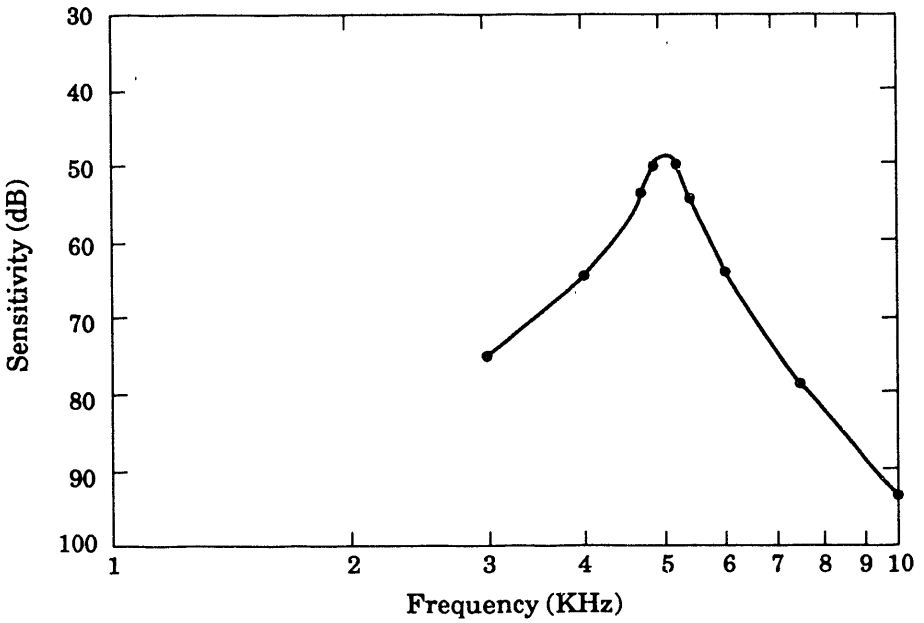


Figure 4-6. Passive sonic sensor frequency response

selectable counting circuit may be employed, requiring a preset number of noise pulses within a time window to generate an output signal. The output signal may be a logic level, but is more commonly a relay actuation.

Routing the microphone's output signal directly to an amplifier without filtering allows an eavesdropping feature to be incorporated into the system. When an alarm is received, the sensor area may be monitored auditorily from a remote location for alarm assessment. Such an installation is not recommended for a high security area because it provides a path for an adversary to monitor information.

4.2.2.2 Performance Characteristics

A passive sonic sensor is unlikely to detect masked penetration noise of breaking glass or splintering wood. If a penetration can be effected in one strike, a system set up to respond to multiple bursts of sound will not alarm. Because of its limited effectiveness, a passive sonic sensor should be used only to protect against a low-level threat, such as low-skill intruders who are expected to generate a lot of noise during an intrusion.

A passive sonic sensor responds to all sound frequencies within its passband, and an impact device nearby may generate the proper spectrum to cause a nuisance alarm. Noises generated by an impact printer or a typewriter are unlikely to be sensed, but noises generated in an area such as a machine shop may render the sensor useless. Impact noises generated outside the area under protection are seldom a problem because high frequency sounds are not transmitted well by most building materials.

4.2.2.3 Installation Guidelines

A passive sonic sensor may be installed anywhere within the area under protection to detect intrusions through the perimeter of the room or structure. Securely mounting the sensor prevents nuisance alarms caused by the sensor's moving and hitting its mount. Mounting the sensor away from impact noise-generating devices also reduces the nuisance alarm rate. Nearby sources of impact noise should be muffled, if possible.

Sound level is a function of the distance from the source and the amplitude of the source, so several sensors may be required to adequately cover the perimeter of the area under protection. Since the sensors are passive, multiple sensors may be utilized without interaction.

4.2.3 Passive Ultrasonic Sensor

The passive ultrasonic sensor is a passive sonic sensor utilizing a high-frequency microphone to detect frequencies above the audible range, usually 30 kHz and higher. The ultrasonic sensor does not respond well to audible sounds, but impact devices nearby may generate the appropriate frequency spectrum to cause nuisance alarms.

4.2.4 Seismic Sensor

Although the seismic sensor is designed for use as a buried sensor in outdoor perimeter applications, seismic sensors, such as geophones or strings of geophones connected to an alarm processor, may be used as structure boundary-penetration sensors. The geophone has low-frequency response and, when attached to the walls of a structure, can be used to detect motion of the walls, such as during an attempted intrusion. Geophone processors often have a monitoring point within the processor that may be used in a listen-in mode, enabling the entire wall of the structure to be used as a sounding board or microphone.

4.2.4.1 Principles of Operation

A geophone consists of a coil and a magnet that are mounted relative to each other. One of the two components is fixed to the housing of the geophone, and the other is mounted on a spring. The spring-mounted component becomes the reference mass and remains fixed in space as the component mounted to the housing moves relative to the reference mass when the housing moves. The voltage generated by the relative motion of the coil and the magnet is processed with logic circuitry; and, if the proper combination of frequency, amplitude, and duration or number of bursts of signal is sensed, a detection of an intruder occurs. The number of bursts of signal required is usually programmable, and sensitivity adjustments are also possible. When a detection occurs, the alarm processor outputs a signal which may be a logic level or a relay actuation.

4.2.4.2 Performance Characteristics

Since a buried seismic sensor is designed to detect disturbances such as walking or vehicle movements, the same sensor will respond well to similar disturbances when mounted on the boundary of a structure. Impacts on the boundary generate alarm signals, so restrictions should be imposed on activities near or on the walls of the structure. Structural disturbances caused by heavy machinery operating in the building or other normal building motion may render seismic sensors useless.

4.2.4.3 Installation Guidelines

Geophones are manufactured as completed units with integral cabling so that the entire string can be buried without being affected by moisture. Such strings of geophones are often supplied in 100 meter lengths, which are rather unwieldy. Shortening the string would improve its applicability to structures.

Geophones are installed by gluing them to the walls of the protected structure as illustrated in Figure 4-7. Dental cement is commonly utilized as an adhesive, but other epoxies are also applicable. A soft epoxy is not advisable because the geophone is intended to be an integral part of the structure. The spacing of geophones along the wall is limited by the spacing on the manufactured string. If testing reveals that some areas of the wall are not adequately covered, it may be necessary to mount the individual geophones closer together. If there are breaks in the structure or joints in the walls, individual geophones may be mounted on each independent section of the wall to provide adequate coverage of the wall surface. Separate signal processing is recommended for walls adjacent to heavy machinery and walls in relatively quiet areas of the same structure. Otherwise common processing may result in a high NAR or insufficient coverage.

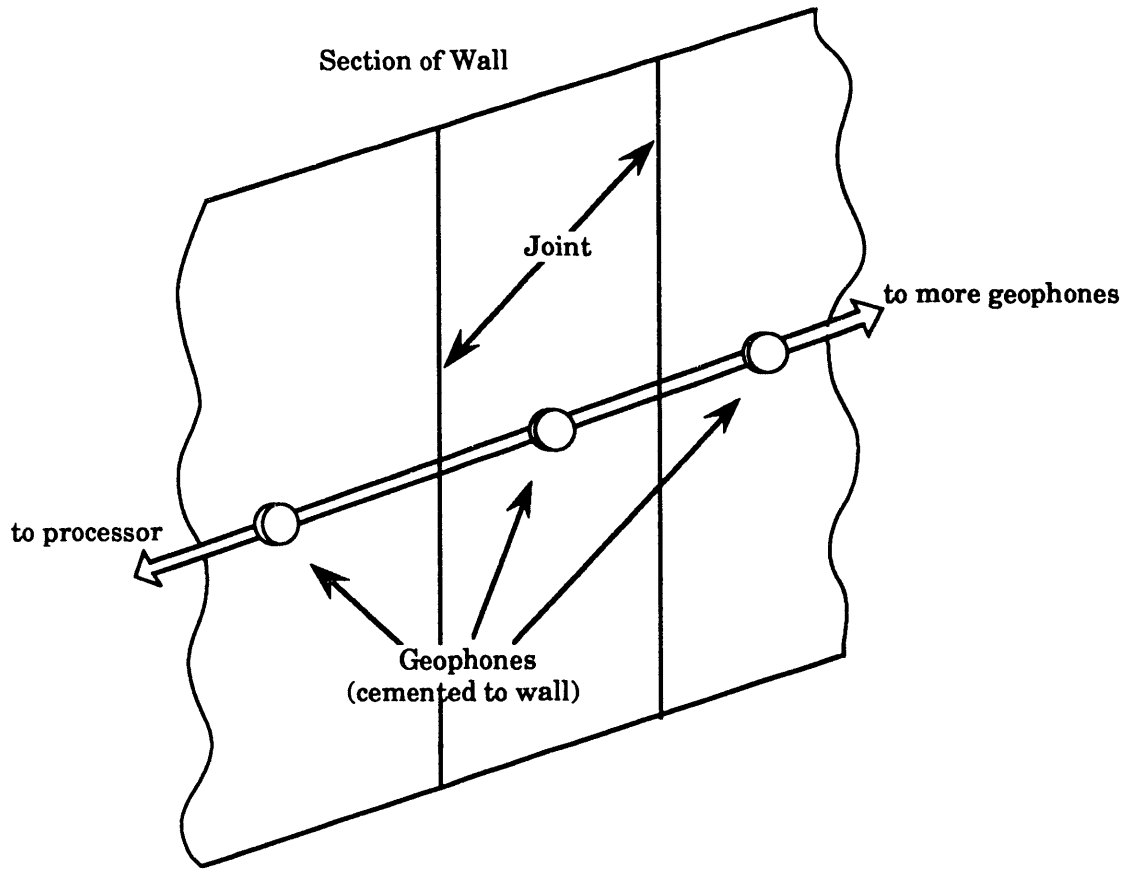


Figure 4-7. Typical geophone seismic sensor installation

4.2.5 Vibration Sensors

A vibration sensor is a passive, visible sensor which detects movement of the surface on which it is fastened. The typical vibration sensor exhibits a detection zone with a radius of approximately ten feet. The sensor may be mounted on the inside of a wall or a window, on the ceiling, or on the floor of a protected room or structure. Breaking through or attempting to break through the surface upon which the sensor is mounted causes vibrations to be transmitted along the surface. The vibrations are detected by the sensor; and, if the proper conditions are met, the sensor signals an intrusion. The primary advantage of employing vibration sensors is to provide early warning of a forced entry.

A wall sensor usually detects frequencies above 4 kHz, the frequency spectrum associated with breaking through building materials; sensors mounted on glass employ a passband above 10 kHz, the frequency spectrum exhibited by breaking glass. Normal building vibrations generated by machinery, such as HVAC equipment, are ignored.

4.2.5.1 Principles of Operation

Vibration sensors may employ piezoelectric sensing elements or electromechanical inertial sensing elements. Both technologies utilize a reference mass that does not move when the mounting surface moves. Sensitivity adjustments and pulse counting logic are features designed to tailor the sensor to its installation environment. Although glass appears to break with a single burst, multiple impacts occur as the falling pieces strike each other, so a multiple-impact counting device may be used.

Both piezoelectric and inertia sensors usually count the bursts of vibration, allowing the sensor to be adjusted to compensate for a noisy surface. When the proper signature is sensed, the sensor produces a detection output. That output may be a logic level or a relay actuation.

Piezoelectric Sensor

The piezoelectric sensing element of a piezoelectric sensor is mounted directly on the vibrating surface and moves with respect to the mass of the body of the sensor. This motion flexes the piezoelectric element, causing a voltage output which varies according to the amplitude and frequency of the vibrations of the surface. The voltage signal is processed by logic and filtering circuits; and, if the proper combination of amplitude, frequency, and duration exists, the sensor signals an intrusion. The passband of vibration frequencies detected by a piezoelectric vibration sensor is 5-50 kHz. When the vibrating surface moves slowly, the output from the sensing element is low, because the sensor moves as a whole, and these slow movements are ignored.

Inertia Sensor

A metallic ball mounted on metallic contacts is usually employed as the sensing element in an inertia sensor. The body of the sensor is mounted on the vibrating surface, and the ball tends to remain stationary with respect to the surface. Therefore, as the body of the sensor moves, the ball's inertia causes the ball to momentarily lose contact with its mount. A voltage is impressed across the metallic contacts of the mount, and the action of the ball acts as a switch. Voltage changes are sensed and processed using logic and filtering circuits. Amplitude is only measured in the sense that enough motion should occur to break the ball's contact with its mount. Two sensitivity levels may be achieved by varying the spacing of the mount contacts. Low frequencies generated by slow motion of the vibrating surface cause the sensor to move as a whole and are ignored because the ball does not have enough inertia to break free from its mount. The vibration frequencies detected by an inertia sensor are usually 2-5 kHz.

4.2.5.2 Performance Characteristics

The vibration sensor is designed to detect attempts to break through the perimeter of the area under protection, so activities in adjacent areas are a potential source of nuisance alarms. Consequently, such activities which cause impacts to the perimeter of the affected area may need to be controlled. Since the wall area that is under surveillance by an individual sensor is generally relatively small, indicators built into the sensor help isolate areas experiencing nuisance alarms.

A vibration glass-break sensor is designed to detect attempts to break through a window in the perimeter of the area under protection, so nuisance alarms are generated by impacting the window with a hard or sharp object. Birds often fly into windows, mistaking them for openings, and generate nuisance alarms. Bushes in contact with a window, loose-fitting glass, hail, and careless people all have the potential for generating nuisance alarms. Indicators built into such sensors help isolate nuisance alarm problems associated with the relatively small area of a single window.

4.2.5.3 Installation Guidelines

Vibration sensors are mounted in intimate contact with the vibrating surface that they are to protect and are mounted on the inside surface so that the sensors are inside the area under protection. Vibration sensors should not be used on structures subject to severe vibration from external sources, such as rotating machinery. However, a pulse accumulator or counting circuit might effectively reduce the nuisance alarm rate for structures subject only to occasional impacts.

The sensors are usually glued to the surface, although the manufacturer may specify another means of mounting, such as double-sided tape. Inertial sensors are orientation sensitive and should be mounted with the proper attitude in order to function. Discontinuities in the perimeter structure limit the area of detector sensing, so careful layout of sensor location is necessary to avoid dead spots. It is necessary to mount a vibration sensor on each continuous section of the area perimeter because vibrations are not

transmitted well by joints in the structure. A glass-break sensor should be mounted on each window pane because glass-break vibrations are not transmitted well by joints in the window frame. Vibration sensors are low cost, and many of them can be connected to a single processor. Multiple vibration sensors may be installed without interaction because they are passive sensors.

After mounting the sensors, signal parameters, such as the number of pulses required for a detection output, should be established. Potential sources of impacts upon the perimeter should be removed from both inside and outside the perimeter. Structural changes may require adjusting, relocating, or adding sensors to maintain the perimeter coverage desired. Window replacement usually requires glass-break sensor replacement, because removing a glued-on sensor usually destroys the sensor.

4.3 Active Boundary-Penetration Detectors

4.3.1 Light-Beam Sensor

A light-beam sensor employs interruption of a beam of light, visible or infrared, to detect boundary penetration. Applications suitable for such sensors range from short gaps, such as gates, doors, and portals, to long distances up to 600 m (2000 ft.), such as hallways. Although a light-beam sensor may be located immediately inside or outside the protected boundary, locating the sensor inside the boundary allows protection of the sensor installation with other boundary-penetration sensors.

4.3.1.1 Principles of Operation

A light-beam sensor may be known as an active photoelectric or active infrared sensor. The sensor transmits a light beam in the visible or near infrared spectrum to a receiver, usually a phototransistor, at the opposite end of the protected corridor. If the beam is not received, an intrusion is indicated. If multiple receivers are placed at the far end of the beam path, interruption of any single beam results in an intrusion indication. Several transmitters and receivers constitute a system with multiple beams arranged in a vertical fence as shown in Figure 4-8.

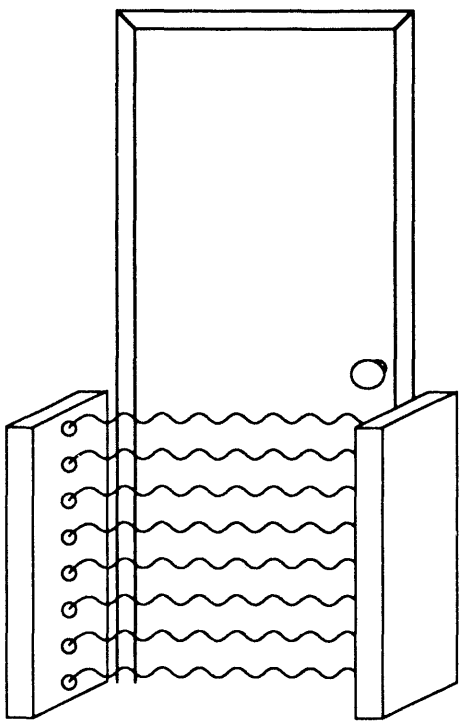


Figure 4-8. Light-beam sensor system using multiple beams

The light transmitter is usually an LED; its associated optics may consist of lenses or mirrors. To avoid interference from ambient lighting, the light beam may be modulated with a square wave utilizing frequencies ranging from a few hundred hertz to 20 kHz.

The geometry of a light beam sensor may vary. Instead of being placed at opposite ends of the protected corridor, the transmitter and the receiver may be collocated and a retroreflector installed at the other end of the beam path. An intruder crossing the primary or the reflected beam changes the amount of energy received at the sensor, causing an alarm.

For long beam paths, a pulsed synchronous technique may be utilized to reduce interference and possible defeat by external light sources. Reception of the primary light beam actuates a second transmitter at the far end of the beam path, eliminating the requirement for supervised wiring between the two locations.

4.3.1.2 Performance Characteristics

The lack of detection outside the beam path of a light-beam sensor means that bypassing the sensor beam will defeat the sensor. Utilizing at least two detectors to form a barrier reduces the vulnerability of the sensor to bypass. Mirrors can be employed to reflect the infrared beam back and forth, forming a fence-like pattern across a gap.

The light-beam sensor may be deceived by capturing the receiver with an external light source or a reflection. Outside light sources may sufficiently excite the receiver of an unmodulated light beam to reduce its sensitivity or even to prevent detection of an interruption of the primary beam. Modulation reduces the likelihood of such problems, but extraneous light may still bias the detector and change the sensitivity of the receiver. Employing modulation may not eliminate the sensitivity of a receiver to external sources of modulated light, such as gaseous discharge lighting.

A reflection may cause reception of a beam other than the intended one in a multiple-beam system, preventing detection of a primary beam interruption. To defeat a system with a collocated transmitter and receiver, an intruder might employ a reflector to return the beam from a point other than the sensor reflector, creating an opening in the beam path.

Infrared sensors are susceptible to various nuisance alarm sources. Smoke and dust in the air can reduce the level of energy at the receiver enough to initiate an alarm. Interruption of the beam by falling objects or small animals may last sufficiently long to cause an alarm.

4.3.1.3 Installation Guidelines

The PPS designer should carefully plan the installation of light-beam sensors in order to prevent easy defeat or bypass. The transmitter and receiver pair should be positioned with an unobstructed path between them and so that extraneous light sources are unlikely to cause nuisance alarms. Measures should be undertaken to prevent blocking of the beam by normal activities.

Mounting the sensor on a sturdy, rigid surface prevents misalignment of the light beam caused by mount vibration. Mount vibration is a significant problem with long-range sensors because alignment is more critical at long ranges. Using an alignment indicator is recommended, especially for long-range sensors.

The light-beam sensor is most effective if the path most likely to be taken by an intruder is perpendicular to the beam so the beam is broken. Avoid placing the beam such that an intruder's path would be likely to be directly into or away from it.

The following guidelines should be considered for reduction of the NAR for active infrared sensors. Remove or shield hot spots which may generate infrared energy, such as open heating elements; incandescent light bulbs; direct sunlight on windows, floors, and walls; and convective heat currents.

Narrow beams may not be subject to nuisance alarm generation by such sources. A final check is to ensure that the sensor is not being excited by a light source other than its primary transmitter.

4.3.2 Active Glass-Break Sensor

A glass-break sensor is mounted on a window or another glass surface to detect the breaking of glass, as in a forced entry. Several technologies are employed to detect glass breaking. The passive sonic glass-break sensor has been discussed in the section on passive sonic sensors, and the piezoelectric and inertia glass-break sensors have been discussed in Section 4.2.5 on vibration sensors.

An active glass-break sensor introduces a vibration signal into the protected glass, usually a four-by-eight-feet sheet of glass, and observes the signal received by a second transducer located elsewhere on the glass. Breaking the glass causes the retrieved signal to change. Although an active glass-break sensor is more expensive than other glass-break sensors, nuisance alarms caused by non-breaking impacts on the glass are avoided.

4.3.2.1 Principles of Operation

An active glass-break sensor employs a transmitting transducer to inject an ultrasonic signal into the glass. The location of the receiving transducer is arbitrary. The receiver may be located at another place on the sheet of glass, or it may be located in a common housing with the transmitter.

The received signal is a combination of a direct signal from the transmitter and a reflected signal from discontinuities in the sheet of glass, primarily the edges. When the glass is impacted but not broken, the discontinuities remain essentially the same. When the glass is broken, the discontinuities and thus the received signal are changed. The receiver analyzes the complex phase/amplitude relationships of the received signal compared to the transmitted signal. When breaking glass is detected, the sensor produces a logic-level output or a relay actuation signal.

4.3.2.2 Performance Characteristics

The structural discontinuity between the window and its frame limits the area of detection to the glass itself. Since a glass cutter functions by breaking a small portion of the glass where it scratches the surface, an attempt to cut the glass will usually be detected if the sensor sensitivity is set appropriately.

4.3.2.3 Installation Guidelines

Active glass-break sensors are mounted directly on the glass inside the area under protection. The sensors are usually glued to the surface, although some manufacturers specify other means of mounting, such as double-sided tape. Multiple active sensors mounted on the same window may interact. A final test is performed by tapping on the protected window. Tapping on the glass should not cause an alarm in the active sensor. Window replacement usually requires sensor replacement, because removing a glued-on sensor usually destroys the sensor.

5 VOLUMETRIC DETECTION

Volumetric detection employs sensors to detect motion in a specified volume, usually in an enclosed area, such as a room or a hallway. Common technologies utilized for such sensors detect infrared radiation and detect changes in microwave, ultrasonic, and sonic frequencies; a video motion detector monitors changes in brightness in a video signal.

Volumetric sensors may be active or passive sensors. Active sensors, which emit a signal and monitor changes in the reflected signal, are more sensitive to radial motion toward or away from the sensor. Passive sensors, which do not emit a signal but monitor changes in the received background energy, are generally more sensitive to motion across the field of view, circumferentially.

Passive sensors are always monostatic, meaning there is only one sensor housing. Active sensors may be monostatic, bistatic, or multistatic. A monostatic active sensor utilizes the same housing for both the transmitter and the receiver. A bistatic sensor employs separate housings for the transmitter and the receiver. A multistatic sensor has one main transmitter with additional transmitters slaved to the same oscillator. Multiple receivers may also be employed.

5.1 Active Volumetric Detectors

5.1.1 Ultrasonic Sensor

An ultrasonic sensor is an active, visible volumetric detector which emits an ultrasonic signal and discriminates between the undisturbed reflected signal and the signal modified by target motion. Ultrasonic sensors may be installed in a monostatic, bistatic, or multistatic configuration.

5.1.1.1 Principles of Operation

The ultrasonic sensor transmits an acoustic signal in the 19 to 50 kHz range, depending upon manufacturer and model. Detection is based upon the Doppler shift between the transmitted signal and the reflected signal. The magnitude and frequency shift of the Doppler signal depends upon the size and the velocity of the object providing the return signal.

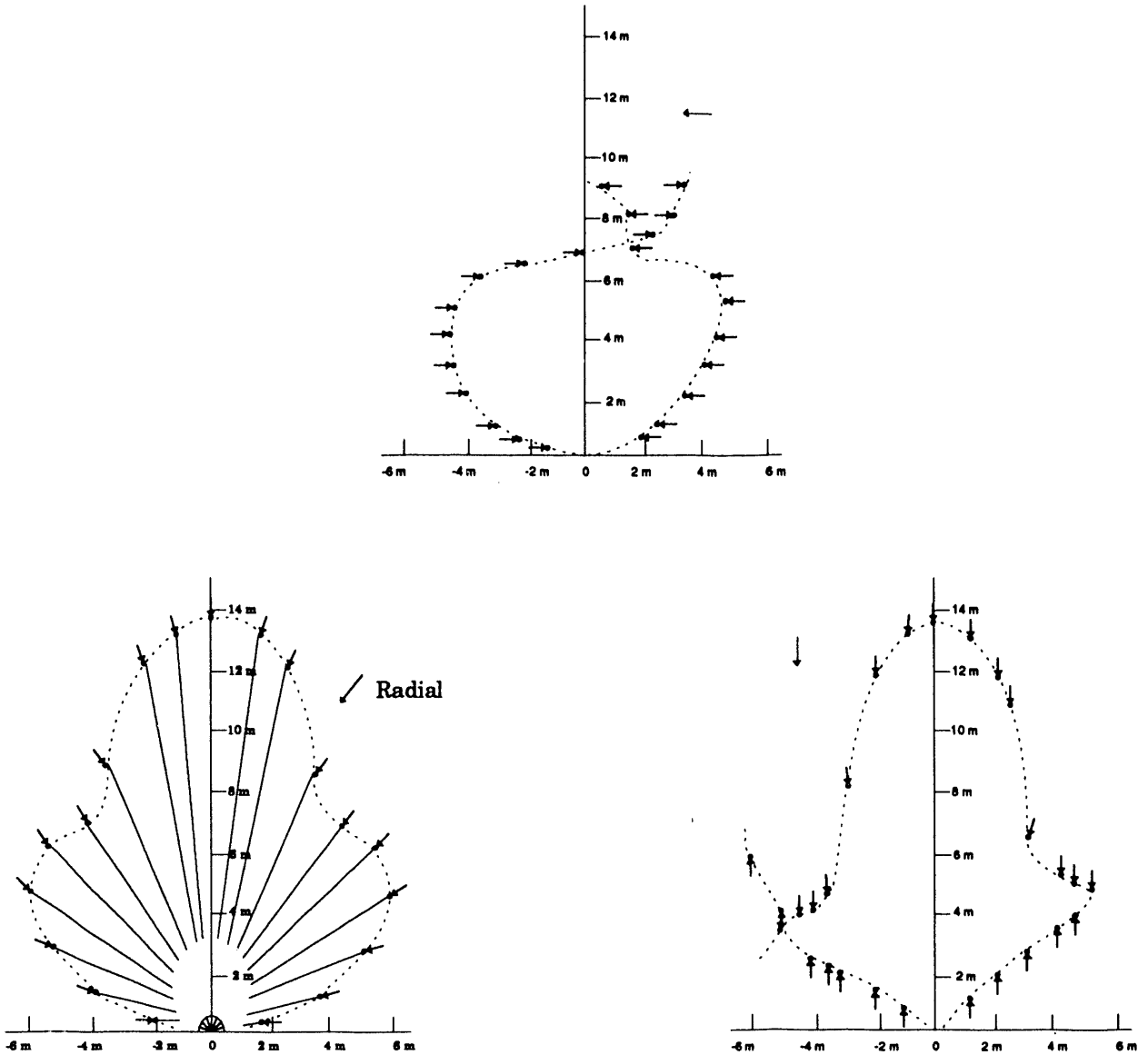
The Doppler frequency shift (f_d) is expressed as

$$f_d = \frac{2v}{\lambda} \qquad (5\text{-}1)$$

where v is the radial velocity of the target and l is the wavelength of the transmitted signal. A velocity of approximately 5 cm/sec is the lowest practical limit of detection due to the minimal frequency shift which occurs below that velocity. A brisk walk is about 100 cm/sec.

Since the frequency shift is dependent upon radial (to or from the sensor) velocity and not overall target velocity, the sensor is most sensitive when the target moves in a radial direction. In practice, even if the intruder is moving in a circumferential manner, some radial movement results from body sway or arm and leg movement. The sensor may also provide a significant level of protection against an intruder moving circumferentially by monitoring the overall signal strength.

A typical monostatic-ultrasonic-sensor detection pattern is shown in Figure 5-1. Some sensors may exhibit patterns which are wider or narrower than the pattern shown. The detection patterns of some commercially available sensors can be modified with deflectors to provide patterns similar to that shown in Figure 5-. The installation of deflectors significantly changes the effective shape of the sensor detection zone. Range adjustments are possible through variation of receiver gain and sometimes through variation of transmitter output.



Note: Arrows indicate walk test direction.

Figure 5-1. Typical detection patterns for an ultrasonic detector without deflectors

A bistatic ultrasonic sensor configuration bases detection on a combination of the Doppler effect and variation in signal amplitude. Receivers and transmitters are usually placed on the ceiling to obtain the desired coverage. Individual receivers have range-adjustment capability, but other characteristics are similar to those of monostatic ultrasonic sensors.

5.1.1.2 Performance Characteristics

Ultrasonic signals are generally contained by most building materials such as glass, wallboard, and heavy curtains, allowing shadow zones to be created by desks, bookcases, and wall partitions. Several sensors may be required for complete coverage of the volume.

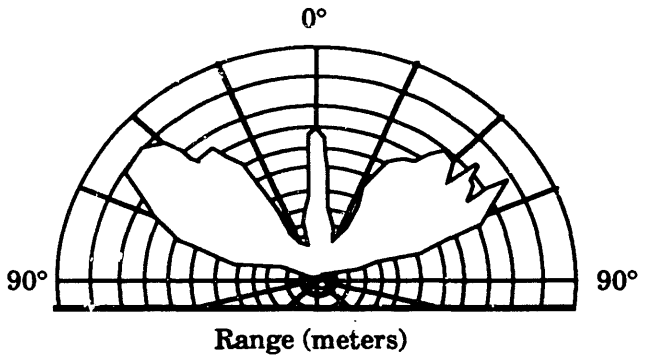


Figure 5-2. Detection pattern for an ultrasonic detector with V-type deflectors

Walls that reflect rather than absorb the ultrasonic signal may reflect the signal into the shadow zones and provide more complete coverage. Such areas of unexpected coverage could also become sources of nuisance alarms. Sources of ultrasonic energy may confuse the signal processor by producing signals similar to an intruder's. Mechanically produced stimuli, such as air turbulence from fans and HVAC ducts, can cause nuisance alarms or reduce the effectiveness of the sensor. Nuisance alarms may also be caused by ultrasonic noisemakers, such as ringing bells and leaking steam pipes, or by TV remote controls and item counters on an assembly line.

Variations in temperature and relative humidity may cause the sensor's sensitivity to increase, causing a higher incidence of nuisance alarms. Extreme environmental changes may cause a sensor that normally works well to be rendered nearly useless.

5.1.1.3 Installation Guidelines

The vulnerability of the ultrasonic sensor to nuisance alarms suggests that the guidelines outlined here be emphasized. The sensor should be installed at least 3 m (10 ft) from ultrasonic noisemakers, such as telephones, bells, and buzzers, and from sources of air turbulence, such as HVAC vents. The sensor detection envelope should avoid equipment whose motion causes nuisance alarms, including overhead doors, fans, and furnishings that move in the wind, such as venetian blinds, curtains, and suspended signs. Isolating individual sensors avoids nuisance alarms caused by cross talk; an alternative is to operate multiple sensors through the same oscillator.

Selecting a height of approximately 2.5 m (8 ft) above the floor and locating the ultrasonic sensor such that expected intruder motion is directly toward or away from the sensor creates the largest Doppler signal. Ultrasonic-sensor detection effectiveness is reduced for motion across its field of view. Providing line supervision and tamper protection for each sensor is essential.

In addition to the acceptance test requirements identified in Section 9 Procurement Guidelines, the following tests are recommended in accordance with the *NILECJ Standard for Ultrasonic Motion Detectors for Burglar Alarms*:

Rejection of Background Noise: The ultrasonic sensor's nuisance alarm susceptibility to background wideband ultrasonic noise can be evaluated by testing in accordance with Paragraph 5.7 of the *NILECJ Standard*. The ultrasonic motion detector should operate without causing an alarm when subjected to the defined background noise level for 10 seconds.

Rejection of Turbulent Air Interference: The effects of moving air on the ultrasonic motion detector's susceptibility to false alarms can be evaluated by following the testing guidelines in Paragraph 5.8 of the *NILECJ Standard*. A satisfactory ultrasonic motion detector will operate without causing an alarm when subjected to the defined environment of moving air for 30 seconds.

Slow-Random-Motion Rejection: Each ultrasonic sensor tested in accordance with Paragraph 5.9 of the *NILECJ Standard* should operate without causing an alarm when subjected to the defined, slow random motion for a period of 30 seconds.

Short-Duration-Pulse Rejection: Each ultrasonic motion detector should be exposed to defined, short-duration ultrasonic pulses for 30 seconds as outlined in Paragraph 5.10 of the NILECJ Standard. Acceptable detectors will not alarm under the given conditions.

Rejection of Extended Background-Noise-Level Increase: Expose each ultrasonic motion detector to an increased background noise level for a period of 60 seconds as defined in Paragraph 5.11 of the *NILECJ Standard.* Acceptable detectors will not alarm under the defined conditions.

5.1.2 Microwave Sensor

A microwave sensor is an active, visible, typically monostatic, volumetric sensor which operates on the Doppler principle, much like the ultrasonic sensor. Either a single antenna, called a transceiver, is employed for both transmitting and receiving or two antennas may be collocated. In addition to surveillance of a fairly large enclosed volume, a microwave sensor is useful for monitoring a very limited area almost as a point sensor, such as the automatic door openers utilized in supermarkets and airports.

5.1.2.1 Principles of Operation

A microwave sensor transmits an electromagnetic signal in the range of 10 GHz. Microwave energy is reflected from conductive surfaces, such as human bodies, and the reflected signal is altered by motion of the reflecting surface. The Doppler shift is a change in the apparent frequency of the signal. The antenna is usually a microwave horn but may be a printed circuit planar or phased array antenna. The shape of the detection zone is governed by the design of the antenna and is similar to an elongated balloon as shown in Figure 5-3. The figure illustrates the shapes of the detection zones at both full and half sensitivity settings. Table 5-1 shows the typical relationships between antenna angle and detection-pattern shape.

Table 5-1. Typical monostatic microwave detection patterns

Antenna Beamwidth (degrees)	Detection Area (width x length [m])
10	10x100
20	15x76
40	18x45
60	21x30
90	24x24

The Doppler frequency shift is related to the velocity of the reflecting surface. Logic circuitry measures the Doppler shift frequency and determines if it falls within the range appropriate for the target of interest. Logic may be employed to reject signals representing oscillator motion such as that exhibited by draperies moving with air currents and by other freely swinging objects. However, an oscillatory-motion rejection circuit creates a dead area at ranges beyond the oscillating object.

A microwave sensor, known as a microwave curtain sensor, whose detection envelope is much wider in one dimension than the other, as shown in Figure 5-4, may be used as a boundary-penetration sensor.

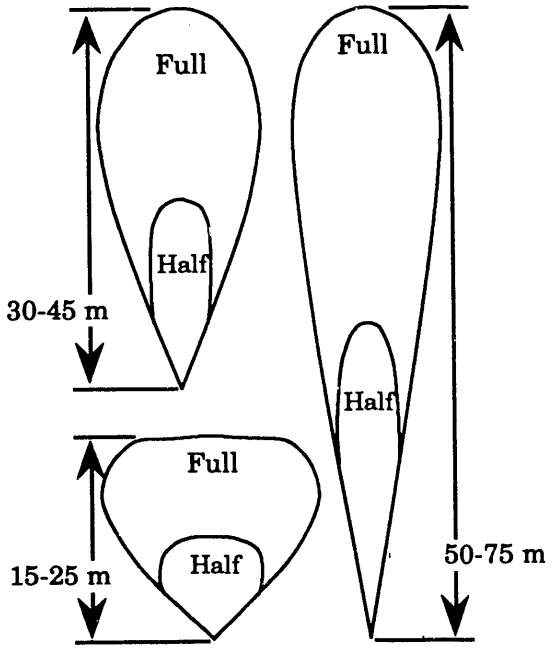


Figure 5-3. Typical microwave detection patterns

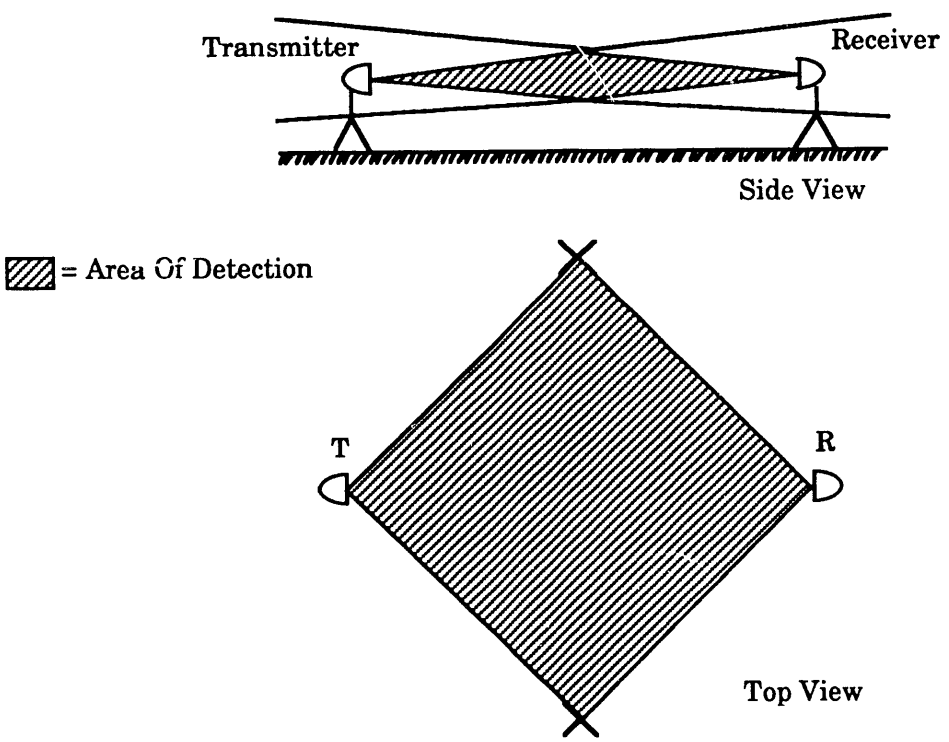


Figure 5-4. Typical microwave curtain sensor's field of view

When the sensor is properly mounted, the narrow dimension of the pattern extends out from the surface to be protected, and the wide dimension extends along the surface. The protected surface may be a wall or a ceiling, or it may be simply a slice through space, such as across a hallway.

A bistatic sensor utilizes signal-level detection in addition to the Doppler principle. A target entering the detection envelope of a microwave transmitter absorbs some energy from the field, and reflects some of the energy in directions away from the receiver, causing a detectable signal reduction. The amplitude of the reflected signal is determined by the size of the surface and its distance from the transmitter. An increase in signal level may indicate the presence of an alternate transmitter being employed in an attempt to spoof the sensor. A bistatic sensor employing signal-level detection best detects a target moving across its detection envelope in the narrow direction and exhibits poorer detection when the target remains within its detection envelope.

Some microwave sensors have a time-window feature for monitoring only those signals returning within a certain time period. This electronic technique, known as time gating, prevents detection beyond a maximum desired range, even if the sensor is otherwise capable of detection at the greater range.

5.1.2.2 Performance Characteristics

Microwaves are capable of penetrating many building materials, such as glass, plastic, Plexiglas™, wallboard, and wood; but materials such as concrete, brick, and metal will contain a microwave signal. Shadow zones may be created by metal bookcases, desks, and wall partitions as illustrated in Figure 5-5. Metal furniture near the sensor may also cause a strong reflected signal that masks the weaker signals from an intruder elsewhere in the area under protection. The signal may bounce off metallic surfaces and cause detection outside the area under protection. Metal air ducts can guide the signal into areas outside the protected volume.

Water moving in plastic plumbing behind wallboard and vehicles moving outside a protected room may generate nuisance alarms. Nuisance alarms may also be caused by the movement of fans and by fluorescent lights or even by small animals, such as mice. Employing multiple sensors in the same area results in cross talk and its associated nuisance alarms. The microwave sensor experiences reduced sensitivity for motion across its field of view or for very slow intruder motion.

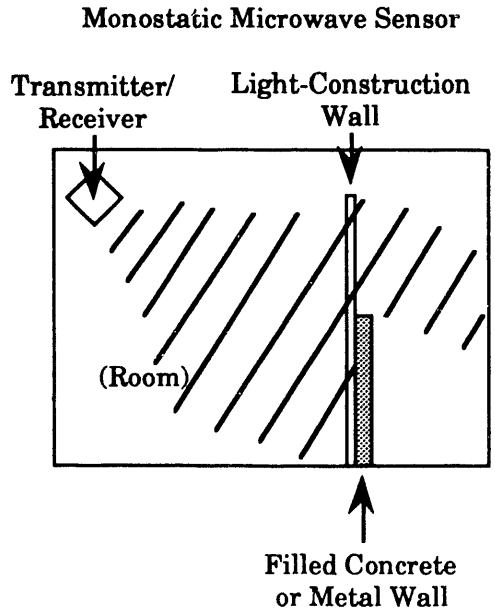


Figure 5-5. Shadow zone created by wall partition

Moving an object into the detection envelope of the sensor can effectively block the sensor's field of view and create an area not under protection. A signal-level sensing device would detect an object moved into its detection envelope if the sensing were absolute; however, most sensors have a long-term, automatic level-adapting circuit so that stationary objects "disappear" after a time.

A microwave oven can be a source of nuisance alarms. The operating frequency bands that are used for microwave intrusion detection are also used by law enforcement agencies for radar speed-measuring devices; however, the likelihood of a radar speed gun interfering with a microwave intrusion sensor are very small. Commercially available radar detectors can be used to detect the presence of an intrusion detector, and such a device would be useful to an intruder wishing to avoid detection.

5.1.2.3 Installation Guidelines

In addition to the general installation guidelines outlined in Section 8, the following procedures are recommended for installation of a microwave sensor. Because microwave energy is difficult to contain, special care should be taken when locating and directing the energy within the area requiring protection. A protected volume surrounded by masonry or metal construction confines microwave energy and prevents detection outside the protected volume. The microwave transceiver should be located so its detection envelope does not overlap fans, blowers, overhead doors, line printers, tape machines, venetian blinds, suspended lamps or signs, or other furnishings and equipment that move or have moving parts. Frequent visual inspections ensure than no blocking objects have been moved into a position that would render the sensor inoperative. To prevent eye damage, the sensor antenna should be placed so that people cannot look into it at very close ranges, less than 30 cm (1 ft).

Fluorescent lights located in the sensor's detection envelope, especially at distances of less than 3 m (10 ft), may cause low-frequency Doppler shifts originating with reflections from the ionized gas within the fluorescent tubes. Blocking the line-of-sight path by metal having less than 0.6-cm (0.25-in) mesh or by a radio-frequency absorber eliminates such signal interference.

The following test can be performed to determine if the sensor rejects fluorescent-light interference. The sensor should be located 2 m (6.5 ft) from a fluorescent light and exposed to continuous fluorescent light for ten minutes followed by exposure to flickering fluorescent light for ten minutes. The microwave sensor is satisfactory if it operates without alarming under the described conditions.

Multiple transceivers facing approximately the same direction and placed such that their fields of view overlap provide the most effective protection. Orienting multiple sensors such that the transceivers do not face each other reduces the potential for cross talk. Manufacturers provide sensors on various frequencies as an alternative method for eliminating cross talk and the resulting nuisance alarms. Placing the sensors so that potential intruder motion is toward or away from the transceivers provides the greatest sensitivity.

5.1.3 Active Sonic Sensor

An active sonic sensor is a visible, audible volumetric sensor which can be deployed in a monostatic, bistatic, or multistatic configuration. The frequencies emitted are well within the hearing range of the human ear and are quite unpleasant. Some active sonic sensors emit a pain-level warble of 135 dB when they alarm. Such features make the active sonic sensor unsuitable for use in or near areas where people are working, such as warehouses next to offices or houses; but such a sensor has the potential advantage of discouraging intruders with its irritating sound.

Because it utilizes the composite returned wave to detect changes in the contents of a volume, the active sonic sensor may be employed as a boundary-penetration detector as well as a volumetric detector. Movement of a wall or breaking through a wall changes the composite wave and causes a detection.

5.1.3.1 Principles of Operation

An active sonic sensor is comparable to the ultrasonic and microwave sensors in that it operates by sensing acoustic wave changes caused by target motion. The audible signal is emitted at frequencies between 500 and 1000 Hz. Wavelengths of 30 to 60 cm (1 to 2 ft) are employed to provide good reflection from most building materials. Three detection principles are employed by an active sonic sensor: total wave amplitude (envelope detection), Doppler frequency shift, and total wave phase changes (phase detection). All three principles are usually incorporated in a single unit, making the sensor extremely sensitive to intruder motion.

For proper active sonic sensor operation, it is necessary to establish standing waves to produce a reasonably large detection range. The very low transmitted frequency obtains good reflections, and standing waves are established in the protected volume even in the monostatic configuration. The standing wave pattern fills the protected room and provides a wide detection range with no shadow zones.

Typical detection patterns for a monostatic active sonic sensor are shown in Figure 5-6. An active sonic sensor is primarily produced as a bistatic or multistatic system; but, because of the low frequencies employed, a single speaker/microphone in a monostatic configuration produces good reflections in the protected volume. In the bistatic and multistatic configurations, slave speakers are employed with a master control unit.

Intruder motion causes the reflected energy from the intruder to exhibit a Doppler frequency shift as described in Section 5.1.1. Experiments performed at frequencies from 500 Hz to 4 kHz have shown the best frequency for active sonic sensor operation to be approximately 1000 Hz.

5.1.3.2 Performance Characteristics

No direction of low sensitivity exists for an active sonic sensor because of the multiple reflections in its detection field. An active sonic sensor is most likely to be defeated by very slow motion of an intruder.

The active sonic sensor is less prone to nuisance alarms caused by air turbulence than are the ultrasonic and microwave sensors, because its longer signal wavelength is less prone to distortion. The longer wavelength also prevents detection of small animals, such as insects, cats, and rodents, and the resulting nuisance alarms. Penetration of the long wavelength into adjacent areas may cause nuisance alarms in other active sonic sensors. To prevent such nuisance alarms from propagating throughout the sensor system, protect large areas with a single sensor in a multistatic configuration or place sensors far enough apart so one does not interfere with another.

5.2 Passive Volumetric Detectors

5.2.1 Passive Infrared Sensor

The passive infrared (PIR) sensor is a visible volumetric detector. Four characteristics of infrared radiation are employed in PIR intrusion detection:

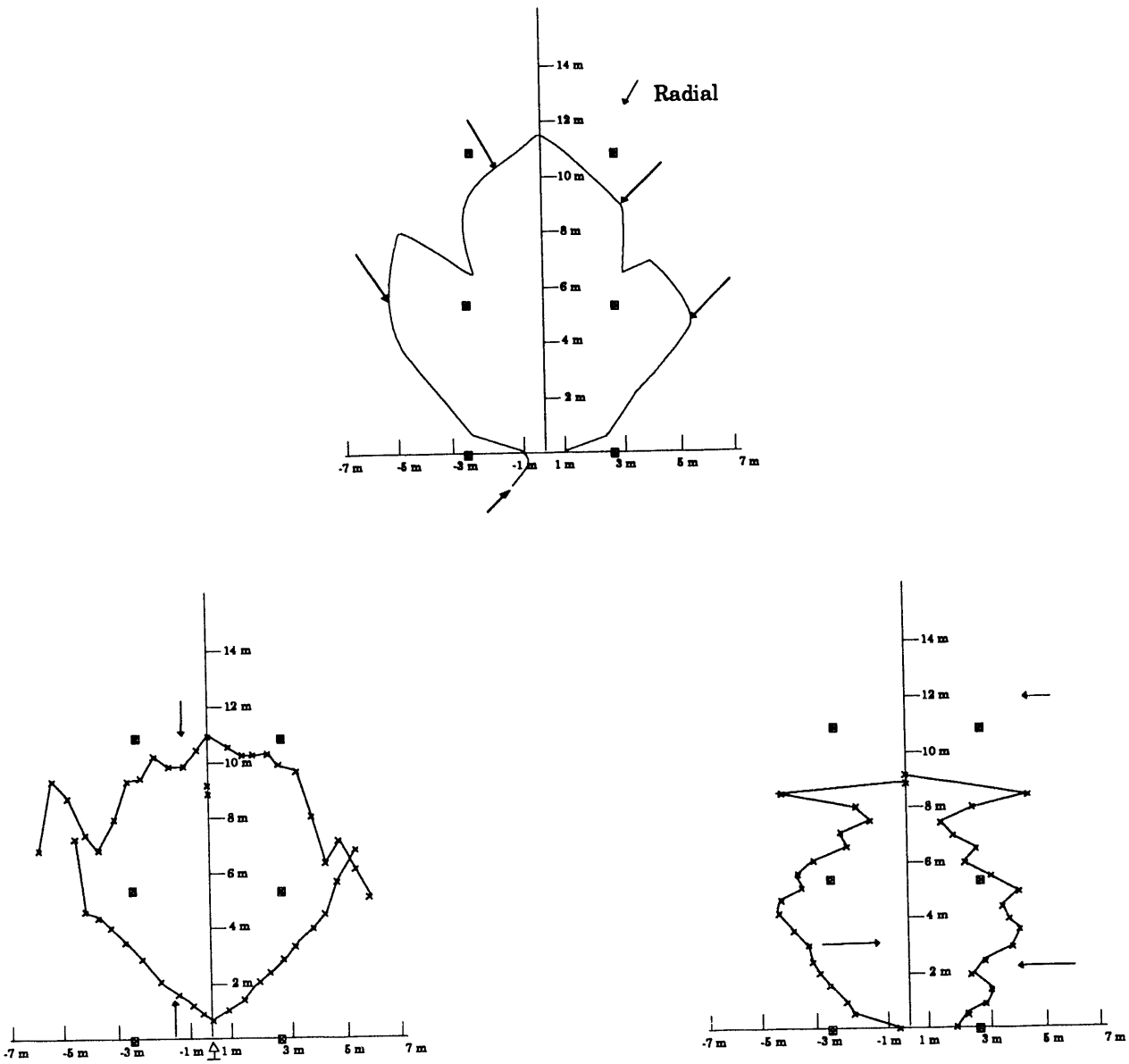
1. Infrared radiation emitted by an object is directly related to its temperature.

2. Infrared energy is transmitted without physical contact between the emitting and receiving surfaces.

3. Infrared energy warms the receiving surface and can be detected by any device capable of sensing a change in temperature.

4. Infrared radiation is invisible to the eye.

The relative radiation emitted by objects at different temperatures is shown in Figure 5-7. The visible region encompasses only those wavelengths between 0.45 and 0.75 micrometer. The infrared region lies



Note: Arrows indicate walk test direction.

Figure 5-6. Detection patterns for an active sonic sensor

between 0.75 and 1000 micrometers. Although the peak energy of the sun is in the visible region, most of its radiant energy is infrared. The human body radiates infrared energy in the 8- to 14-micrometer region. Even apparently cold objects such as dry ice and liquid air emit infrared radiation.

A PIR sensor detects the movement of an object through its field of view when an object has a different temperature than the temperature of the background. The sensor does not transmit a signal for interruption or reflection. Instead, the sensor responds to the energy emitted by a human intruder, which is approximately equivalent to the heat radiated by a 50-W light bulb.

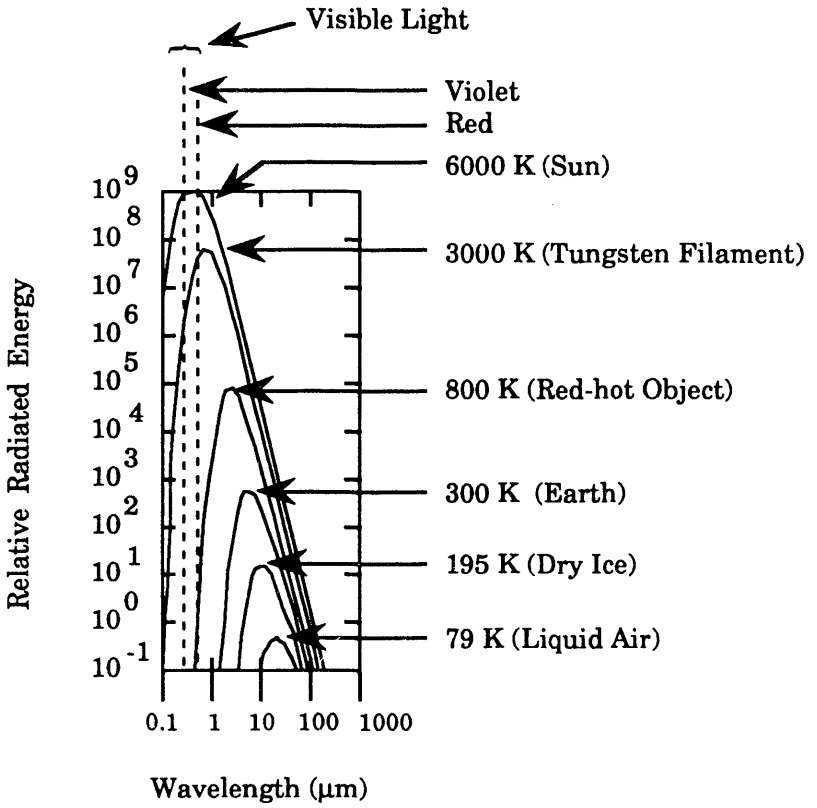


Figure 5-7. Family of curves showing energy versus wavelength for radiation emitted by objects at various temperatures

An infrared curtain sensor may also be used as a point detector. A sensor mounted on the ceiling surrounds an object on the floor with an invisible curtain. An alarm is generated when someone approaches or reaches out to touch the object.

5.2.1.1 Principles of Operation

The PIR sensor responds to the heat energy emitted by a human body or to changes in background radiation caused by a person blocking out the background in the sensor's field of view. A typical PIR detection pattern is shown in Figure 5-8. Subdivision of the pattern into the solid angular segments shown is accomplished optically to allow the detection of motion between the segments. The range of the multiple-beam sensor is 6 to 9 m with a 70° - 120° beamwidth.

By properly designing the optics, the PIR sensor's field of view can be tailored to provide various coverage patterns, such as a single segment, a curtain, or a hemisphere. A sensor having a single sensitive zone has a range of 15 to 18 m and is well suited for use in a hallway or a corridor.

A PIR sensor may be used as a boundary penetration sensor, called an infrared curtain sensor, when its detection envelope is configured to be much wider in one direction than the other. Its curtain of protection can be positioned to extend along a wall or a ceiling to detect an intruder entering the structure through the wall or the ceiling. The curtain may also be positioned in space to generate an alarm when the invisible curtain is interrupted. A curtain positioned in a doorway, such as the one shown in Figure 5-9, becomes an automatic door bell when coupled to an audible signaling device.

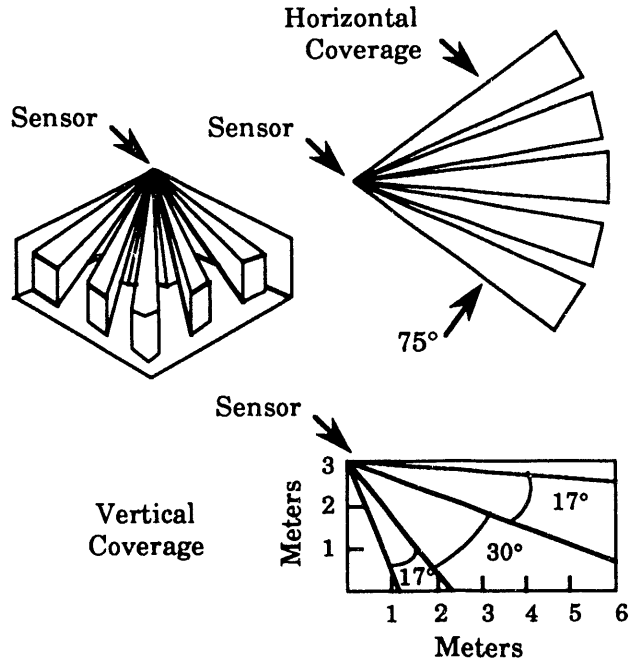


Figure 5-8. Typical PIR detection pattern

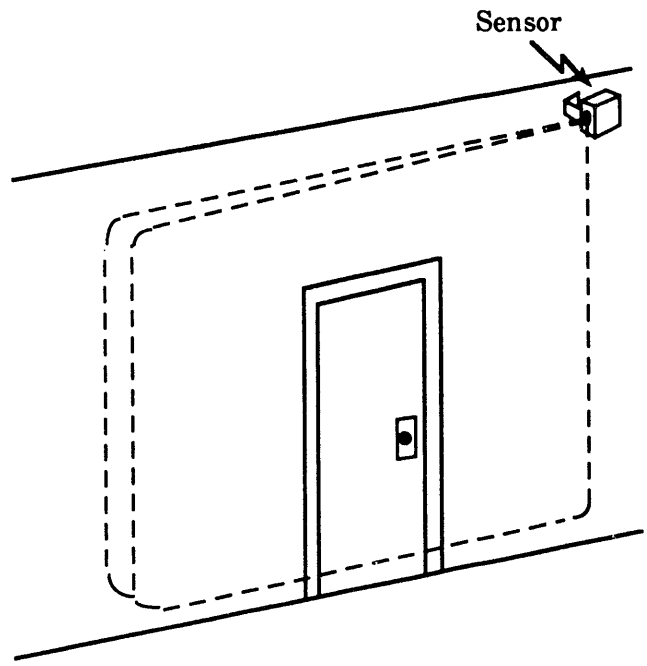


Figure 5-9. Field of view for a PIR curtain sensor

The sensor optics generally employ front-coated mirrors because infrared energy is significantly attenuated when passed through glass. Usually the mirror is plated onto molded plastic for ruggedness and to reduce the cost. Additional focusing may be accomplished by using a Fresnel lens. At the focus of the optics, an infrared-sensitive phototransistor is employed to convert the infrared energy to an electrical signal. An amplifier may be employed here to increase the signal above the noise level.

The electrical signal varies as a heat source moves out of one sensitive zone into the next, providing detection of a heat source in motion. Logic circuitry is usually applied to the received signal to differentiate among various situations. If the signal pattern matches that of a person in motion rather than generalized heating and cooling, an alarm is generated. The PIR sensor is more sensitive to motion across the field of view than to motion toward or away from the sensor.

5.2.1.2 Performance Characteristics

A PIR sensor requires a minimum temperature differential between an intruder and the background in order to provide a detection. An intruder who appears to be the same temperature as the background is invisible to the sensor. Good housekeeping practices prevent the accumulation of clothing or other covering materials that have equilibrated to the room temperature and which could be used as a screen to spoof the sensor. The sensor can also be defeated by very slow motion of the intruder.

Since PIR sensor operation is primarily geometric, its field of view can be masked by applying tape to portions of the optics. Tape is used legitimately to eliminate trouble-causing spots in the field of view, but tape could also be applied covertly to prevent proper operation.

Any object displaying the appropriate temperature differential can generate nuisance alarms in a PIR sensor. The required temperature differential may be caused by rapid localized heating and cooling effected by sunlight, incandescent light bulbs, radiators, space heaters, HVAC vents, or hot pipes. The sensor adapts to nuisance alarm sources that exist over a period of minutes or more but may respond to short duration changes. In practice nuisance alarms are seldom generated by localized heating and cooling because the temperature does not usually change rapidly enough to generate an alarm.

Small animals or large insects moving in the PIR sensor's field of view may be detected. Devices displaying the required temperature differential and swaying in the sensor's field of view may also generate nuisance alarms. Vibration of the sensor may generate nuisance alarms by causing a heat source to appear to move. Insects crawling on the detector elements inside the sensor or condensation in the sensor may also cause nuisance alarms.

The detector elements in a PIR sensor may be subject to interference from varying electromagnetic fields generated by devices such as hand-held radios. However, infrared sensors are not generally subject to nuisance alarms caused by sound, vibration, electrical, or radio disturbances.

5.2.1.3 Installation Guidelines

Acceptance Testing

Specifications for acceptance testing are outlined in the *NILECJ Standard for Infrared Motion Detectors*. In addition to the acceptance tests identified in Section 9, Procurement Guidelines, the following tests should be performed:

Short Wavelength Cutoff

It is unacceptable for the detector to alarm when exposed to the radiation which passes through window glass. Place a piece of clear single-strength window glass in front of the detector window so that all radiation entering the detection window should pass through the glass. Move an intense source of radiation, such as a bare 100-W incandescent lamp, back and forth within the field of view at a position

that would, in the absence of the window glass, cause an alarm. The radiation source should be sufficiently removed from the detector so that local heating of the window glass (thus emission of infrared energy) does not result.

Stationary Source Test

Place a bare, 60-W incandescent lamp in an active zone near the center of the field of view of the detector, approximately 1 meter from the detector window. Turn the lamp on and off three times for alternate 30-second periods. The test is satisfactory if the detector does not alarm when exposed to this stationary source of changing thermal energy.

Minimum Detectable Temperature-Difference Test

The manufacturer will determine the minimum temperature difference which the sensor is capable of detecting. A description of the test, including details of the test fixture, the temperature stimuli, and the background infrared radiation, should be obtained.

Horizontal Ranges

The horizontal ranges determined by the walk test depend somewhat on the background infrared radiation level. A description of the environment during walk tests should be obtained from the manufacturer.

Site Preparation

In addition to the general site-preparation guidelines in Section 8, all hot spots which may generate infrared energy should be removed or shielded. Radiant energy from such sensors may produce thermal gradients that might change the background energy pattern. Hot spots may be open heating elements; incandescent light bulbs; direct sunlight on windows, floors, and walls; and convective heat currents. Sunlight may enter the area under protection directly through openings such as broken window panes, ventilation grids, and poorly fitting doors.

Installation

The actions outlined in this section should be followed for a PIR sensor in addition to the general installation guidelines described in Section 8. For the most sensitive intruder detection, aim the sensor so the path most likely to be taken by an intruder will be across the sensor's field of view rather than toward or away from the sensor. To prevent an intruder from circumventing the sensor, its detection envelope should not be smaller than the physical boundaries of the area under protection. Do not mount the detector directly above a doorway or a window or in any position that would allow an intruder access to the sensor from the rear. Such access would allow an intruder to mask or otherwise tamper with the sensor.

Avoid aiming the PIR sensor toward radiant heat sources, such as radiators, light bulbs, radiant heaters, or surfaces which receive direct sunlight. Placing the sensor near a light source may generate nuisance alarms caused by insects attracted to the light. A varied sensor background, such as alternating light and dark colors, provides greater sensitivity to intruders.

5.2.1.4 Maintenance Guidelines

In addition to the general maintenance guidelines outlined in Section 9, the sensor optics should be periodically cleaned. Frequent visual inspections ensure that no objects have been moved into a blocking position that would render the sensor inoperative.

5.2.2 Light-Level Sensor

A light-level sensor utilizes the ambient level of light in a volume as a reference to detect changes in the light level. Detectable changes occur when a light fixture is turned on or off or when an intruder blocks some of the light entering the volume or changes the light reflections within the area. Unless an intruder is very skilled, it is unlikely that an intrusion can be effected without introducing some change in the light in a volume. Light-level sensors consume very little power and can be operated from a small battery for a number of years before replacement is required.

5.2.2.1 Principles of Operation

A light-level sensor employs a light-sensitive element, such as a phototransistor or a photo electric cell, as the sensing element. Some light-level sensors employ optics to define a field of view, while others use the entire field of view of the light-sensitive surface without optics. The optics may consist of a lens, such as a Fresnel lens, utilized to gather light to the sensing element. In general, the more restricted the field of view, the greater is the sensor's sensitivity. A sensor with greater sensitivity requires less light for operation and less change in light for intrusion detection.

The light-level signal is amplified, and AC coupling is employed to eliminate the DC component and slowly changing components, such as day-to-night light variations. More quickly changing light levels are recognized by logic circuitry to initiate an output signal indicating an intrusion detection. The output signal may be a logic level but is commonly a relay actuation.

5.2.2.2 Performance Characteristics

Since light-level sensors respond to the existing light level in a volume, any change in the light in the volume generates an intrusion detection. Operations in the area which cause the light level to change under normal conditions generate nuisance alarms. Some nuisance alarms can be eliminated by using light-level sensors with optics that define the field of view. The most useful application for a light-level sensor is a darkened vault or a vault in which the light level remains constant and nothing moves to change the reflections within the room.

5.2.2.3 Installation Guidelines

Modification of the environment may be necessary to permit operation of a light-level sensor. If intrusion into a protected volume is likely to introduce light into the area, making the room dark will ensure detection of an intrusion. It may be necessary to block windows through which light can enter the protected volume in order to prevent motion outside the area from causing shadows that generate nuisance alarms.

A light-level sensor should be mounted so that the perimeter of the volume containing the sensor is within the sensor's detection envelope. If a lens is employed to restrict the sensor's field of view, the sensor should be rigidly mounted to ensure that the field of view is constant. The detection envelope should not contain changing sources of light. Multiple sensors may be installed in an area without interaction since the sensor is passive.

5.2.3 Video Motion Detection

A video motion detector is a passive sensor that processes the video signal from a closed-circuit television (CCTV) camera. A single camera installed to view the scene of interest may be jointly utilized for detection, surveillance, and alarm assessment. Artificial lighting is required for continuous 24-hour operation.

5.2.3.1 Principles of Operation

A video motion detector (VMD) is an electronic device that monitors a video camera signal and detects changes in brightness in a video scene. During setup of a typical VMD system, as illustrated in Figure 5-10, an area within the video scene is defined for motion detection. The size of this detection area can usually be varied over a wide range as a percentage of the total camera field of view. A change is detected when the brightness of the detection area becomes either lower or higher than a stored reference level by a predetermined threshold. Depending on the complexity of the VMD system, an external alarm is generated either at the time of detection of the change or after a number of additional conditions are satisfied. Once an alarm is generated, the VMD highlights the section where the detection has occurred on the CCTV monitor to aid the responsible security guard to assess the alarm (Figure 5-11).

A variety of video motion detectors is available in the commercial market, each with its own unique operational characteristics. VMDs can be divided into two basic types: analog and digital. Analog video motion detectors have been in existence longer, and they are more simple and less expensive. Digital VMDs are more complex, more expensive, and usually have greater performance capability and features.

Analog Video Motion Detectors

Analog VMDs typically monitor changes in one entire detection area. The video signal level in the detection area is averaged and then compared to a previously stored, average reference level. The reference level is obtained by the VMD at start-up and is continuously updated in small increments in order to compensate for very slow changes in scene illumination. An alarm is generated if the average brightness level is suddenly low - or higher than the reference level. The sensitivity or threshold setting is defined as the amount of cha..ge required for the VMD to generate an alarm.

Digital Video Motion Detectors

Digital systems divide the motion detection area into sections which may be referred to as cells, zones, dots, or boxes. These small sections are monitored for brightness level changes on an individual basis using digital processing. In most digital systems, a change in one small section does not generate an alarm; additional digital processing is usually performed before an alarm is declared. A few examples of this prealarm processing incorporated into various digital systems are

- tracking changes through a number of the small sections for logical intruder movement
- requiring a specified number of small sections to change simultaneously

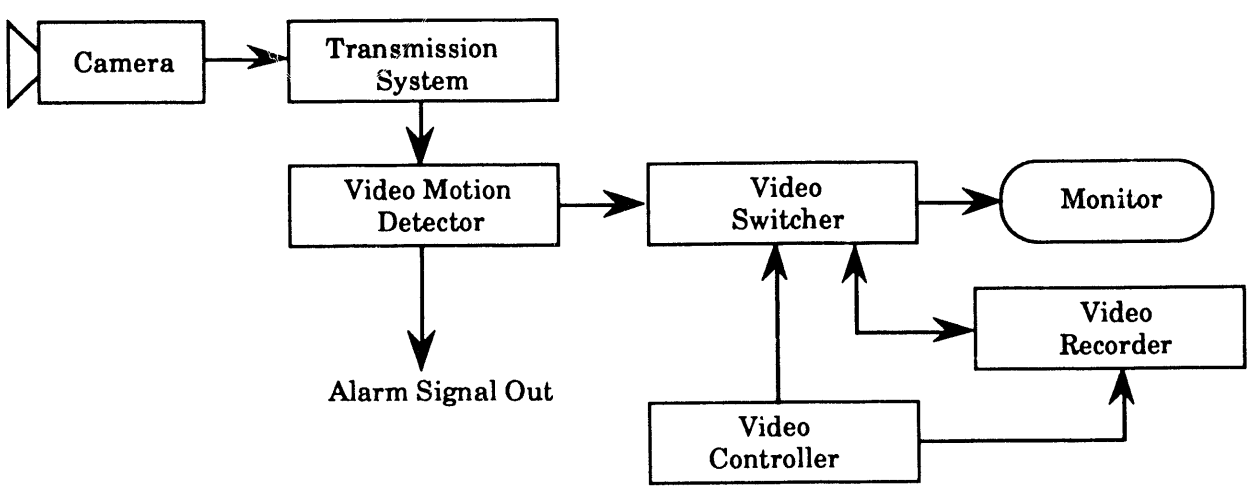


Figure 5-10. Typical VMD installation within a video assessment system

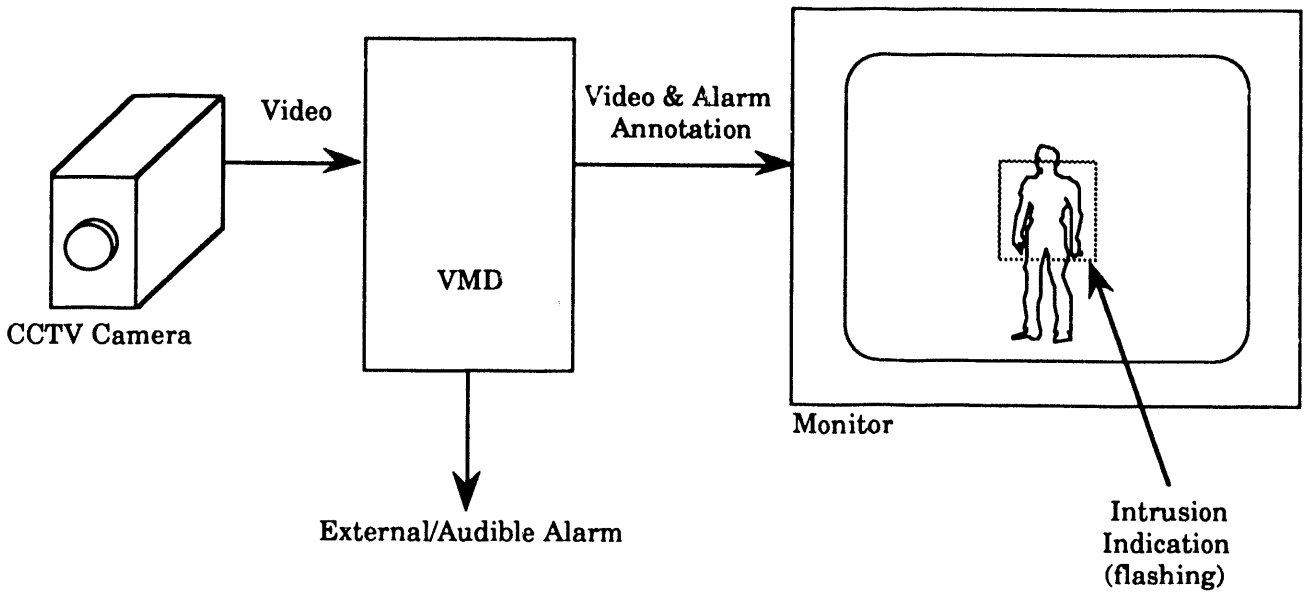


Figure 5-11. A typical video motion detector

- determining object size by the number of small sections changing simultaneously
- determining if a global change occurred by checking whether or not all small areas changed at the same time
- filtering out high velocity objects, such as flying insects

Prealarm processing is aimed at reducing the NAR while maintaining good detection capability. The amount of prealarm processing varies widely among the available systems.

5.2.3.2 Performance Characteristics

Video motion detectors can be set up and adjusted for high detection capability. During setup, the minimum relative contrast and size of an object to be detected should be considered. Because of camera lens perspective, objects look smaller as they move away from the camera. In less sophisticated VMD systems, this creates varying sensitivity with respect to distance from the camera. In the more sophisticated digital systems, compensation for lens perspective results in fairly even sensitivity throughout a detection area. The detection area is dependent on the type of VMD but generally comprises 20 to 100 percent of the monitor screen.

If an object casts a shadow into a portion of a camera scene, camera averaging characteristics can cause low contrast and thus reduce detection within the shadow area. The best results have been obtained with a relatively featureless detection area.

The assessment camera is an integral part of a VMD sensor system. Camera characteristics affect both detection capability and NAR. A low contrast output from a camera reduces detection capability. High noise levels from a camera can increase nuisance alarms. Enough light is required for proper operation of CCTV cameras, and the light should be uniform to avoid excessively dark or light areas. When the camera view is obscured, such as during failure of lighting, a VMD may have severely reduced capabilities. During times when the camera view is obscured, a VMD system is easily defeated. Other defeat methods do exist but require technical knowledge of the particular system in use.

Since a VMD detects changes in the video brightness level, any change can cause an alarm. Flickering lights, camera movement, etc. can lead to excessively high NARs.

Very slow movement through the detection area can defeat most VMDs. This requires an intruder to remain in the detection/assessment area for a very long time, perhaps allowing for detection by another method. The actual velocity required for defeat depends on the system and at times on the type of lighting; velocities of 8 to 13 cm/sec (3 to 5 in/sec) have been shown to defeat various VMD systems.

5.2.3.3 Installation Guidelines

Many VMDs are effective for interior applications with controlled lighting. The following installation factors and site characteristics should be evaluated before selecting a VMD:

- number of objects in the detection area
- amount of shadowing caused by nearby objects
- vibration of the camera
- traffic flow near the detection area
- moving objects, such as fans, curtains, and small animals

Some advantages of using video motion detection are the ease and low cost of installation if CCTV already exists or is planned. The installation cost is much lower than for other sensor technologies because there is no hardware or cabling to install in the field. However some VMD systems require the cameras to be synchronized to the video motion detector. Such VMD systems generate sync signals that require sync distribution and protection equipment and additional cables to the cameras.

5.2.3.4 Performance Testing

Performance testing is required to establish proper settings for both high detection probabilities and the lowest possible NAR. Detection tests should be performed with a low profile target, such as a crawler, and with a high velocity target, such as a fast runner. Such tests should be performed under the lowest contrast lighting conditions expected, such as at night under artificial light. If any detection areas are partially covered by a shadow, testing should be performed within the shadow.

Some digital systems have operator-adjustable parameters for nuisance-alarm rejection features. Such parameters can also affect detection. Additional testing of the system at various settings will provide an understanding of system operation for optimum detection and the lowest possible NAR.

5.2.3.5 Maintenance Guidelines

Maintenance of VMD equipment is generally minimal. All maintenance guidelines established by the manufacturer should be followed.

Proper maintenance of associated CCTV cameras and equipment is important. All exposed camera optics should be cleaned. Measurements to ensure proper video signal levels should be made periodically. Checks to ensure that the camera is aimed properly and checks for VMD detection-area coverage should be performed often. Periodic low-contrast walk, run, and crawl tests are necessary.

The lighting system for operation of cameras should also be well maintained. Any light fixtures which are not operating properly should be repaired as soon as possible, because a nonoperating lamp could cause a hole in detection at night.

5.3 Dual-Technology Sensors

Dual-technology or combination sensors are motion detectors that combine a passive sensor, such as an infrared sensor, with an active sensor, such as an ultrasonic or a microwave sensor. Ideally, absolute alarm confirmation is achieved by combining two technologies that individually have a high P_d and do

not have common nuisance-alarm-producing stimuli. Manufacturers are currently combining the outputs of such sensors in a logical AND configuration, requiring nearly simultaneous alarms from the combined sensors to produce a valid alarm. If one technology of the sensor is defeated or fails, then the whole sensor is defeated. Employing a time window that evaluates the sensor outputs according to time received reduces the dual-technology sensor's NAR.

When sensors are combined in a logical AND configuration, the P_d for the combined detectors is less than the P_d of the individual detectors. If an ultrasonic sensor with a 0.95 P_d is combined with a PIR sensor having a 0.95 P_d, the resulting 0.90 P_d for the dual-technology sensor is the product of the individual probabilities. See Section 7 for a more complete discussion of the logical combination of sensors.

A higher Pd may be obtained from separately mounted, logically combined sensors than from a dual-technology sensor. Ultrasonic and microwave sensors have their highest P_d for motion radially toward and away from the sensor, but a PIR sensor has its highest P_d for motion circumferentially across its field of view. Thus the P_d for the sensors combined in a single unit and aimed in the same direction is less than the P_d for individual detectors mounted perpendicular to each other with overlapping detection envelopes. The highest P_d is achieved by annunciating the individual sensors separately.

6 POINT PROTECTION

Point protection, also known as proximity detection, employs sensors in the proximity of a protected object. In an IIDS (interior intrusion detection system), the point sensors form the third layer of protection encountered by an intruder, after boundary-penetration sensors and volumetric sensors.

Capacitance proximity sensors, pressure sensors, and strain sensors are commonly employed for point protection, but a number of sensors which have previously been discussed as boundary-penetration and volumetric sensors are readily applicable to point protection.

6.1 Boundary-Penetration Sensors

Point protection may be accomplished by surrounding a protected object with an enclosure protected by a boundary-penetration sensor. An alarm is generated by the sensor when the enclosure is breached. Enclosing a protected object in a glass case and mounting a glass-break sensor on the case provides point protection for the object. A passive-sonic glass-break sensor is able to monitor several glass cases concurrently.

Point protection is provided by surrounding a protected object with light-beam sensors to detect any attempt to touch the object. One infrared light-beam sensor employs the time of flight of reflected light to create a small protective zone. Moving the protected object within the zone or removing it from the zone changes the reflection parameters and generates an intrusion alarm.

A mechanical switch, such as a spring-loaded switch affixed to a display or mounting platform, provides point protection. The object to be protected is placed such that its weight or position maintains switch closure. Removal of the object causes the switch to change state and produce an alarm.

6.2 Volumetric Sensors

A volumetric sensor may be set at a very limited range, perhaps only a few inches, so that detection occurs only when an attempt is actually being made to touch the protected object. An invisible curtain generated by one or more microwave or passive infrared sensors can also provide point protection for a relatively small object. An attempt to touch the object would interrupt the curtain and generate an intrusion alarm. Museums often utilize such sensors to protect their displays.

6.3 Capacitance Proximity Sensor

A capacitance proximity sensor is an active, covert point sensor employed to detect unauthorized access to a conducting medium, such as a metal object. An attempt to touch or move the object results in an intrusion detection. Such sensors may be utilized to protect an object as large as a 747 aircraft or as small as a quarter ($.25).

The capacitance proximity sensor is usually connected directly to the protected object, which should be insulated from ground. If the protected object should be grounded, it may be covered with a protection blanket which incorporates a conducting layer connected to the proximity sensor. Such blankets may employ the earth's magnetic field or the capacitance between the blanket and the object as the detection medium. Touching the blanket or moving it with respect to the protected object results in an intrusion detection.

The capacitance proximity sensor may also provide boundary-penetration detection for HVAC grills and ducts, metal window frames and doors, or the walls of a building. A wall protected by a capacitance proximity sensor should be covered by or impregnated with a conducting surface, such as a wire grid stapled to the wall and covered with paneling for physical protection. Chicken wire embedded in security glass can be connected to the sensor electronics.

6.3.1 Principles of Operation

A capacitance proximity sensor operates on the same principle employed by an electrical capacitor. An electrical capacitor comprises two conductor plates separated by a dielectric medium. A change in the electrical charge of the dielectric medium causes a change in the capacitance between the two plates. In the case of the capacitance proximity sensor, the protected metal object corresponds to one plate, and an electrical reference ground plane under and around the protected object corresponds to the second plate. An insulator isolates the protected object from ground. The air between the object and ground comprises the dielectric medium.

The capacitance proximity sensor operates by electrically charging the metal object 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 charge as the intruder approaches or touches the object.

The control unit of a capacitance proximity sensor employs an electronic oscillator that utilizes the capacitance of the protected surface as a frequency-determining element for the oscillator. The frequency of oscillation varies from approximately 10 to 40 kHz. A loop of wire, known as the protection loop, is connected between the protected object and the tuned circuit in the control unit. The tuned circuit is adjusted to resonance either automatically or manually with a potentiometer.

The change in capacitance between the protected object and ground, caused by the approach of an intruder or another conducting object, causes a disturbance of the resonance condition. If a detected change is of sufficient magnitude, usually less than 10 pF and in some cases as low as 1 pF, an intrusion alarm is generated.

The amount of surface area that can be protected by a capacitance proximity sensor depends on the capacitance to ground of the conducting surface, which may be as high as 100,000 pF for some sensors. A single sensor can monitor multiple surfaces, provided all the surfaces are connected by wire and none is connected to earth ground, as illustrated in Figure 6-1.

The distance from the protected surface at which detection occurs depends upon the rate of approach. The circuit attempts to balance itself and does not detect easily when approached very slowly. The quick, large capacitance change caused by touching the protected surface, even by a slow-moving intruder, generates an alarm because capacitance change is an exponential function. A fail-safe configuration is provided for the sensor such that an intrusion, a loss of power, or a break in the protection loop generates an alarm. The alarm output may be a logic level or a relay actuation.

6.3.2 Performance Characteristics

A self-adjusting capacitance proximity sensor may be defeated by extremely slow approach to the protected object. An adversary can detect the presence of a capacitance proximity sensor by employing RF-field-sensing equipment like that used by a telephone company to find underground telephone cables.

Relocating any conducting object closer to or farther away from the protected surface may cause a small capacitance change between the protected surface and ground, generating a nuisance alarm. Such objects include persons walking near or leaning on the surface, cabinets or other objects being moved close to the surface, or loose-fitting components of the protected object itself.

The sensitivity of a capacitance proximity sensor is affected by changes in the relative humidity. Such changes vary the dielectric characteristics of air by either increasing or decreasing its conductivity. If the sensor's sensitivity is adjusted to detect an intruder several meters from the object, the change in conductivity may be enough to initiate a nuisance alarm. Capacitance proximity sensors employing a self-balancing circuit adjust automatically to changes in relative humidity and to relocation of conducting objects near the protected object.

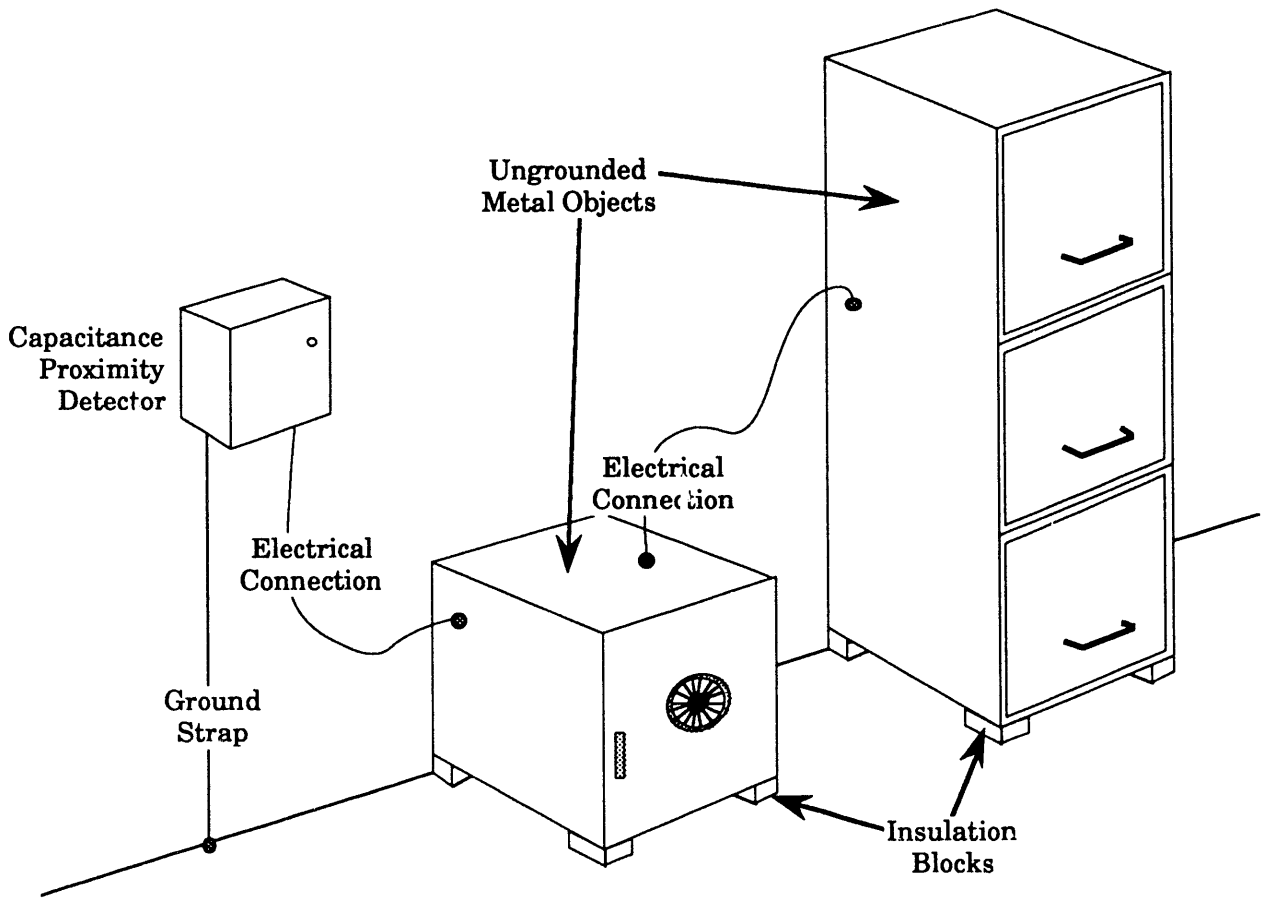


Figure 6-1. Typical connections of a capacitance proximity sensor

6.3.3 Installation Guidelines

The first step in installing a capacitance proximity sensor is establishment of the detecting surface. The object to be protected should be located away from walls and insulated from ground. Such isolation provides a minimum capacitance. Avoid using wooden blocks to isolate the protected object from ground. Moisture absorbed by wooden blocks over a period of time may change the dielectric enough that the object is no longer isolated from ground, resulting in nuisance alarms. If the floor is nonconductive, an electrically grounded conductive mat or foil should be placed on the floor under the object in order to provide a good ground reference plane.

For applications requiring the object to be grounded, the object is the ground plane, requiring the fabrication of a capacitive blanket to be draped over the protected object as shown in Figure 6-2. The conductive layer on the capacitive blanket should not come in contact with the grounded object or the building ground. The conductive-layer area compared to the insulated-layer thickness should result in an object-to-blanket capacitance which falls within the range of the sensor. If the blanket is large enough to cover the object entirely, any access attempts will cause blanket movement and/or capacitance change, resulting in an alarm.

The second installation step is connection of the detecting surface to the sensor control unit. All objects to be protected are connected to the protection loop with secure electrical connections to provide stable circuit reactance for tuning purposes. If the sensor cannot be tuned to a balanced condition, the total

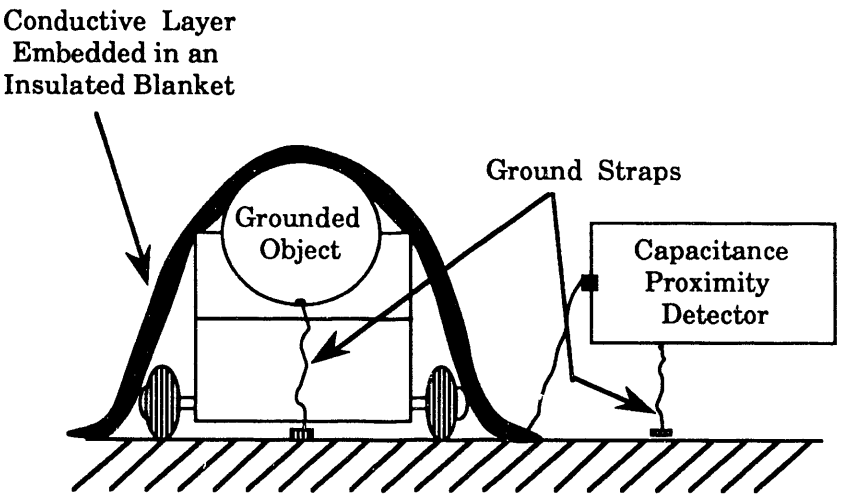


Figure 6-2. Capacitive blanket employed with a capacitance proximity sensor

capacitance load may be too large, requiring the protected surface to be divided among several sensors. Physically separating the sections prevents interaction among the sensor control units.

Performance testing is carried out to test the system for detection capability under conditions normally encountered in the location where it is installed. General sensor performance-testing guidelines are outlined in Section 8. The performance standard for a capacitance proximity sensor typically is detection of a human touch by a person wearing gloves and isolated from ground.

6.3.4 Maintenance Guidelines

In addition to the general maintenance guidelines described in Section 9, the following maintenance activities are recommended. Extremely good housekeeping is required in the proximity of the protected object because the capacitance proximity sensor is very sensitive to the environment within a few inches of the protected surface. Any conducting object large enough to change the capacity to ground of the protected surface should be removed. Wet mopping or liquids spilled on wooden floors under and around the protected object can change its capacitance significantly.

6.4 Pressure Sensors

A pressure sensor is a passive covert sensor which detects the presence of a load that has been placed upon it. The pressure sensor may be a spring-loaded switch or a pressure mat activated by the weight of the protected object. Removing the object results in a switch actuation, generating an intrusion alarm. Alternatively, the pressure sensor may be a pressure mat or hose placed beside the protected object to detect the weight of an intruder.

A pressure sensor may be used as a boundary-penetration sensor. Pressure mats may be placed in doorways as illustrated in Figure 6-3 or in other likely intruder paths around the boundary of an area under protection. In a form resembling a gas station hose, a pressure sensor may encircle the boundary of the area under protection. Pressure sensors are not widely used as boundary-penetration sensors because of size limitations.

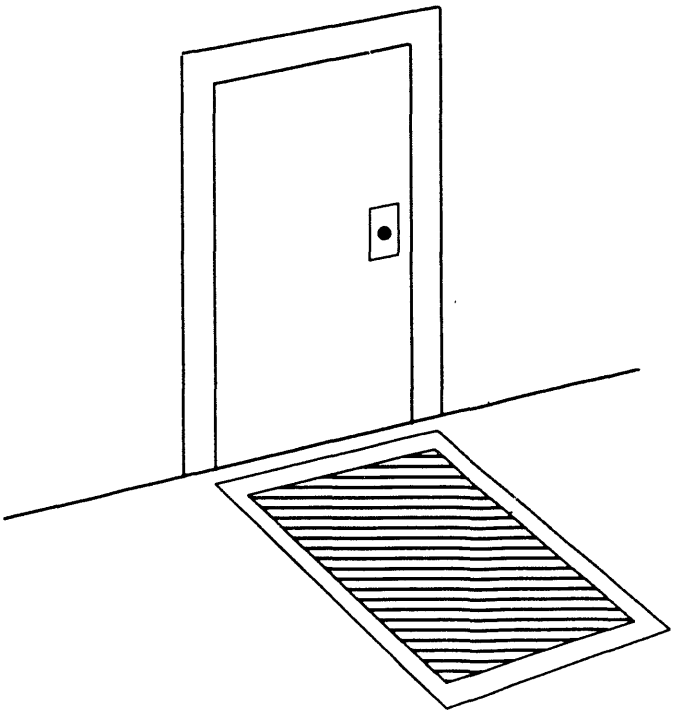


Figure 6-3. Typical pressure mat installed in a doorway

6.4.1 Principles of Operation

A pressure sensor incorporates a sensing device that responds to deformation of the sensor caused by a weight placed upon it. The operation of a pressure mat is representative of the operation of pressure sensors in general.

An electrical pressure mat contains a long electrical switch, consisting of two ribbon conductors separated by compressible foam pads spaced at intervals along the length of the switch. When pressure is applied to the pad, the foam compresses and the ribbon conductors touch each other, resulting in a switch closure which can be used to operate an annunciating device such as an alarm bell.

A mechanical pressure mat contains a hose filled with a gas, such as air, or a fluid. The hose follows a serpentine path through the mat. When weight is applied to the pad, the hose is compressed, reducing the volume and increasing the pressure in the system. The increase in pressure is sensed by means of a pressure switch which operates a device such as an alarm bell.

The pressure sensor's output signal can be routed to an alarm console or other alarm system to indicate to the console operator that assessment is necessary.

6.4.2 Performance Characteristics

A pressure sensor is vulnerable to bridging, e.g., by a board placed on bricks, or by jumping or stepping across it.

6.4.3 Installation Guidelines

The pressure sensor is usually concealed from an intruder by its appearance as a doormat or by placing it under a disguising cover, such as tile or linoleum. Installing a pressure sensor in the path that an intruder is likely to take ensures detection. The pad is manufactured as a unit that is usually installed in a depression in a concrete floor and becomes a part of the floor. If the mat is supplied in a roll, such as tapeswitch, it is placed under a protective cover, such as a rug or a rubber welcome mat. The protective cover should be fastened down around the edges to prevent the mat from being moved around by traffic or from being removed. If the pressure sensor is a hose, it is clamped to the surface of the path, and no attempt is made to conceal its location. The electrical wiring or hose extending from the pad should be routed to prevent damage or tampering. A pressure sensor is subject to considerable wear from normal traffic, and periodic tests should be performed to ensure that the sensor is operating effectively.

6.5 Strain Sensor

A strain sensor applies a strain gauge as a point sensor. A strain gauge is a piezoresistive sensor utilizing the principle that the resistance of a conductor or a semiconductor varies with the strain applied to it. Semiconductors have much higher sensitivity than conductors and are therefore more commonly used in this application.

As a boundary-penetration sensor, a strain sensor is applied to a surface that is expected to flex when an intruder attempts to enter an area under protection, such as to roof or floor joists or to stairways as shown in Figure 6-4. The strain sensor can be applied to walls; but other sensors, such as vibration sensors, are usually better suited for such applications. Strain sensors are not applied to concrete because concrete flexes only very slightly under the weight of a human and would require operating the sensor with very high sensitivity, resulting in the generation of a large number of nuisance alarms. However, a strain sensor attached to a concrete roof should easily detect helicopter landings on the roof.

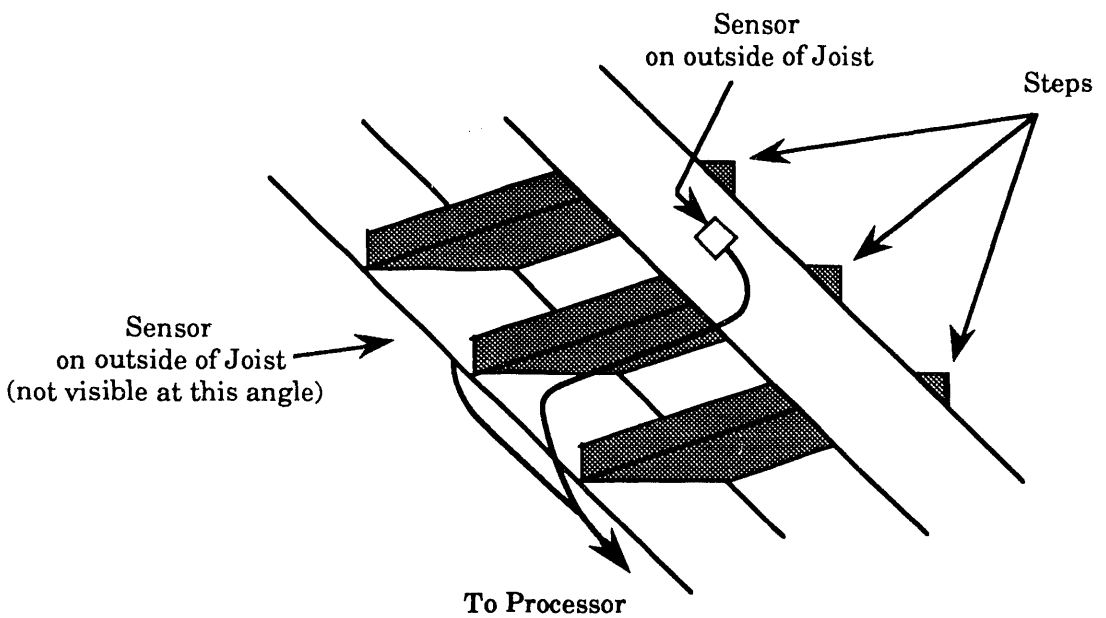


Figure 6-4. Application of a strain sensor to a stairway

6.5.1 Principles of Operation

A strain sensor is attached to a surface that will flex under the weight of an intruder. When the surface flexes, the attached strain gauge is elongated or contracted, causing its resistance to change (piezoresistance). The electronics associated with a strain sensor include a strain-gauge bridge, logic and filtering circuits, and drivers for an output indication. The sensor is one or more arms of a resistance bridge, like the one illustrated in Figure 6-5. The output of the bridge circuit is amplified and applied to logic circuits. If the proper combination of frequency, amplitude, and duration is observed, an output is generated from the sensor. That output can be a logic level or a relay actuation.

6.5.2 Performance Characteristics

A strain sensor responds to any action that causes the surface upon which it is mounted to flex. Heavy machinery in operation in the protected building or vehicular traffic adjacent to the building can be sources of nuisance detections. Although the sensor has response down to very low frequencies, limiting the low-frequency response avoids responses to long-term drift, slow deformation of the structure over time, or even moving the furniture. The sensor should not be applied in areas where activities in adjacent rooms could cause the sensed surfaces to flex.

6.5.3 Installation Guidelines

A strain sensor is mounted on the surface it has been selected to protect. Since the sensor detects deformation of the surface, the sensor should be mounted at the point where the largest deflection of the surface is most likely to occur. If that point cannot be defined, then the best procedure is to mount the sensor in the center of the surface. The sensor is bonded to the surface as rigidly as possible so that when the surface flexes the sensor will be forced to elongate or contract and will not slide along the surface or separate from it. Each sensor requires its own bridge amplifier and bridge power supply.

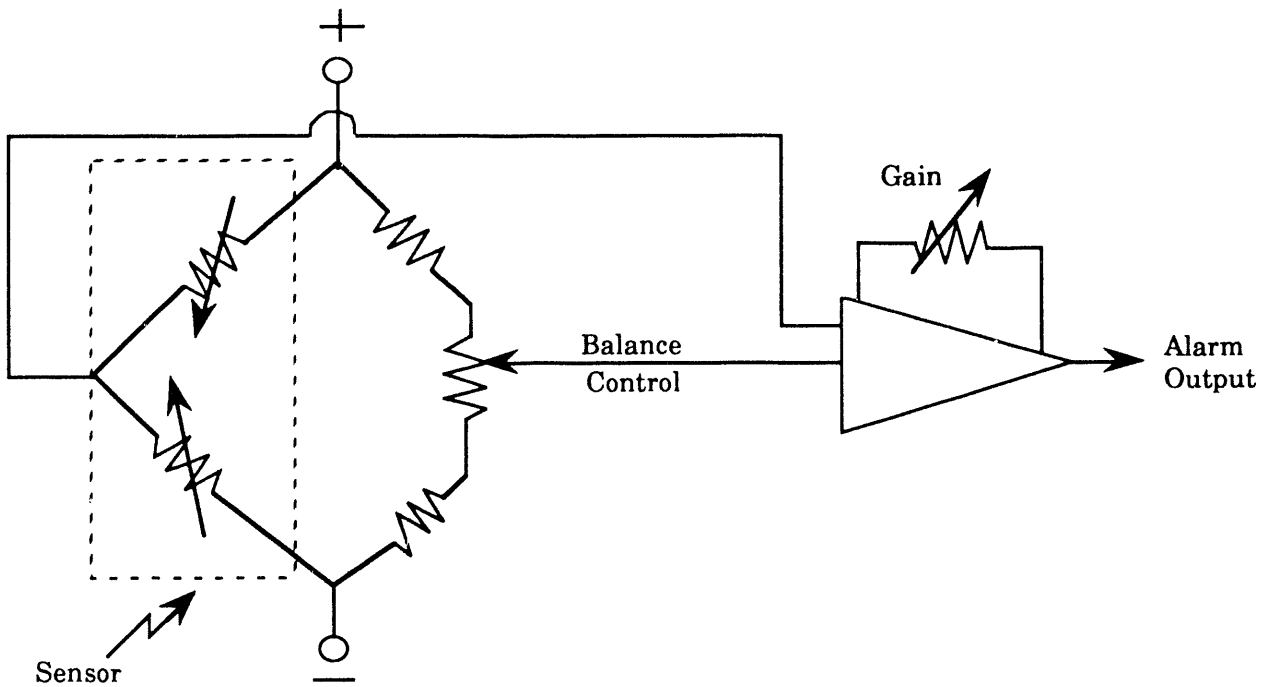


Figure 6-5. Typical strain-sensor bridge configuration

7 LOGICAL COMBINATION OF SENSOR ALARMS

A sensor or sensor system should have a high P_d for all expected types of intrusion and a low NAR for all expected environmental conditions. No single interior sensor presently available meets both of these criteria; all are limited in their detection capability and all have high NARs under certain operating conditions. For this reason, multiple sensors are recommended for an IIDS. A variety of technological sensor types are generally chosen so that the same defeat methods cannot be used on the sensors and so that sensors have different nuisance alarm sources. All sectors of the IIDS should have approximately the same detection capability and the same immunity to defeat.

Site characteristics may severely limit which sensors appear applicable. It is conceivable that during sensor selection all sensor types will be judged unacceptable; then the sensor selection process should be repeated to select sensors with the fewest negative and the most positive qualities. Although it is recommended that the logical combination of alarms be approached with caution, the methods discussed in Section 7 may alleviate the problem if site characteristics yield a higher than acceptable NAR.

Current technology makes it possible to select sensors for most sites to yield an acceptably low NAR under most conditions. The hierarchical scheme, also called priority scheme, is the preferred method of nuisance alarm reduction discussed in this section because no alarm information is lost, it is only prioritized. Nevertheless, the pros and cons of various methods of logical alarm combination and priority generation are discussed.

7.1 Factors That Affect P_d and NAR

The P_d and NAR of a sensor both tend to increase as the sensor sensitivity is increased. Both characteristics are also dependent upon installation parameters. Table 7-1 shows estimates of the detection capability of sensors discussed in this report for various types of intrusions. The tabulation indicates that a sensor's P_d depends upon the actions of the intruder. The relative susceptibility to nuisance alarms is shown in Table 7-2 for sensors installed with sensitivity set to detect the crawling intruder. Both tables represent the experience of Sandia National Laboratories.

Sensors can be combined to achieve an acceptably high system P_d for various types of intrusions and a low system NAR. In addition to the detection capability and NAR characteristics of the sensors, the vulnerability to defeat should be considered for each sensor and for the combination of sensors. The variety of sensors, variations in installation and adjustment, several types of combination logic, and the possible addition of barriers result in a large number of combinations and permutations.

Some of the basic techniques for combining sensors include

- hierarchical schemes
- OR combination
- AND combination, including majority logic such as "two-of-three sensors"
- composite AND-OR combination

Table 7-1. Estimates of detection capability

	Sensor	Walking	Slow Walk	Running	Crawling	Roll	Cutting
Boundary-penetration	Glass-Break	NA	NA	NA	NA	NA	M [1]
	Continuity	NA	NA	NA	NA	NA	H
	Infrasonic	L	VL	L	VL	VL	L
	Light-Beam	VH	VH	VH	H	H	NA
	Magnetic Switch: BMS	VH	VH	VH	NA	NA	VL
	Magnetic Switch: Simple	VH	VH	VH	NA	NA	NA
	Mechanical Switches	VH	VH	VH	NA	NA	NA
	Passive Sonic	H	H	H	M	M	H
	Passive Ultrasonic	NA	NA	NA	NA	NA	H
	Seismic	NA	NA	NA	NA	NA	H
	Vibration	NA	NA	NA	NA	NA	H
Volumetric	Active Sonic	H	M	H	M	M	M
	Light-Level	M	L	L	L	L	L
	Microwave	H	H	H	M	M	NA
	PIR	H	H	H	M	M	NA
	Ultrasonic	H	H	H	M	M	NA
	VMD	H	H	H	M	M	NA
Point	Capacitance Proximity	H	M	H	NA	NA	H
	Pressure Switch	H	H	H	H	H	H
	Strain	H	H	H	H	H	L

Key: VH - very high L - low
H - high VL - very low
M - medium NA - not applicable

[1] High for Breaking

Table 7-2. Relative susceptibility to nuisance alarms

	Sensor	Environment			Animals Small	Electrical Interference			Seismic
		Wind	Temp	RH		Lightning	Power	RF	
Boundary-penetration	Glass-Break	L	VL	VL	VL	L	L	L	L
	Continuity	VL	VL	VL	VL	VL	VL	VL	VL
	Infrasonic	H	L	L	L	L	L	L	L-M
	Light-Beam	L	L	L	M	L	L	L	L
	Magnetic Switch: BMS	VL	VL	VL	VL	L	L	L	L-M
	Magnetic Switch: Simple	VL	VL	VL	VL	L	L	L	L
	Mechanical Switches	VL	VL	VL	VL	L	L	L	L
	Passive Sonic	M	L	L	M	L	L	L	L
	Passive Ultrasonic	M	L	L	M-H	L	L	L	L
	Seismic	L-M	L	L	L	L	L	L	H
	Vibration	L-M	L	L	L	L	L	L	M-H
Volumetric	Active Sonic	M	L	L	L	L	L	L	L
	Light-Level	VL	VL	VL	L	M	L	L	VL
	Microwave	L	L	L	M	M	M	M	L
	PIR	L	H	L	M	M	M	M	L
	Ultrasonic	L	L	M	M	M	M	M	L
	VMD	L	L	L	M	M	M	M	L
Point	Capacitance Proximity	L	L	M	M	M	L	L	L-M
	Pressure Switch	L	L	L	L	L	L	L	L
	Strain	L	L	L	L	L	L	L	M

Key: H - high L - low
M - medium VL - very low

7.2 Hierarchical Schemes

The number and type of sensor outputs from an IIDS can provide graduated levels of system alarms which could require graduated responses from the guard force. For example

Level 1

Alarm: Any single sensor activation
Action: CCTV assessment as time permits

Level 2

Alarm: Any two sensors activated within a specified time window
Action: Immediate CCTV or protective force assessment

Level 3

Alarm: Activation of a boundary-penetration sensor and at least two volumetric sensors
Action: Immediate protective force response without waiting for CCTV assessment

One solution for a combination of sensors with the detection regions of the individual sensors not overlapping, uses a modified majority logic scheme with hierarchical output levels. Such a combination scheme includes different generic types of sensors so that nuisance alarms are uncorrelated. Specific sensor selection considers the NAR characteristics of each sensor type for the anticipated environmental conditions.

A typical sensor arrangement employing three levels of alarm indication places the sensor exhibiting the lowest NAR farthest from the protected object, followed by the sensor with the second lowest NAR. The remaining sensor is located closest to the protected object. When the first sensor alarms, a level-1 indication occurs and a time window is opened. A subsequent alarm on either of the two inner sensors during the time window results in a level-2 alarm.

All sensor alarm indications are employed in a hierarchical scheme. To allow for possible defeat of the first sensor, an alarm from the second sensor would output a level-1 alarm and open a time window. In that case an alarm from the third sensor during the time window would raise the alarm output to a level-2 indication. A level-1 indication occurs if the third sensor alarms without a concurrent alarm from either of the two outer sensors. The logic circuitry processes the sequence in which alarms occur and the relative times of alarm occurrence.

7.3 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 that make up for the detection deficiencies of each other; each sensor is intended to detect particular types of intrusions. Thus, individual sensors designed to detect a door opening, glass breaking, and breaking and entering intrusions should be combined by an OR gate.

The total nuisance alarm rate of the OR combination, NAR(OR), is greater than the NAR for each sensor. Neglecting the possibility of simultaneous activation,

$$NAR(OR) = \sum_{i=1}^{n} NAR_i \qquad (7\text{-}1)$$

where NAR_i is the nuisance alarm rate of the i'th sensor in a system of n sensors. Since this combination results in an increased NAR, it is most useful for sensors that individually have low NARs.

The OR combination can be used to ensure that compensation is provided for the vulnerabilities of each sensor. The vulnerability is reduced and the P_d increased for configurations in which the sensors are collocated.

7.4 AND Combination

Significant reductions in NAR can be accomplished by combining sensors with AND logic if the nuisance alarms of each sensor are not correlated. Since alarms activated from a single penetration attempt do not occur simultaneously, coincidence of outputs cannot be required. However, a system can be designed to generate an alarm if each sensor produces an output within a preselected time interval, T. A long time window is desirable to assure detection of slow-moving targets; but, if the window is too long, the NAR may not be sufficiently reduced. By installing sensors so their detection zones overlap or cover the same general area, the time window can be kept small.

Detection probability of the AND combination, $P_d(AND)$, is lower than the detection probability of each sensor. If detection performance is independent and coverage by n sensors is spatially overlapping,

$$P_d(AND) = \prod_{i=1}^{n} P_{di} \qquad (7\text{-}2)$$

where P_{di} is the probability of detection for the i'th sensor in the system of n sensors.

To assure a reasonable P_d for the system, the individual P_d for each sensor should be high. For example, if two sensors are used, the individual P_d should be 0.95 to assure a system $P_d(AND)$ of 0.90. This reduction in detection can be compensated for by increasing the sensitivity of each sensor. One advantage of the AND combination is that the sensors are normally operated in a sensitive mode.

The NAR of the AND combination, NAR(AND), will be less than the NAR of each sensor. If the sensor outputs are uncorrelated and occur at a random rate that is much less than one output per the selected interval, T, then for two sensors,

$$NAR(AND) = \frac{T}{60}(NAR\ 1)(NAR\ 2) \qquad (7\text{-}3)$$

where T is in minutes and NAR_1 and NAR_2 are in alarms per hour. Table 7-3 shows values of NAR(AND) for several combinations of two sensors. As indicated in this table, the AND combination is desirable because nuisance alarms can be reduced by several orders of magnitude. The time window, T, may be site specific, depending upon the installation geometry and sensor characteristics; however, it will probably be in the 0.25- to 2-minute range. Since sensor nuisance alarms are rarely completely uncorrelated, actual NARs are not as low as predicted by the equation above.

As previously mentioned, the AND combination should employ sensors whose alarms are uncorrelated, and the sensors should be installed so that the detection coverage is spatially overlapping. The choice of sensors should also consider the vulnerability to defeat, since spoof or bypass of one sensor results in no output alarm being generated.

The vulnerability to defeat for the AND combination of two sensors can be greatly reduced by employing three sensors and majority logic such that an alarm is generated by activation for any two of the three sensors. It would then be necessary for the intruder to defeat two of the three sensors; by using different types of sensors with different vulnerabilities, such defeat can be made very difficult. Since majority logic

Table 7-3. Expected NAR (AND) for two sensors subject to uncorrelated nuisance alarms

NAR_1 (alarms/hr)	NAR_2 (alarms/hr)	T (minutes)	NAR (AND) (alarms/hr)	NAR (AND) (days/alarm)
1	1	0.25	0.004	10
		1	0.02	2
		2	0.03	1
1	0.1	0.25	0.0004	100
		1	0.002	25
		2	0.003	12
1	0.01	0.25	0.00004	1000
		1	0.0002	250
		2	0.0003	125
0.1	0.1	0.25	0.00004	1000
		1	0.0002	250
		2	0.0003	125

Key:
NAR_1 - Nuisance alarm rate of first sensor

NAR_2 - Nuisance alarm rate of second sensor

T - Preselected time window for occurrence of an alarm on both sensors

NAR(AND) - Nuisance alarm rate of the AND combination of first and second sensors

increases the probability of detecting an intruder who is attempting to defeat the sensors, the additional complexity of a three-sensor system may be warranted if the system threat includes the insider who has intimate knowledge of the sensor system and its characteristics.

7.5 AND-OR Combination

A combination of sensor systems for which the detection regions do not overlap is vulnerable to defeat when two sensors are combined in an AND configuration or when more than two sensors are arranged in a majority logic system. An intrusion may begin in a sector covered by one such system and proceed to an adjacent sector, thus defeating the AND combination. If an intruder defeats one of the two inner sensors of a three-sensor system after crossing from an adjacent sector, the majority-logic system is defeated as well.

AND-OR sensor logic is applied to AND-combination sensor systems in adjacent sectors to prevent the adjacent-sector defeat method. The output indications for the second sensors of adjacent sectors should be ORed; and, for a three-sensor configuration, the output indications for the third sensors should also be ORed. This type of interconnection pattern results in a pyramidal detection region for each sector.

With the OR combination for adjacent sectors, the NAR might be expected to follow the NAR(OR) relation described above. However, the same environmental conditions would be present for the same generic type of sensor in adjacent sectors, so the nuisance alarms would be very highly correlated. As a result, the NAR of the OR combination of three adjacent sectors would not increase by a factor of three as is indicated by the NAR(OR) relation given above, because the three systems would alarm simultaneously, giving only one OR output.

Another useful AND-OR combination results when an AND combination of sensors to detect wall intrusions is ORed with sensors to detect overhead intrusions.

8 DESIGN

Although intrusion detection is an important element of a PPS (physical protection system), equally important are assessment, communications, delay, and response. Similarly, although interior intrusion detection is an important element of an IDS (intrusion detection system), equally important are barriers, entry controls, and perimeter intrusion detection. Further, system design is an important element of an IIDS (interior intrusion detection system), but equally important are procurement, installation, and maintenance. The very best design is worthless if hardware quality is disregarded during procurement, if installation is haphazard and incomplete, or if maintenance is ignored. All these elements should be considered for continued effective operation of an IIDS.

8.1 IIDS Design Principles

The integration of individual sensors into an IIDS should consider the skill level of the expected intruder, the design goals, the effects of environmental conditions, and the interaction of the IIDS with a balanced and integrated PPS. The system designer should have a thorough knowledge of the performance characteristics and other features of interior sensors in order to design an effective IIDS. The basic components of an IIDS may include line supervision, annunciators, and power supplies in addition to the sensors. The final design of such a system incorporates protection in depth, provides timely detection to allow for adequate response, and includes tamper protection and self-test capability.

The success of interior intrusion detection depends on how well the system has been designed as a system. The objective is to provide repeated opportunities to detect an intrusion as an adversary enters the building and moves through the interior to the target. Installing sensors that use different technologies at the boundary of a building, in the interior space, and at the target, provides three layers of protection. Technologies may also be mixed within each layer for redundant protection. This concept of protection in depth is very effective.

Boundary-penetration sensors should detect someone penetrating the enclosure or shell either through existing openings like doors, windows, and ventilation ducts or by destroying walls, ceilings, and floors. Building construction may provide some delay during entry; and, since early detection gives more time for the response team to arrive, detection should occur during rather than after entry.

The second opportunity for detection is afforded by volumetric sensors designed to detect an intruder moving through the interior space toward a target. The interior space usually affords little delay except for the time it takes to move from the boundary to the target.

Finally, point sensors should be placed on or around the anticipated target. Some delay may be gained if the protected object is inside a safe or a vault.

Although all sensors are vulnerable to defeat, sensors with different technologies have different weaknesses. A successful intrusion is much more difficult with the establishment of protection in depth because the adversary should be familiar with all the technologies used in order to avoid detection during the mission. Without protection in depth, a single sensor failure may eliminate any chance for detection, whereas a system with layers offers backup protection.

A subtractive approach to sensor selection sets no predetermined limits on the selection of sensors: All sensors are considered viable candidates until they are eliminated by the constraints imposed by a particular facility. These constraints are determined from information about the building, its contents, its interior environment, operations, and the expected threat. Potential nuisance alarm stimuli should be included in the data. Every facility is different, and so no two system designs are the same.

8.2 Facility Characterization

Selection of interior intrusion sensors depends on the physical and environmental characteristics of each specific facility. Each site's physical and environmental characteristics affect the NAR and the

applicability of specific sensors. Therefore, in addition to having a broad knowledge of interior sensors, the IIDS designer should gather a great deal of information about the area or the building to be protected. The designer should know the definition of the expected threat and the level of protection required. An on-site inspection may be necessary to obtain details of the building construction and its contents, the environmental conditions, and the operational characteristics of a facility. Finally, consideration should be given to the interaction among buildings, equipment, the environment, operations, and potential intruders.

The following activities have been identified to help characterize the protected facility in order to be able to define an appropriate IIDS.

A. Threat Definition
Describe the following characteristics expected to be associated with the threat to the protected facility:
1. The expected threat to the facility: theft of nuclear material, theft of information
2. The expected adversary: insider, outsider, or outsider in collusion with insider; covert or overt
3. Expected adversary capabilities in a situation other than an all-out attack: number of persons, type of weapons, and kind of equipment
4. The adversary's motivation: ideological, economic, personal
5. The adversary's level of dedication: a desire to harass or a willingness to risk death
6. The adversary's purpose: theft of SNM, monetary gain, disruption of operations, destruction of information, publicity

B. Facility Description
Ascertain the following parameters associated with the protected facility:
1. Briefly describe the volume to be protected: a vault may be described as stand-alone or underground; as a fuel storage repository, a shop, or a laboratory; or as part of a larger facility or building
2. Ascertain the approximate dimensions of the volume: length, width, and height
3. Describe the shape of the volume: regular, such as a cube; irregular; has many corners or alcoves
4. Is the volume an isolated entity, or is it associated with other parts of the facility?
5. Does the volume have exterior walls exposed to the environment?
6. Does the volume contain interior walls or partitions exposed to other parts of the volume or exposed to parts of a larger structure containing the volume?
7. Are ceilings exposed to the environment through a roof, or are they contained within a larger structure?
8. Describe the type of floor: concrete, wood, dirt
9. If the protected volume is only part of a building, describe activities conducted elsewhere in the building
10. Describe activities conducted immediately outside any interior walls containing the protected volume
11. Describe activities conducted immediately outside any exterior walls containing the volume
12. Is the protected volume part of a building in which vibrations are produced by sources such as heavy equipment, a machine shop, HVAC equipment on a roof?
13. Describe the construction of the walls, floor, and ceiling containing the protected volume:
    a. Construction material
    b. Thickness
    c. Penetrable openings, such as doors, windows, and skylights
    d. Insulation
14. Describe unusual features of the volume: a tunnel under the floor, a roof hatch, an overhead crane, a tower, a labyrinth, a dropped ceiling, a raised floor, a pit, a water reservoir, radiation
15. Describe all contents of the protected volume other than the structural features described above:
    a. Include movable ancillary items, such as forklifts and roll-around carts
    b. Do the contents of the protected volume change frequently?

C. Environment

Describe the environmental features of the protected volume:

1. The environment surrounding the protected volume: railroads; airports; highways; manufacturing plants; bodies of water; sources of strong electromagnetic fields, such as radio and television stations
2. Weather conditions at various times of the year
3. The environment within the protected volume:
   a. HVAC components: ducts, grills, vents, fans, sources
   b. The lighting system: fluorescent, incandescent, natural
   c. Power: frequency and voltage
   d. Pipes, conduits, hanging fixtures, and similar items
   e. Direction doors open: inward or outward
   f. The presence of computers or peripherals within the volume
   g. Exposed flat metal surfaces
   h. Locations on the walls, floor, and ceiling from which the protected contents cannot be seen

D. Operations

Describe the operations associated with the protected volume:

1. Frequency of occurrence of access to the contents: daily, weekly, etc.
2. Extent of facility occupation: eight hours per day, five days per week, weekly, monthly
3. Manner in which the protected volume is secured when unoccupied
4. Manner in which access to the protected volume is controlled

E. Security System

Describe the features of the desired security system:

1. Type of system: perimeter, volume, specific object
2. Type of alarm reporting: all alarms; some alarms always and other alarms sometimes; silent alarm or local annunciation
3. Time of alarm reporting: immediate; stored in computer file for occasional access
4. Alarm response: alarm-initiated response; security force response within 5 minutes; no response
5. Events and activities to be detected
6. Events and activities to be rejected by the alarm system
7. Restrictions on the types or models of sensors which may be used
8. Desired completion date

8.3 IIDS Design Definition

The IIDS should be defined through a series of engineering drawings. When the general protection requirements have been identified, knowledgeable design groups determine what detection and assessment hardware is necessary to fulfill the requirements. The hardware design groups produce information drawings that can be used by an architectural engineering (AE) firm in the preparation of complete IIDS drawings. The drawings produced may also be complete engineering drawings requiring very little modification to become final installation drawings.

The assignment of the installation definition responsibilities and administrative controls provides the project management group with an effective way to manage the creation of the drawing package. Each design group provides project management with information for projecting costs and schedules. Periodic drawing reviews provide feedback to eliminate bottlenecks and schedule delays. Figure 8-1 illustrates an IIDS design and implementation flow chart.

The following outline describes recommendations which should be considered in the design of an IIDS.

A. Promote the attitude among personnel and management that a security system is an asset, not a liability

B. Sensor Selection
   1. Require vendors to demonstrate or provide independent verification of their claims
   2. Consider sensor installation requirements during the selection process; the IIDS installer may be inexperienced
   3. Select more than one sensor or sensor type

C. Sensor Placement
   1. Place sensors before the delay mechanism in an intruder's path
   2. Place each sensor in another sensor's detection envelope to provide complete coverage
   3. Detection is unreliable outside a sensor's predicted detection range
   4. Keep the sensor's detection envelope clear of clutter
   5. Place sensors on stable mountings
   6. Motion sensors
      a. Do not use motion sensors in an area which has moving things other than people, such as small animals, fans, or fluttering curtains
      b. Do not include weak partitions or lightly constructed walls which may move or cause slight air currents in a motion sensor's detection envelope
      c. Do not install motion sensors next to or above openings such as doorways or windows

D. Consider environmental influences which may affect sensor performance
   1. Power line transients can cause nuisance alarms
   2. Radio-frequency sources, such as portable radio transmitters
   3. Outside sources such as trains, power lines, and weather phenomena

E. Wiring
   1. Install wiring in conduit so it is not exposed to tampering
   2. For wires in conduit, include as spares 50 percent more than the essential number

F. Tamper protection
   1. Equip junction boxes with tamper switches
   2. Do not place tamper switches in series with alarm outputs

G. Provide line supervision
   1. Line supervision circuits should be active even when the system is in the access mode
   2. Do not employ a carrier system on a power line which passes through a transformer

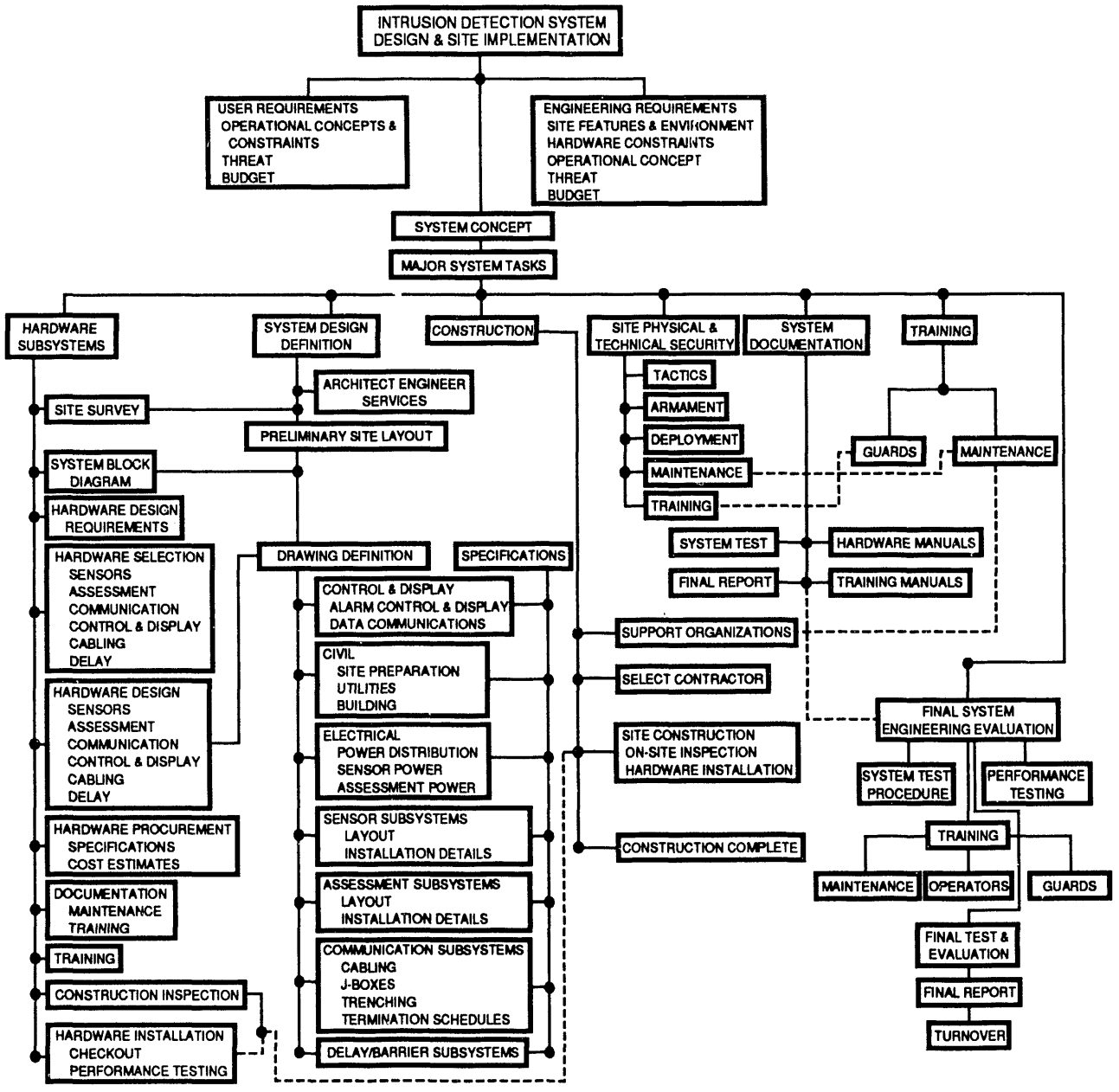


Figure 8-1. Intrusion detection system design and site implementation

9 PROCUREMENT GUIDELINES

Some of the requirements to be considered when procuring an interior intrusion detection system (IIDS) are discussed in this section. The performance characteristics addressed are those which affect the reliability and security of the detector as well as those characteristics which affect its false alarm susceptibility. No present IIDS meets all of the requirements presented in these guidelines; consequently, procurement should be based on systems which come closest to satisfying the customer's requirements listed while demonstrating compatibility for integration with future generation systems.

9.1 Sensor Selection

Sensor selection requires identification of the equipment and installation methods which best meet the objectives of the desired IIDS. Table 9-1 summarizes the typical classifications of the interior sensors which have been discussed in this report. Selection of a specific sensor depends upon the level of protection required, the physical surroundings, and the environmental conditions which exist within the volume to be protected. Two important aspects of the physical surroundings which affect sensor performance are the building or room construction and the various equipment and objects which occupy the area to be monitored, both of which are discussed in Section 3.3. Environmental conditions which can affect IIDS sensors include electromagnetic energy, nuclear radiation, acoustic energy, thermal changes, optical phenomena, seismic phenomena, and meteorological phenomena as discussed in Section 3.4.

Consideration should be given to the interaction among equipment, environment, and potential intruders. Correct sensor choice requires that the nuisance alarm stimuli to which a sensor is susceptible be known. The major characteristics of several types of IIDS sensors suitable for fixed-site applications are shown in Table 9-2. The environment associated with interior areas is normally controlled and is, therefore, predictable and measurable. Consequently, it is possible to identify appropriate sensors which will perform acceptably in the environment in question.

9.1.1 Environmental and Operational Requirements

The ability to withstand the following environmental extremes is a characteristic to be considered in the selection of IIDS sensors. Specifications are noted for both operating and nonoperating modes:

Nonoperating	
Temperature	-25 to 66 °C (-13 to 151 °F)
Humidity	100% RH
Shock	Bench handling
Operating	
Temperature	-18 to 50 °C (0 to 122 °F)
Humidity	85% RH (approximate), 0 to 10 °C (32 to 50 °F)
	100% RH, 11 to 50 °C (51 to 122 °F)
Vibration	0.1 g, 5 to 200 Hz

9.1.2 Material Requirements

Ideally, the materials and components of the sensor conform to the requirements of Underwriters Laboratories Standard UL-639, Sections 5 through 18. To the extent practical, all electronic parts should be solid-state and should meet MIL SPEC standards. It may be desirable to specify devices which are radiation hardened in order to minimize the effects of radiation on the system's performance.

Table 9-1. Typical classifications of interior sensors

	Sensor	Passive or Active	Covert or Visible
Boundary-penetration	Glass-Break	A	V
	Continuity	P	C
	Infrasonic	P	V
	Light-Beam	A	V
	Magnetic Switch: BMS	A	V
	Magnetic Switch: Simple	A	V
	Mechanical Switches	P	V
	Passive Sonic	P	V
	Passive Ultrasonic	P	V
	Seismic	P	V
	Vibration	P	V
Volumetric	Active Sonic	A	V
	Light-Level	P	V
	Microwave	A	V
	PIR	P	V
	Ultrasonic	A	V
	VMD	P	C
Point	Capacitance Proximity	A	V
	Pressure Switch	P	C
	Strain	P	V

Key: P - Passive
A - Active
V- Visible
C -Covert

Table 9-2. Characteristics of interior sensors suitable for fixed-site applications

Application	Sensor	Detection					Conditions Causing Unreliable Detection	Typical Defeat Methods	Major Causes of Nuisance Alarms										
		Portal Opening	Breaking Through Wall/Floor/Ceiling	Radial Motion	Transverse Motion	Touching Object			Air Humidity/Temp Wind Velocity	Localized Heating (Sunlight)	Movement >0.025m/s	Movement from Outside (Vibration)	Fluorescent Lights	Loose-fitting Doors	Mount Vibration	Ambient Acoustic Noise (Thunder)	Animals	RFI Radio Transmitter
Boundary-penetration	Glass-Break	✓					vibrations		X						X			
	Continuity		✓					bypass										
	Infrasonic	✓	✓						X					X				
	Light-Beam	✓			✓			bridge									X	
	Magnetic Switch: BMS	✓					improper setup/ adjustment	bypass						X	X			
	Magnetic Switch: Simple	✓												X				
	Mechanical Switches	✓												X				
	Passive Sonic		✓	✓	✓				X			X			X	X	X	
	Passive Ultrasonic			✓	✓				X			X			X	X	X	
	Seismic		✓					slow attacks				X			X			
	Vibration		✓						X			X			X			
Volumetric	Active Sonic	✓		✓	✓		slow-moving intruder		X		X				X	X	X	
	Light-Level	✓	✓										X			X		
	Microwave	✓		✓			small radial motion				X	X	X		X	X	X	X
	PIR				✓		unstable thermal temp.	target temp		X					X	X	X	X
	Ultrasonic	✓		✓			small radial motion		X		X				X	X	X	X
	VMD	✓		✓	✓		low contrast, speed			X					X		X	
Point	Capacitance Proximity					✓	gross changes in relative humidity, temperature or pressure	disable electronics	X								X	X
	Pressure Switch					✓											X	X
	Strain					✓									X		X	X

9.1.3 Power Requirements

The system requires primary power of 115±10 VAC and 6±5 Hz and an emergency battery source for use when the primary power fails. The emergency battery, when fully charged, should be capable of maintaining full operation of the system for 24 hours at 0 °C (32 °F). Switchover to battery power should be instantaneous and automatic upon failure of the primary power source in order not to cause an alarm. An indicator for system primary power failure is essential.

Nicad batteries should be constant-current charged and never fully discharged. All other batteries should be arranged so that they are fully charged at all times when primary power is available. Chargers should have sufficient capacity to recharge the batteries from a fully discharged state to more than 90 percent of capacity in 12 hours.

9.1.4 Probability of Detection

The volume in which a single detector unit provides reliable detection is called the protected volume. Within the protected volume the P_d of the system should be 0.95 at a 95 percent confidence level when the system is tested according to the following section on acceptance testing. Unit-to-unit or system-to-system variability should be considered in verifying the P_d.

9.1.5 Self Test

A system with self-test capability responds with a self-test status indication when interrogated by a command initiated at the control unit or from a remote site. The self test should be designed to determine the operational status of the entire system. A true end-to-end self test is not presently available for most sensors.

9.1.6 Line Supervision

The system circuits between the detector and the control unit should be supervised to provide security against tampering or any covert action. Between control boxes and central receiving facilities the best supervisory system is digital signals over the circuit lines with interrogation and reply schemes. The signal technique used for the interrogation should be different from that used for the reply.

9.1.7 Tamper Protection

Controls and switches which are not used in the normal daily operation of the IIDS and which affect its sensitivity should be mounted inside tamper-protected enclosures. All enclosures and accessible critical components and terminals can be protected against tampering by being equipped with tamper switches. Internal wiring should be such that tamper switches are not bypassed, even when the system is in the access mode. Tamper switches should not cause the device to signal an alarm until the cover or cover screw has moved 6.0 mm (0.24 in). However, an alarm should occur before the cover or cover screw has moved a sufficient distance to permit direct line of sight to electrical circuits or adjustment controls.

9.1.8 Operational Reliability

The intrusion detection system should have a mean time to (first) failure (MTTF) of 8500 hours (1 year).

9.1.9 Maintainability

It is wise to design the intrusion detection system to have a mean time to repair (MTTR) of 30 minutes or less, with 90 percent of all failures requiring no more than 1 hour to repair. Maintenance is defined as troubleshooting and isolation of failures due to defective detectors, control units, and power supplies and the repair or replacement of the defective parts.

9.1.10 Detector Sensitivity Control

Selected detector units should have an adjustable sensitivity (range) control located in the detector enclosure.

9.1.11 Detector Sensitivity Variation

Once the detector sensitivity has been set, the detection envelope should not vary more than ±10 percent under the operational environments specified. An alarm should be given when the sensitivity exceeds those limits.

9.1.12 Secure/Access Modes

Detector units should be chosen which can be placed in the secure (detector active) or access (detector ignored) mode of operation by remote command. When in the access mode, the tamper capability should not be bypassed. It is essential to provide the capability of monitoring and controlling the status of each detector at a remote location.

9.1.13 Alarm Indicator

Incorporating into each detector unit an audible or visible alarm indicator which can be recognized from 10 m (35 ft) facilitates walk testing of the unit. The indicator should be capable of being activated or deactivated.

9.1.14 Nuisance Alarm Rejection

The detector selected should be designed to minimize nuisance alarms. Undesired alarms should not occur more than once per sensor zone per day of operation.

9.1.15 Detector Identification

A unique two-digit digital code should identify each detector either when it is in the alarm state or when it is interrogated for self test.

9.1.16 Mounting Options

Detector units should be mountable on a wall or the ceiling with minimum change in the unit's enclosure and mounting hardware. The detector units need to be adjustable with a positive locking feature.

9.1.17 System Outputs

The following list outlines the essential output features for an IIDS:

- detector identification - a two-digit code
- detector state - secure, alarm, access modes
- tamper alarm - unique two-digit code
- self-test status - for control unit as well as detector heads
- primary power status

9.2 Acceptance Testing

Acceptance testing is normally completed at the manufacturer's plant, but it could be performed at the buyer's plant instead or at both locations.

9.2.1 Protected Volume

The protected volume is defined as the volume in which a single detector unit provides reliable detection. This volume should be ±10 percent of the specified coverage over the temperature and humidity ranges specified in the Environmental and Operational Requirements outlined in Section 9.1.

9.2.2 Test Target

Utilize a test target which has been designed to closely resemble a human being. The target cross-sectional area should be the minimum cross-sectional area presented by a human 1.5 m (5 ft) in height and 0.2 m (0.66 ft) wide. The target is clothed with typical material, such as cotton, wool, or polyester fabrics. The detector unit should detect the target before the target can move approximately 1.5 m (5 ft) by any means at velocities varying from 12 to 500 cm/s (5 to 200 in/s).

9.2.3 Test Facility

It is desirable to install the test system in a test facility large enough to accommodate the maximum detection envelope. The facility should be free of spurious stimuli which may cause nuisance alarms in the system being tested. Divide the floor of the test facility into a grid of walk-test lines which will be used to determine the configuration of the detection envelope. A minimum spacing of 1.5 m (5 ft) between grid lines is suggested.

9.2.4 Test Procedures

Perform the following tests on every product being considered for incorporation in an IIDS system:

9.2.4.1 Walk Tests

Perform walk tests to ascertain the detection envelope. If the test target described in Section 9.2.2 is not available (or practical for an operational system performance test), a human test target can conduct these tests. The target person performing the walk tests should have a height of 1.5 ± 0.3 m (5 ± 1 ft) and a weight of 59 ± 5 kg (130 ± 10 lb) and should walk with arms folded over his chest at a rate of approximately 12 cm/s (5 in/s). The walk tests should be along the grid lines established in the preceding paragraph describing the test facility. There should be a minimum of three walks per grid line. A simple metronome, available at most music stores, is an invaluable aid in maintaining a consistent velocity.

9.2.4.2 System Sensitivity Reference

With the aid of the walk test, the detector can be adjusted for maximum sensitivity at ambient room conditions. All test sensitivity measurements should be referenced to this sensitivity setting.

9.2.4.3 Voltage Variation Test

In order to ascertain how the sensor will perform under power-line voltage variations, a variable power supply should be used. Without changing the sensitivity, the walk test should be performed at least three times per grid line with the input voltage at 110 percent and then at 85 percent of normal operating voltage. The detection envelope as determined above, will not vary more than 10 percent in an acceptable test.

9.2.4.4 Temperature and Humidity Test

This test determines the variation in a sensor's performance at various temperature extremes. Desirable testing parameters are

1. -18±2 °C (0±4 °F) and 85% RH (approximate)
2. 0±2 °C (32±4 °F) and 85% RH (approximate)

3. 50±2 °C (122±4 °F) and 100% RH (approximate)

The sensitivity of the system is not changed from that used to determine the detection zone. The system should be stabilized at each condition for 4 hours. If possible, tests are conducted while the system is located within the temperature chamber. If this is not possible, the walk test should be completed within 15 minutes after the system is removed from the temperature chamber. The test is satisfactory if the detection envelope does not vary by more than 10 percent from the envelope originally determined.

9.2.4.5 Electromagnetic Susceptibility Tests

The parameters for a radiation susceptibility test of 1 V/m from 10 kHz to 1.9 MHz and 3 V/m from 2.0 MHz to 12 GHz are found in MIL-STD-462, Notice 3, Requirements RS03 and RS03.1. The system will not enter the alarm state in a satisfactory test. Alarms occurring within the frequency band allowed for the microwave sensor by the Federal Communication Commission are not considered failures. In addition, the system should be subjected to conducted interference in accordance with MIL-STD-462, Notice 3; MIL-STD-461A, Requirement CS02; and MIL-STD-461A, Notice 4, Requirement CS06. The system is satisfactory if it does not enter the alarm state during any of these tests.

9.2.4.6 Vibration Tests

With the system functioning at the same sensitivity settings used in previous tests, it is vibrated with simple harmonic motion at frequencies from 5 to 200 Hz at a sweep rate of 1.0 Hz/s. An acceleration level of 0.1 g rms is maintained for three complete sweeps. The system should not enter the alarm state during this test.

9.2.4.7 Standby Power Tests

Turn on the system and allow it to stabilize. An alarm should not occur when the line voltage is interrupted or when it is restored. In a satisfactory system, the detection envelope will not be degraded by more than 10 percent from the average normal detection range after 24 hours of continuous operation on standby power.

9.2.4.8 Handling Shock Test

This test determines the ability of the equipment to withstand shocks encountered during servicing. The units are prepared as if for servicing in the field by removing the chassis from the enclosure and placing it in a suitable position on a horizontal, solid wooden bench top at least four centimeters thick. Perform the test as follows to simulate shocks liable to occur during servicing. No power is applied during the test. Using one edge as a pivot, lift the opposite edge of the chassis until one of the following conditions exists.

1. The chassis forms an angle of 45 degrees with the bench top.
2. The lifted edge of the chassis has been raised 4 inches above the horizontal bench top.
3. The lifted edge of the chassis is just below the point of perfect balance.

Let the chassis drop back freely to the horizontal bench top. Repeat, using other practical edges of the same horizontal face as a pivot point, for a total of four drops per pivot point. At the conclusion of the test, the test item is walk tested. The sensitivity of the system should not have changed + 10 percent following the test.

9.2.4.9 Burn-In Period

In addition to the above tests, subject each system to a 7-day burn-in time. Test each system at the conclusion of the burn-in period: The sensitivity of the system should not have changed + 10 percent.

9.3 Application and Installation Manuals

Obtain a comprehensive set of manuals. The manuals should include complete circuit schematics, parts lists, application and installation guidelines, operational theory, maintenance procedures, and trouble-shooting guidelines. Enough detail should be included to allow an electronic technician to install, maintain, and troubleshoot the system.

10 INSTALLATION

10.1 Site Preparation

In order to minimize the NAR (nuisance alarm rate), the volume to be protected should be modified to control thermal, acoustic, and mechanical energy; to control all rubbish or loose paper which might be blown around the volume; and to secure items, such as banners, signs, curtains, and window blinds, to prevent swinging or fluttering.

10.2 Installation Guidelines

In addition to the manufacturer's recommendations, use of the following guidelines may be helpful in installing line-of-sight sensors:

1. Detection of moving objects or people outside the room or building in which the sensors are installed can cause alarms. Using the protection coverage pattern best suited for the sensor, adjust the range control or sensitivity setting to protect the key area only.

2. Direct line of sight affords optimum protection. Avoid obstructions, such as columns, beams, bins, racks, and desks. In extremely cluttered areas with high ceilings, line-of-sight transceivers may be mounted on the ceiling, beaming directly down to employ the full coverage pattern.

3. Locate the transceiver in an area which offers protection from physical damage and tampering.

4. Avoid positioning transmitters, receivers, or control units within 20 meters of a radio transmitter.

5. Place all wiring in conduit, with a section of flexible conduit at the detector to permit detector-location adjustment for optimum performance.

6. Avoid installing transmitter/receiver wiring near AC power lines, telephone lines, or other sources of EMI.

7. Install shielding to eliminate unwanted cross talk between the signal wires.

8. Use only shielded wire for transmitter and receiver wiring if the manufacturer does not specify the wire to be used.

9. Securely mount the detector head on a rigid surface only. Nuisance alarms can be created by vibration or motion of a sensor mounted on an insufficiently sturdy foundation.

10. Ensure that all shielding is properly grounded to a good earth ground unless specified differently by the manufacturer.

11. Movement of objects, such as those in storage areas, could possibly alter the protected volume. Designate an area for storage of each protected item in order to prevent compromising of the detection pattern in the secured area.

12. Avoid placing sensors in areas containing strong emitters of electric fields, e.g., radio transmitters, or magnetic fields, e.g., large electric motors or generators.

Every sensor installation should include rigid mounting, supervised wiring run in conduit, fail-safe operation, standby power in the event of main power failure, and tamper protection of the sensor. Enclosing the sensor in a tamper-protected box prevents access to the wiring terminals. End-to-end self test is desirable as is a final test to verify that normal activities in the area under protection are not sources of nuisance alarms and to verify the detection zone.

10.3 Adjustment and Alignment

Adjust the detector range for the sensitivity which will provide adequate coverage of the area. After installation is complete, turn on all possible nuisance alarm stimuli, such as heaters, fans, bells, and machinery, and allow no human movement. The unit is functioning properly if no nuisance alarms occur.

10.4 Performance Testing

All sensors should meet applicable FCC, National Electrical Code (NEC), and OSHA requirements. Since the performance of an installed sensor depends on the method of installation and the operating environment, the sensor supplier should supply the appropriate information to ensure that a properly installed sensor will meet those requirements. Installation, operational, and corrective and preventive maintenance information provided by the supplier, which may include drawings and photographs, should be followed for the sensor to perform as certified by the supplier. The supplier's certification provides information about environments to be avoided and other necessary precautions required for effective sensor performance. The supplier's performance-level certification is determined for all performance requirements in a single installation configuration, including sensor orientation and the direction the sensor is aimed, range adjustment, and mounting site, e.g., wall or ceiling.

A general equipment evaluation is performed to determine the life of a sensor's standby battery, the vulnerability of the sensor to radiated and conducted electrical interference, its ability to withstand shocks during servicing, its nuisance alarm rate (NAR), and its resistance to defeat. The sensor's resistance to defeat is dependent upon its capability for self-test, for signal-line supervision, and for alarming when an electronic component fails. However, total system self-test modes are not currently available on most sensors. In addition, the supplier defines the sensor's minimum operational life, mean time to failure (MTTF), mean time between failures (MTBF), and mean time to repair (MTTR), subject to the review and approval of the user.

Ideally, all tests should be conducted with the aid of a specialist in intrusion alarm tampering and antidetection techniques. The specialist is given access to the protected facility to review the protection system, thus simulating an intruder with full access to building and alarm information. Any flaw in the original alarm system installation design or in subsequent modification to the building or alarm system will be revealed by the test.

Standard walk tests, as described in Section 9.2, are performed to ascertain and verify alarm sensitivities. During a walk test, the threshold and the output from the sensing element should be monitored and adjusted if necessary.

10.4.1 Motion Sensor Evaluation

In addition to a general equipment evaluation, detection capability, covert action rejection, and nuisance alarm rejection are determined using standard motion sensor evaluation techniques.

The detection capability of a specific sensor is evaluated by establishing a velocity factor curve (Figure 10-1), a range factor curve (Figure 10-2), a detection pattern, and sensitivity (Figure 10-3), defined as integration time to alarm. The velocity factor estimates the sensor's changes in performance resulting from various intruder velocities. Variation in the velocity factor curve is also determined as a function of sensor temperature and of sensor input power. The range factor measures the changes in performance resulting from adjustments in the range, or gain. The detection pattern for a specific sensor may be determined electronically (Figure 10-4) or through walk testing. For walk testing, five walk tests (Figure 10-5) should performed twice, each in opposite directions: A) parallel to the direction the sensor is aimed, B) perpendicular to the direction the sensor is aimed, C) angled +45° from the direction the sensor is aimed, D) angled -45° from the direction the sensor is aimed, and E) radial to the sensor. Part F of Figure 10-5 shows the composite detection pattern formed by combining patterns A-E to determine the detection zone within which the sensor is reliable. If sensor sensitivity is adjustable, a walk test determines the effects of varying the sensitivity setting.

Covert action rejection is determined by the ability of the motion sensor to monitor for an object blocking its field of view and by its reliability in signaling tampering. Nuisance alarm rejection is evaluated according to the sensor's background-monitoring output, oscillatory-motion rejection, and susceptibility to fluorescent-light interference.

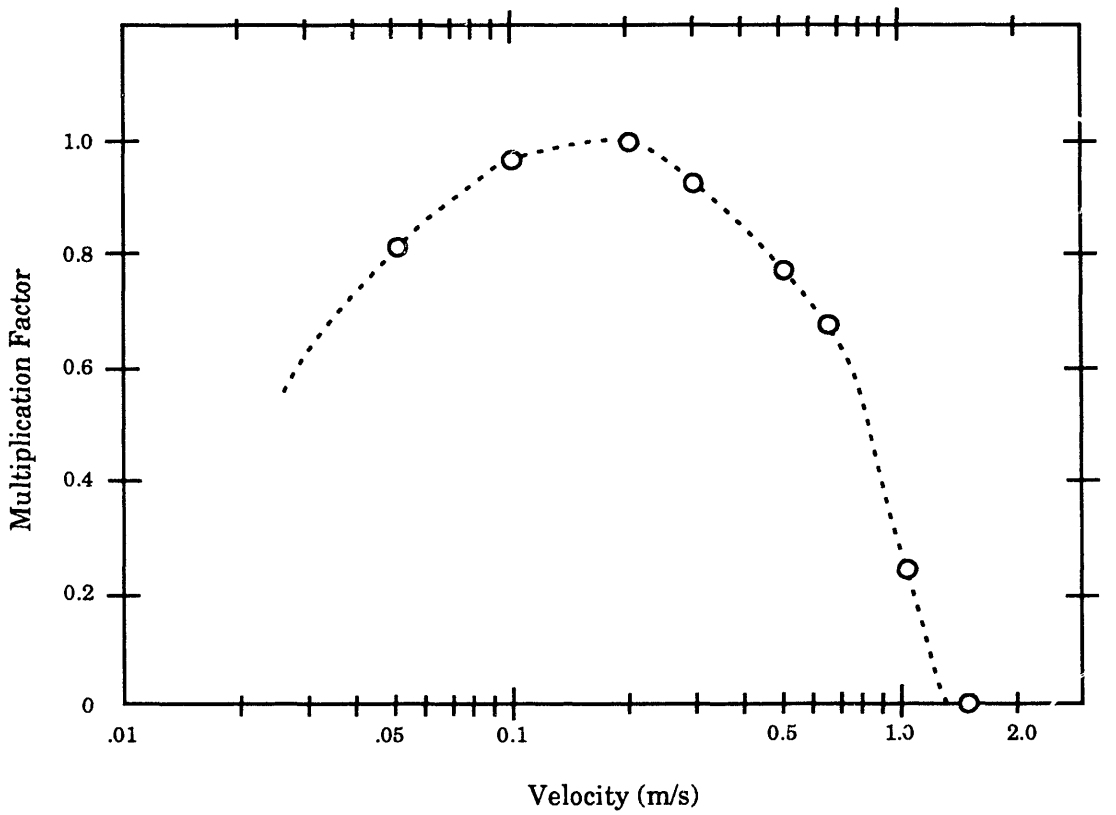


Figure 10-1. Typical velocity factor curve

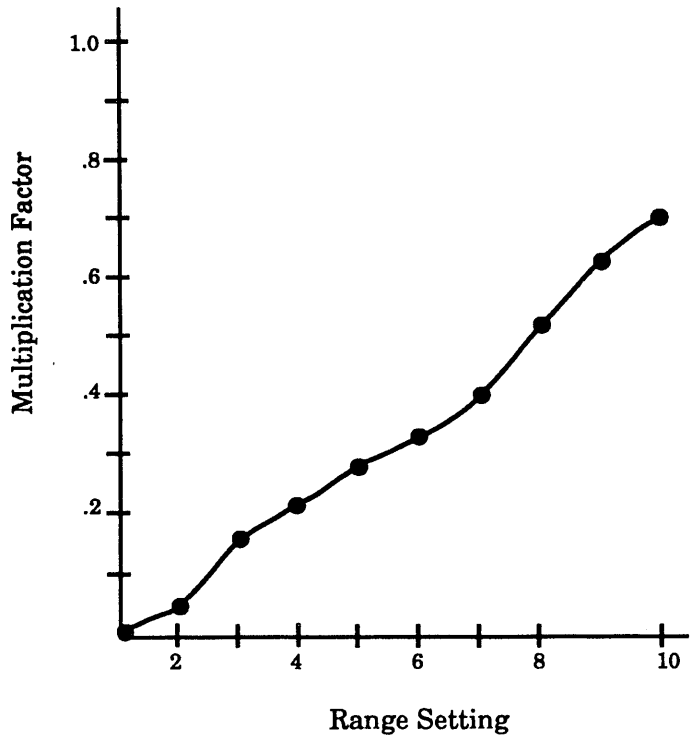


Figure 10-2. Typical range factor curve

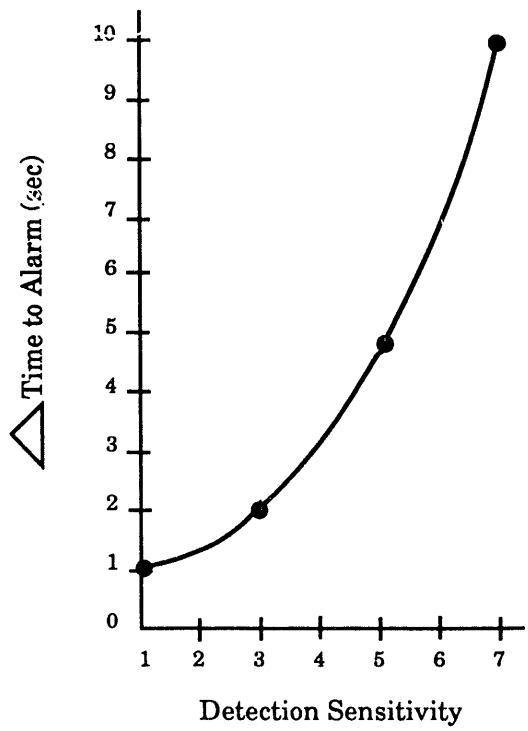


Figure 10-3. Typical sensitivity curve

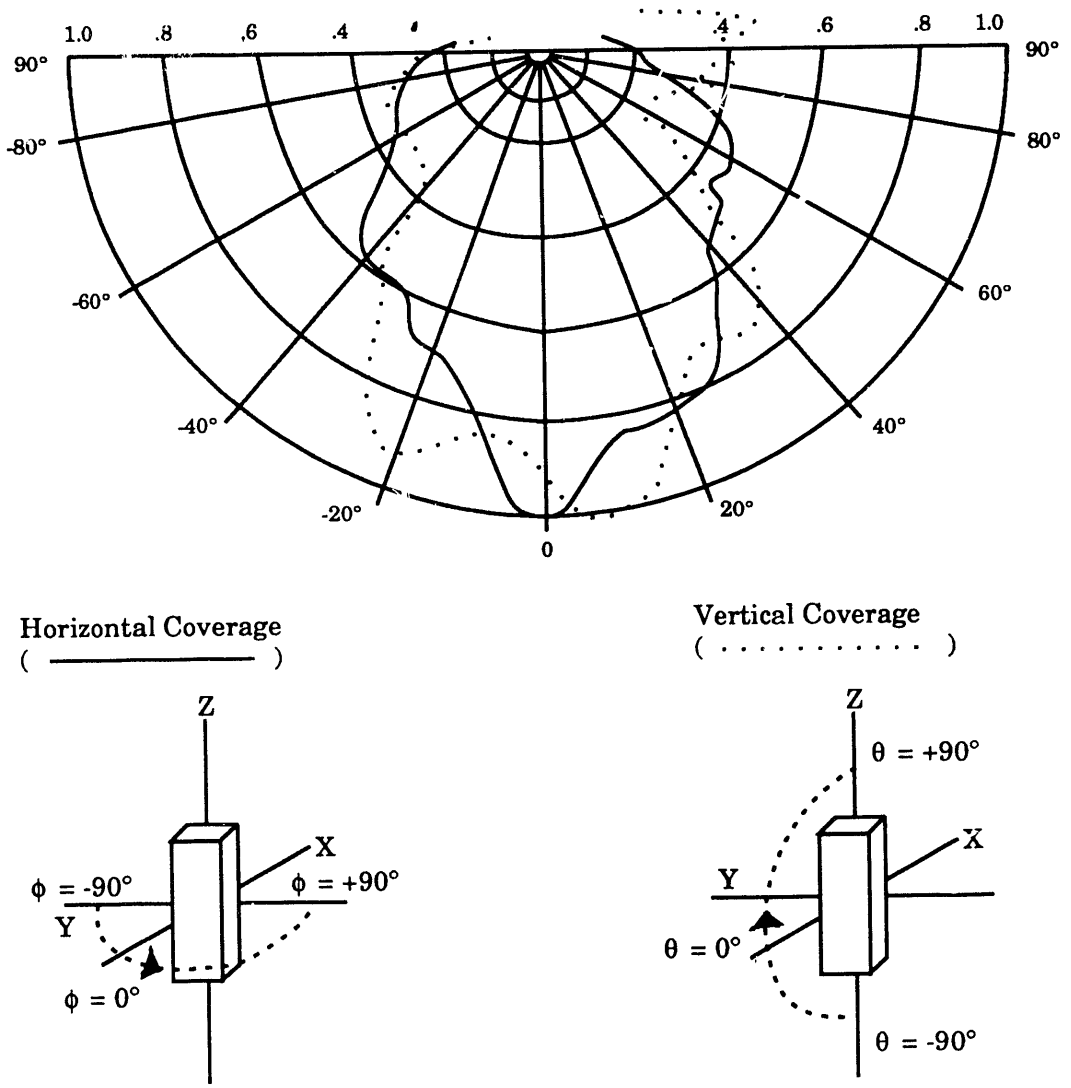
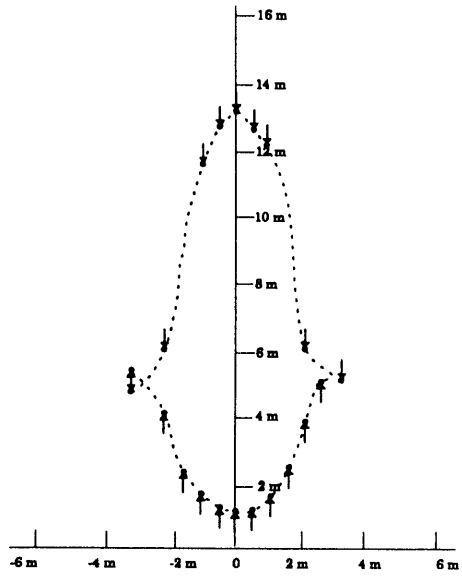
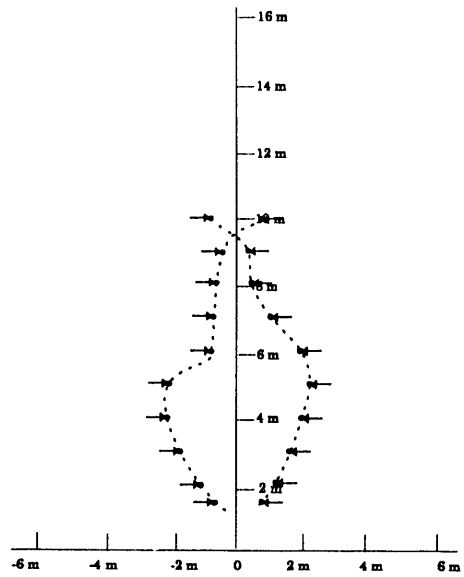


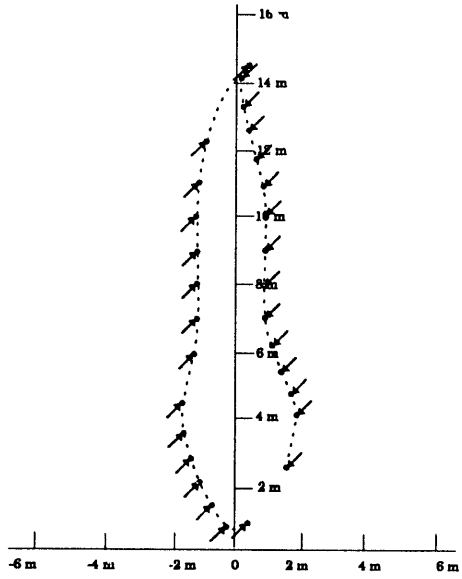
Figure 10-4. Typical electronic detection patterns



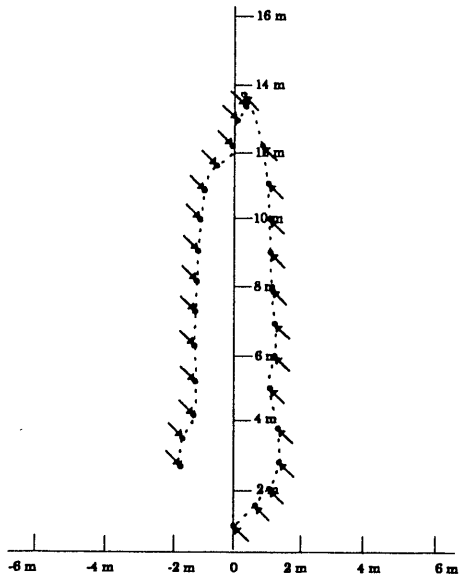
A - Typical Parallel Walk-Test Pattern



B - Typical Perpendicular Walk-Test Pattern



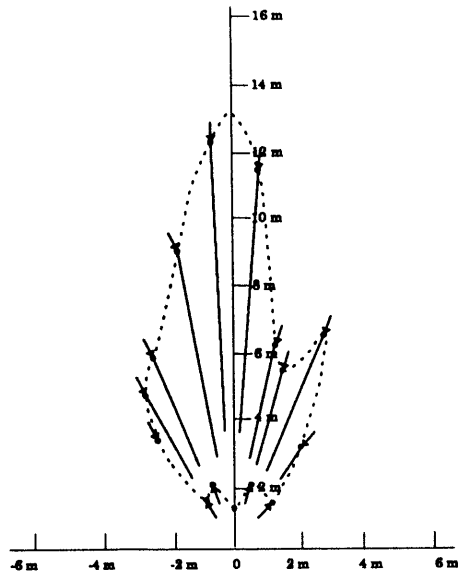
C - Typical +45° Walk-Test Pattern



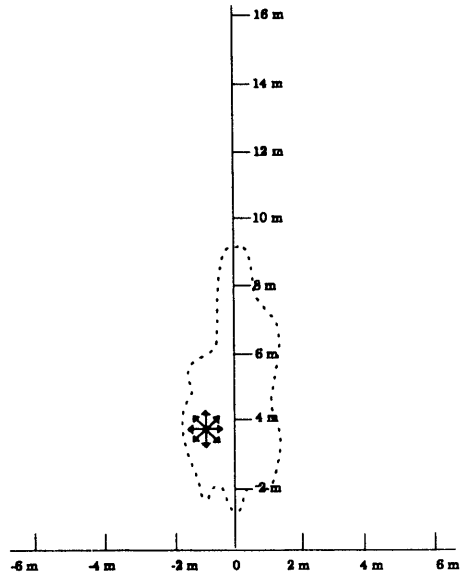
D - Typical -45° Walk-Test Pattern

Note: Arrows indicate walk test direction.

Figure 10-5. Typical motion sensor walk-test patterns



E - Typical Radial Walk-Test Pattern



F - Composite Walk-Test Pattern

11 MAINTENANCE GUIDELINES

Once the IIDS has been installed, it should not be forgotten. Regular maintenance activities will keep the IIDS operating at peak efficiency. The maintenance recommendations delineated in this section are offered in support of and in addition to the maintenance guidelines provided by sensor manufacturers.

Periodic exercise of each sensor, in addition to self tests invoked by the sensor or the system, ensure that the sensor is operating effectively; over time some adjustments may become necessary. A visual inspection of the sensor installation should be undertaken periodically, particularly after any repairs or modifications to the building. An inspection of building repairs or structural additions is necessary to ensure the integrity of the area under protection. Replacing standby batteries on a conservative schedule assures uninterrupted service in the event of power failure. A log of every service call should be maintained, including date, time, corrective action, and an assessment of the cause of the problem.

11.1 System Testing

A self-test feature which provides a true end-to-end system check on command from the monitoring location is desirable but is not presently available for most sensors. A simple walk test should be performed periodically, daily if possible, to verify sensor operation.

NRC licensees should refer to specific NRC regulations for intrusion alarm testing requirements.

11.2 Equipment Repair

IIDS equipment can be maintained through a service contract with the dealer or manufacturer. If a portion of the system fails, the failure should be immediately compensated and repair or replacement initiated. The service contractor should be able to respond within 24 hours with replacement equipment or for on-site repairs. Full surveillance of the protected volume is usually impossible during equipment failures; therefore, the system should be designed so that any one component failure will result in only a small unprotected volume. Critical volumes should have protection redundancy or protection backup incorporated into the installation.

Equipment repair guidelines generally recommend keeping 10 to 20 percent spare parts on hand. This stipulation may be adjusted as maintenance data are accumulated on the failure rate of specific sensors and sensor components. If replacement parts can be obtained quickly from regional distributors, smaller on-site inventories should be available.

11.3 Environmental Modification Guidelines

Changing the locations of detectors or of objects which might be nuisance alarm stimuli should be avoided. Relocating large objects within the area under protection modifies the detection envelope as well as possibly creating a source of nuisance alarms. Requiring approval of plant modification plans by plant security minimizes modifications which would degrade sensor performance.

Readjustment of detector sensitivity may be necessary following remodeling in the area under protection; such readjustments should only be performed by authorized personnel. Reducing a detector's nuisance alarm rate by lowering its sensitivity is not recommended, because lowering sensitivity also reduces system coverage.

Every precaution should be taken to prevent physical or electrical damage to the IIDS. In addition the nuisance alarm rate can be reduced by denying access to the area under protection by maintenance and janitorial personnel when the IIDS is activated.

GLOSSARY

The definitions found in the glossary include technical terms used in the report; words having specialized definitions when applied to interior intrusion detection; and initialisms, acronyms, and abbreviations which appear in the report.

acceptance testing means performing evaluations on newly acquired equipment to determine if it is operating according to specifications.

access mode means the operational state of an intrusion sensor in which only line-tamper alarms are displayed at the operator's console; intrusion alarms are not displayed, thus permitting traffic through the normally alarm-covered area. (See also secure mode.)

active sensor means an intrusion detection sensor which emits a signal from a transmitter and detects changes in or reflections of that signal by means of a receiver. (See also passive sensor.)

active sonic sensor means an active, visible, volumetric intrusion detector which transmits audible sound waves and detects the presence of an intruder within its detection envelope by means of changes in the reflected signal.

adversary means a person performing hostile acts in pursuit of interests antagonistic to those of the facility; an adversary may be an insider or an outsider.

ambient means the characteristics of the environment surrounding the object under consideration, for example, temperature, humidity, and pressure.

AND means a type of gate, in digital systems and other switching circuits, which delivers an output signal only when all the several input signals occur simultaneously or within a designated time window. (See also OR.)

antenna means that part of a transmitting or receiving system which is designed to radiate or to receive electromagnetic waves.

anticapture circuitry means circuitry designed to counter attempts to defeat an active sensor by using a transmitting device to substitute a signal of the correct frequency and energy to maintain a no-alarm signal at the sensor's receiver.

armature means the moving element of an electromechanical relay.

assessment means the determination of the validity and priority of an alarm signal.

background (noise) means an electrical signal inherent to a particular circuit, system, or device and which is present even in the absence of any other signal.

balanced magnetic switch (BMS) means a passive, covert boundary-penetration sensor that initiates an alarm when the balance between its two magnetic fields is disturbed; a balanced magnetic switch is more difficult to defeat than a simple magnetic switch. (See also simple magnetic switch.)

bistatic means an active intrusion detection sensor in which the transmitter and the receiver are located separately.

BMS see balanced magnetic switch.

boundary-penetration sensor means an intrusion sensor designed to detect an intrusion through the boundary of the area under protection.

breakwire sensor means a wire-grid continuity sensor.

bridge means a four-arm balancing circuit, all arms of which are predominantly resistive, used to measure an unknown resistance in terms of a standard resistance.

burn-in means a period of time during which an intrusion detection sensor is allowed to operate in order to stabilize its characteristics and to identify early failures before it is performance tested.

bypass means to defeat an intrusion sensor by avoiding its detection volume. (See also spoof.)

capacitance (capacity) means that property of a system of conductors and dielectrics which permits the storage of electricity when potential differences exist between the conductors; a capacitance value, which is always positive, is expressed as the ratio of a quantity of stored electrical charge to a potential difference (unit: F).

CCTV means closed-circuit television.

circumferential means relating to, placed like, or moving along a circumference, perpendicular to a radius.

collocated means occurring in conjunction; collocated sensors or sensing elements are situated in the same housing or location.

communication means the function of transmitting or interchanging information, including both transmission of alarm signals to a central processing station and transmission of response information to security personnel.

continuity sensor means a passive, covert, boundary-penetration sensor which generates an alarm when its conducting wire or fiber is broken.

covert sensor means an intrusion sensor which is hidden from view. (See also visible sensor.)

cross talk means 1) undesired transfer of signals between systems or between parts of a system. 2) undesired energy appearing in one signal path as a result of coupling from other signal paths; such signal paths may be wires, waveguides, or other localized or constrained transmission systems.

curtain means a boundary-penetration sensor whose sensitive area in space is very narrow in one dimension and much wider in the other two dimensions.

delay means the element of a physical protection system designed to impede adversary penetration into or exit from the area under protection.

detection means the element of a physical protection system designed to discover and to verify that an unauthorized act has occurred or is occurring, including sensing the action, communicating the alarm to a control center, and assessing the alarm: detection does not exist without assessment. (See also assessment.)

detection envelope (detection zone) means the volume of space in which an intrusion sensor will detect an intrusion.

deter means to discourage an adversary from attempting an assault by making a successful assault appear to be very difficult or impossible.

dielectric means a medium which is a nonconductor of electricity, such as glass, wood, plastic, dry air, and pure water, and in which it is possible to maintain an electric field with little or no supply of energy from outside sources.

Doppler effect means the apparent change in the frequency of reflected sound or reflected electromagnetic energy, caused by the motion of the reflecting object.

Doppler frequency shift (f_d) means the magnitude of the change in the observed frequency of a wave in a transmission system, caused by a time rate of change in the effective length of the path of travel between the source and the point of observation (unit: Hz).

dual technology sensor (combination sensor) means a motion detector incorporating a passive sensor technology, such as a passive infrared sensor, with an active sensor technology, such as an ultrasonic or a microwave sensor.

electret microphone means a condenser microphone incorporating an electret, a permanently polarized dielectric layer, between the capacitor electrodes.

EMI means electromagnetic interference.

entry control means the equipment and procedures used to verify access authorization and to detect contraband and nuclear materials; generally considered part of the physical protection function of detection.

f_d see Doppler frequency shift.

fail-safe see redundancy.

fail-soft means the capability of the physical protection system to operate, perhaps in a reduced capacity, during failure of an element of the system.

false alarm means an alarm caused by internal equipment malfunction; since a false alarm has no readily assessable cause, it is actually an unknown alarm.

fiber-optic means the optical technology concerned with the transmission of radiant power through fibers made of transparent materials, such as glass, fused silica, or plastic, by means of internal reflections.

field of view means the area visible through the lens of an optical instrument.

Fresnel lens means a usually square, thin plastic lens consisting of progressively thicker concentric sections, resulting in a large-diameter lens of short focal length.

geophone means an instrument designed to detect vibrations passing through a solid medium, such as rock, soil, or ice.

harden means to enhance a wall, a door, or a container to make it more difficult to penetrate in order to protect against unauthorized access and perhaps to reveal intrusion attempts.

horn means an antenna consisting of a waveguide section in which the cross-sectional area increases toward an open end which is the aperture.

HVAC means heating, ventilating, and air-conditioning equipment.

IDS see intrusion detection system.

IIDS means interior intrusion detection system.

inertia sensor means a passive boundary-penetration sensor which initiates an alarm when it has experienced movement caused by shock or vibration.

infrared (IR) means the region of the electromagnetic spectrum between the long-wavelength extreme of the visible spectrum, about 0.7 μm, and the shortest microwaves, about 1 mm.

infrasonic means frequencies below the range of human hearing.

infrasonic sensor means a passive boundary-penetration sensor designed to detect a change in pressure, such as the pressure change caused by opening a hinged door.

intruder means a trespasser who has entered an area for any reason without permission.

insider means a person having authorized access to facility premises and information and who thereby has the opportunity to carry out or to aid others to carry out malevolent acts which could adversely affect the safety, security, or operational capability of the facility.

intrusion detection system (IDS) means a subsystem of a physical protection system which combines sensing, controlling, and annunciating functions such that intrusion attempts into the area under protection are detected and reported with a minimum of direct human observation.

intrusion sensor means a device which detects and annunciates an unauthorized entry or attempted entry into an area under protection in response to an event or stimulus within its detection zone resulting from the intrusion; also called an intrusion detector.

laser means light amplification by stimulated emission of radiation, refers to a device which produces an intense, coherent directional beam of ultraviolet, visible, or infrared light by stimulating electronic, ionic, or molecular transitions to lower energy levels.

LED means light-emitting diode, a semiconductor crystal that illuminates when electric current passes through it.

line-of-sight sensor means an intrusion sensor requiring line of sight between its transmitter and receiver or between the target and the receiver.

line supervision means capability of detecting tampering and/or circuit interruption, usually provided by digital modulation over circuit lines accompanied by interrogation and reply schemes.

logic level means 1) an electronic-signal voltage level that defines the presence or absence of an event. 2) one of the two logic states, expressed as zero or one, on or off, high or low.

magnetic reed switch means an electromechanical boundary-penetration sensor designed to change switch states by the action of a magnet.

magnetic switch means a passive, covert, boundary-penetration sensor which is a magnetic position indicator. (See also balanced magnetic switch.)

mask means to disable certain areas of an intrusion sensor's field of view.

master means a device which is capable of asserting or controlling an operation.

mean time between failures (MTBF) means a statistical figure representing the average time between equipment or component failures.

mean time to failure (MTTF) means a statistical figure representing the average time between initial start-up and the first failure of components or pieces of equipment for a given grouping of identical devices.

mean time to repair (MTTR) means a statistical figure representing the average time between component or equipment failure and the completed repair of the unit.

microswitch means a mechanical switch, derived from the trade name Microswitch.

microwave means extremely short electromagnetic wave, 1 GHz or higher in frequency, especially one shorter than 30 cm in wavelength.

microwave sensor means an active, visible volumetric sensor which employs microwave energy to detect motion of an intruder.

MIL SPEC means military specifications.

modulate means to vary the amplitude, frequency, or phase of an electronic signal in order to encode information on the signal.

monostatic means an active intrusion sensor in which the transmitter and the receiver are collocated.

motion sensor means any intrusion sensor employing the principle that motion in an area under protection upsets an established balance to generate an alarm.

MTBF see mean time between failures.

MTTF see mean time to failure.

MTTR see mean time to repair.

multistatic means an active intrusion sensor which has multiple separate receivers and/or transmitters.

Mumetal means a high-permeability alloy of iron and nickel especially valued for use as a magnetic shield.

NAR means nuisance alarm rate.

NEC means National Electrical Code.

NFPA means National Fire Protection Association.

Nicad battery means the trade name of an alkaline storage battery in which the positive active material is nickel oxide and the negative contains cadmium; characterized by low-temperature and low-discharge features as well as a relatively long and trouble-free operational life.

NILECJ means National Institute of Law Enforcement and Criminal Justice.

nuisance alarm means an intrusion alarm resulting from a stimulus other than an intrusion.

OR means a type of gate, in digital systems and other switching circuits, which delivers an output signal when one of several input signals is present. (See also AND.)

OSHA means U. S. Occupational Safety and Health Administration.

outsider means a person who does not have authorized access to facility premises and information.

P_d see probability of detection.

passive infrared (PIR) sensor means a passive, visible volumetric sensor designed to detect rapid thermal changes in its field of view.

passive sensor means an intrusion detection sensor which produces no signal from a transmitter but simply detects energy emitted in the proximity of the sensor. (See also active sensor.)

passive sonic sensor (sound discriminator) means a passive, visible, boundary-penetration detector which employs microphone circuitry to detect specific sounds or sound frequencies, such as those produced by breaking glass.

passive ultrasonic sensor means a passive, visible boundary-penetration sensor, known as a sound discriminator, employing a high-frequency microphone to detect frequencies associated with breaking and entering which occur above the audible range, usually 30 kHz and higher.

phototransistor means a transistor in which current carriers emitted as a result of illumination constitute an input-signal current which is amplified by the transistor.

physical protection system (PPS) means a security system concerned with physical measures designed to safeguard people and to prevent unauthorized access to equipment, facilities, nuclear material, and documents and safeguard them against damage and loss.

piezoelectric means a material, such as crystalline quartz, Rochelle salt, tourmaline, or various synthetics, which delivers a voltage when mechanical force is applied to its faces or which changes shape when a voltage is applied.

piezoelectric sensor means a passive, covert, vibration boundary-penetration sensor which converts mechanical vibrations into electrical signals utilizing a piezoelectric element designed to respond to a specific frequency range, such as that associated with the sound of breaking glass.

piezoresistance means the tendency for the electrical resistance of a semiconducting material to change when the material is stretched or compressed.

PIR see passive infrared sensor.

plunger means a common term for the actuating arm of a mechanical switch.

point protection means the use of sensors to detect activity at or immediately adjacent to a protected object or the placement of the protected object inside a hardened container such as a vault or a safe.

position indicator means a boundary-penetration sensor which employs a principle that allows the sensor to ascertain whether a door or window is open or closed.

PPS see physical protection system.

probability of detection (P_d) means the likelihood of detecting an adversary within the zone covered by an intrusion sensor.

protected volume means the volume in which a single detection unit provides reliable detection.

pyroelectric means the production of electricity in certain crystals caused by a change of temperature.

radio frequency (RF) means an electromagnetic wave frequency intermediate between audio and infrared frequencies, named because of its application to radio communications, considered to be approximately 10 kHz to 100,000 MHz.

range gating see time gating.

reactance means the opposition to the flow of alternating current caused by inductance or capacitance of a component or a circuit.

redundancy (fail-safe operation) means including duplicate or alternate system elements in a system design to enhance operational reliability by ensuring continuing operation in the event of failure of a primary system element. The use of multiple components, each capable of performing the same function, in order to increase the reliability and thus the availability of the overall system.

relay means an electrically operated switch which opens or closes contacts when voltage is applied or removed.

resonance means the enhancement of the response of an electrical circuit to a periodic excitation when the excitation frequency is equal to a natural frequency of the system. (See also tuned circuit.)

response means the act of alerting, transporting, and staging a security force to intercept the adversary and to stop him before his goal is achieved.

retroreflector means a device which reflects radiation, such as light, so that the paths of the reflected rays are parallel to the paths of the incident rays.

sector means a defined portion of the intrusion detection system that may have multiple sensors and dedicated CCTV coverage.

secure mode means the security state of a sensor during which no traffic is permitted through the area under protection and both intrusion and tamper alarms are displayed at the operator's console. (See also access mode.)

self test means a feature often available on sensors which allows them to be tested readily to determine whether they are functioning properly.

SNM see special nuclear material.

sonic means producing or responding to a frequency or frequencies within the audibility range of the human ear, considered to be 15 to 20,000 Hz.

sound discriminator see passive sonic sensor.

sound wave means a longitudinal pressure wave in any material medium, called a sound wave regardless of whether or not it constitutes audible sound; infrasonic, seismic, and ultrasonic waves may be called sound waves.

special nuclear material (SNM) means (1) plutonium, ^{233}U, uranium enriched in the isotope 233 or in the isotope ^{235}U, and any other material which the Commission pursuant to the provisions of Section 51 of the Atomic Energy Act, determines to be special nuclear material, but does not include source material, or (2) any material artificially enriched by any of the foregoing but does not include source material.

spoof means to defeat an intrusion sensor by means of any technique that allows a target to pass through the detection volume without generating an alarm. (See also bypass.)

standby battery means a secondary power source for use, usually by automatic switchover, when the primary power source fails.

strain sensor means a passive, covert intrusion sensor employing a strain gauge to detect the presence of added weight or stress upon a surface.

synchronous detection means a scheme by which a receiver is informed when to expect an input signal to be present.

tamper alarm means an alarm generated by an attempt to access or disable a piece of equipment.

tamper switch means a device designed to produce an alarm when a piece of equipment is disturbed.

time gating means employing a circuit which produces an output only when a specified time interval is satisfied. (See also time window.)

time window means an interval of time during which conditions are favorable or an opportunity exists. (See also time gating.)

transceiver means a radio transmitter and receiver sharing a single housing and perhaps some components.

transducer means a device which converts one kind of energy into another kind of energy, specifically when one of the quantities is electrical, e.g., acoustic or mechanical energy to electrical energy.

tuned circuit means a circuit adjusted in relation to frequency to secure optimum performance: commonly the adjustment is to resonance.

ultrasonic means producing or responding to a frequency above the audibility limit of the human ear, considered to be approximately 20,000 Hz.

ultrasonic sensor means an active, visible, volumetric sensor which detects distortion of its established standing wave pattern caused by motion within its detection envelope.

unknown alarm means an alarm for which the cause is unidentified.

vault means a windowless enclosure designed as a secure repository; having walls, floor, roof, and one or more doors; and constructed to delay penetration from forced entry.

vibration sensor means a passive, visible intrusion sensor designed to detect a specific frequency of vibration in order to provide door or window protection.

video motion detector (VMD) means an electronic device which monitors video signals and senses changes in brightness levels.

visible light means the spectrum of electromagnetic radiation which the human eye perceives as light, commonly described as wavelengths between 0.4 and 0.7 μm or as frequencies from 4.3×10^{14} Hz to 7.5×10^{14} Hz.

visible sensor means an intrusion sensor that is exposed to view. (See also covert sensor.)

VMD see video motion detector.

volumetric sensor means an intrusion sensor whose field of view is a defined volume in space.

vulnerability means the relative accessibility of an area under protection or item to specific risks or threats.

walk test means walking in a specified pattern inside an area under protection to ascertain a volumetric sensor's field of view.

zero field (null; balance) means a magnetic field of zero, the condition of a balanced magnetic switch when it is not in alarm.

zone means a specific volume of space.

DISTRIBUTION:

Barbara Dry (2)
BE Inc.
P. O. Box 381
Hwy 278, Airport Industrial Park
Barnwell, SC 29812

6400 D. J. McCloskey
9540 D. S. Miyoshi, Acting
9543 J. C. Matter (2)
9549 B. J. Steele
9549 J. R. Rodriguez (2)
3141 S. A. Landenberger (5)
3151 G. C. Claycomb (3)
8523-2 Central Technical Files

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-5722
SAND91-0948

2. TITLE AND SUBTITLE
Interior Intrusion Detection Systems

3. DATE REPORT PUBLISHED
MONTH: October
YEAR: 1991

4. FIN OR GRANT NUMBER
L1387

5. AUTHOR(S)
J. R. Rodriguez, Sandia National Laboratories
B. Dry, BE Inc.
J. C. Matter, Sandia National Laboratories

6. TYPE OF REPORT
Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION – NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)
Sandia National Laboratories
Albuquerque, NM 87185

Subcontractor:
BE Inc.
P.O. Box 381
Hwy. 278, Airport Industrial Park
Barnwell, SC 29812

9. SPONSORING ORGANIZATION – NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)
Division of Safeguards and Transportation
Office of Nuclear Material Safety and Safeguards
US Nuclear Regulatory Commission
Washington, DC 20555

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

The purpose of this NUREG is to present technical information that should be useful to NRC licensees in designing interior intrusion detection systems. Interior intrusion sensors are discussed according to their primary applications: boundary-penetration detection, volumetric detection, and point protection. Information necessary for implementation of an effective interior intrusion detection system is presented, including principles of operation, performance characteristics, and guidelines for design, procurement, installation, testing, and maintenance. A glossary of sensor terms is included.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
intrusion detection systems, safeguards, security, physical security

13. AVAILABILITY STATEMENT
Unlimited

14. SECURITY CLASSIFICATION
(This Page)
Unclassified
(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

END

DATE FILMED

01/24/92