NUREG-1959
Revision 1

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Intrusion Detection Systems and Subsystems

Technical Information for NRC Licensees

Office of Nuclear Security and Incident Response

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at the NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Mail Stop SSOP
   Washington, DC 20402-0001
   Internet: http://bookstore.gpo.gov
   Telephone: 1-866-512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Road
   Alexandria, VA 22161-0002
   http://www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at the NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference 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—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
http://www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG-XXXX) or agency contractors (NUREG/CR-XXXX), (2) proceedings of conferences (NUREG/CP-XXXX), (3) reports resulting from international agreements (NUREG/IA-XXXX), (4) brochures (NUREG/BR-XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG-0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-1959
Revision 1

Intrusion Detection Systems and Subsystems

Technical Information for NRC Licensees

Manuscript Completed: September 2017
Date Published: September 2017

Prepared by:

J. W. Bowen, Principal Investigator
S. M. Sohinki
E. L. Potter

Dade Moeller & Associates, Inc.
Richland, WA 99354

James E. Vaughn, PM, NRC Project Manager

NRC Job Code: V6103

Office of Nuclear Security and Incident Response

ABSTRACT

This report provides information about the design, installation, testing, maintenance, and monitoring of intrusion detection systems (IDSs) and subsystems used for the protection of facilities licensed by the U.S. Nuclear Regulatory Commission. It contains information on the application, use, function, installation, maintenance, and testing parameters for internal and external IDSs and subsystems, including information on communication media, assessment procedures, and monitoring. This information is intended to assist licensees in designing, installing, employing, and maintaining IDSs at their facilities.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ac	alternating current
AC&D	alarm communication and display
AGC	automatic gain control
AM	amplitude-modulated (monostatic microwave system)
BMS	balanced magnetic switch
C	Celsius
CAS	central alarm station
CCTV	closed-circuit television
CIF	common intermediate format
codec	coder decoder
dc	direct current
DSP	digital signal processor
DVR	digital video recorder
F	Fahrenheit
f-c	foot-candle
FM	frequency-modulated (monostatic microwave system)
FPS	frames per second
HPS	high-pressure sodium
HTVL	horizontal television lines
I^2	image intensification
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
JPEG	Joint Photographic Experts Group
LED	light-emitting diode
MCP	microchannel plate
M-JPEG	motion JPEG
mm	millimeter
MPEG	Motion Picture Experts Group
NIR	near infrared
nm	nanometer
NRC	U.S. Nuclear Regulatory Commission
NVR	network video recorder
PCU	premise control unit
P_D	probability of detection
PIDAS	perimeter intrusion detection and assessment system
PIR	passive infrared
P_S	probability of sensing
PTZ	pan-tilt-zoom
RF	radiofrequency
SAS	secondary alarm station
SNR	signal-to-noise ratio
UPS	uninterruptible power supply
VMD	video motion detection

1 INTRODUCTION

This report provides information about the design, installation, testing, maintenance, and monitoring of intrusion detection systems (IDSs) and subsystems used for the protection of facilities licensed by the U.S. Nuclear Regulatory Commission (NRC). Title 10 of the *Code of Federal Regulations* Part 73, "Physical Protection of Plants and Materials," addresses the NRC's requirements for the physical protection of nuclear power reactor facilities, independent spent fuel storage facilities, fuel cycle facilities, strategic special nuclear materials, and special nuclear material of moderate and low strategic significance. The specific requirements for physical protection programs at NRC-licensed facilities are determined by the type of NRC licensee and the special nuclear material authorized for possession by that licensee. The use of IDSs at NRC-licensed facilities is one component of a physical protection program.

The effectiveness of a physical protection program depends on the coordination and integration of all the various components of that program, including equipment, procedures, policies, and personnel, and the ability of the licensee to monitor and maintain these components to ensure they operate as intended. A physical protection program should be designed for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks.

This report provides technical details on IDSs suitable for use in physical protection programs that require moderate- to high-level security applications. The report contains information for licensees to consider when designing an IDS and a broad overview of IDS equipment and specialized detection devices. The provisions of this report are not intended as staff positions found in guidance nor as substitutes for regulatory requirements. Licensees considering implementing the technology or practices discussed in this report should consult regulatory guidance specific to the subject matter before implementing any specific IDS measures.

2 INTRUSION DETECTION SYSTEMS

2.1 Overview

A physical protection program typically has three functions: (1) detection, (2) delay, and (3) response. Intrusion detection is the identification of an unauthorized entry. This report addresses the detection function of a physical protection program that includes intrusion sensing, alarm communication, and alarm assessment:

A. Intrusion Sensing. A sensor reacts to a stimulus and initiates an alarm. There are three different types of alarms: (1) zone detection, (2) penetration, and (3) nuisance alarms.

(1) Zone Detection

Volumetric sensors detect intrusion in a volume of space, or the zone of detection. Upon detecting a stimulus within the zone of detection, a sensor initiates an alarm. The detection volume is generally not visible and is hard to identify precisely. Performance tests are used to confirm the detection of intrusion at the proper parameters.

(2) Penetration

A sensor will also react upon detecting penetration or attempted penetration of the established zone of detection and is commonly associated with a barrier. Performance tests are used to confirm the detection of penetrations at the proper parameters.

(3) Nuisance Alarms

A nuisance alarm is any alarm that is not caused by an unauthorized entry, zone detection, or penetration. The nuisance alarm rate is a function of the number of nuisance alarms over a given time period. Usually, nuisance alarms are classified by source. Both natural and industrial environments can cause nuisance alarms. Common sources of natural nuisance alarms are vegetation (trees and weeds); wildlife; weather conditions (wind, rain, snow, fog, and lightning); ground swelling; and soil uplifting. Industrial sources of nuisance alarms include ground vibration, debris moved by wind, electromagnetic interference, traffic, and adjacent industrial activity.

Nuisance alarms generated by the equipment itself (whether by poor design, improper application, inadequate maintenance, or component failure) are called false alarms. Because of design and configuration differences, some intrusion detection sensors are more susceptible to nuisance or false alarms than others.

For any IDS, when choosing a sensor, one needs to consider the applicable nuisance alarms associated with that sensor.

B. Alarm Communication. The information from the sensor and assessment subsystems is reported and displayed for assessment.

C. Alarm Assessment. Security personnel assess the information to judge whether the alarm is valid or invalid. Detection without assessment is not considered detection. Because not all sensor alarms are caused by unauthorized entries, an alarm assessment system is needed. Assessment is the process of determining whether the source of the alarm is an unauthorized entry or a nuisance alarm. If the alarm is assessed as a nuisance alarm, it is not considered a valid attempt at intrusion.

Intrusion detection and assessment systems are an integral part of any physical protection system. Detection and assessment provide a basis for the initiation of an effective security response. IDSs should be designed to facilitate the detection of attempted and actual unauthorized entry into designated areas and should provide the security force with prompt notification of the detected activity from which an assessment can be made and a response initiated. The design of the detection and assessment aspects of a physical protection system should incorporate various methodologies to provide a fully integrated detection capability. The integration of various detection and assessment methodologies not only contributes to a superior detection and assessment capability but also provides multiple overlapping layers that support each other if one method fails.

An IDS consists of exterior and interior intrusion sensors, video assessment, and alarm communication systems all working together. The intrusion detection boundary is ideally a box that encloses the assets or facilities under protection and enables detection of all intrusions or attempted intrusions.

The Perimeter Security Sensor Technologies Handbook, issued 1997, by the Defense Advanced Research Projects Agency contains additional information on typical methods that an intruder may use to bypass or avoid detection by an IDS.

2.2 Exterior Intrusion Sensors

2.2.1 Microwave Sensors

2.2.1.1 Principles of Operation and Performance

Microwave sensors are motion detection devices that flood a specific area with an electronic field. Movement in the area disturbs the field and generates an alarm. Microwave sensors are typically used for detection in long, flat, narrow perimeter zones. They are classified as active, visible, volumetric, freestanding, and line-of-sight sensors. Microwave sensors typically transmit microwave signals in the X or K band (10 or 24 gigahertz). A diode that operates within preset limits that do not affect humans or the operation of pacemakers generate these signals. Figure 1 depicts the application of microwave sensors within a perimeter intrusion detection and assessment system (PIDAS). Note that the illustrated detection zone goes from the front microwave to another one that is more than 90 meters (more than 300 feet) away. The middle microwave transmits to a unit behind the photographer. This configuration is referred to as a “basketweave” layout.

Figure 1 Application of microwave sensors within a PIDAS

The effective detection zone width and height of a given microwave system will largely depend on the mounting height of the antennas when it is operating over the same type of surface at the same range. The mounting height is measured from the center of the antenna aperture to the ground. When properly aligned, the maximum detection height and width will occur at midrange. During installation in the field, antenna heights can be adjusted for maximum signal while monitoring the signal at the receiver. Detection zone sizes are normally stated for midrange between the transmitter and receiver at the maximum antenna separation.

2.2.1.2 Types of Microwave Sensors

Microwave systems have two basic configurations:

(1) bistatic configuration, which consists of a transmitter and receiver antenna located at either end of a perimeter sector

(2) monostatic configuration, which uses a transceiver

The bistatic microwave link consists of a transmitter at one end of a long, flat location and a receiver module at the other end. The transmitter emits a modulated, low-power signal in the microwave frequency band. The signal at the receiver antenna is combined in a vector summation of the direct line-of-sight signal and the reflected signals from the ground and nearby objects. The receiver monitors this signal for small changes that occur when objects move into the detection zone of the sensor. When the changes in the zone exceed an established threshold, an alarm is generated.

Automatic gain control circuitry is used to allow the microwave sensor to compensate for very slow changes in signal because of environmental conditions.

The size and shape of the detection zone are determined by the antennas, the transmitted frequency, and the distance between the antennas. The detection zone typically resembles an oblate spheroid, much wider and taller in the middle of the detection zone and narrowing on each end (refer to Figure 2).

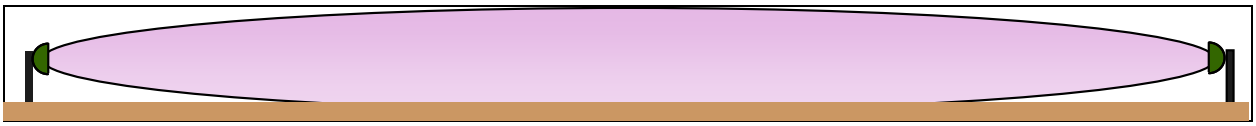


Figure 2 The detection zone of a typical bistatic microwave

A monostatic microwave unit consists of a transmitter and receiver located in the same unit (refer to Figure 3). The two types of monostatic microwave systems are amplitude modulated (AM) and frequency modulated (FM). An AM monostatic microwave system detects changes in the net vector summation of the received signal, similar to a bistatic system. Because an FM monostatic system operates on a pulsed Doppler principle, it can determine range information. To help minimize nuisance alarms, some pulsed Doppler microwave sensors can be set up to detect only motion moving toward or away from the sensor. These are finding usage in some specialty applications, such as on ladders or stairs where the adversary has only limited approach options.

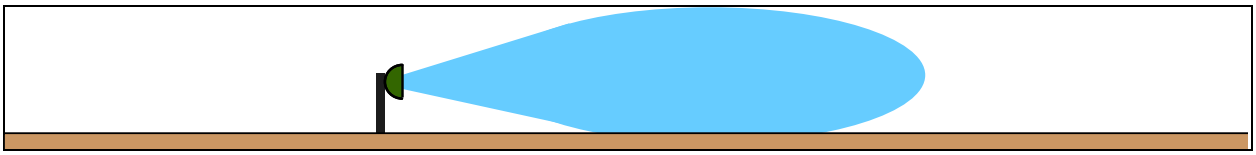


Figure 3 The detection zone of a typical monostatic microwave

In general, the useful range of a monostatic microwave is considerably less than that of a bistatic system. Monostatic microwave sensors are usually recommended only for application in areas inappropriate for a bistatic microwave.

2.2.1.3 Sources of Nuisance Alarms

Although a microwave sensor works fairly well in most weather conditions, some types of weather extremes may cause nuisance alarms (in particular, the first few seconds of a hard rain). Normally, after the rain has started, the sensor recognizes and adapts to the rain. Large puddles of standing water can cause nuisance alarms if wind creates ripples on its surface. Running water is also a major source of nuisance alarms if the sensor zone does not have proper drainage.

Most flying debris (e.g., leaves, paper, cardboard, tumbleweeds) will not cause an alarm because these objects are not reflective. However, if these same objects were wet or icy, they would likely cause the system to alarm. Because it is highly reflective, an aluminum can will also cause an alarm.

Although a microwave will normally not detect an animal as small as a mouse or a single bird, it will likely detect animals the size of a rabbit or a flock of birds.

If the fabric of a chain-link fence moves, the reflection may cause an alarm even though the fence is outside of the zone of detection.

2.2.1.4 Characteristics and Applications

Microwave sensors have the following characteristics and applications:

- The microwave is a volumetric sensor and has a large detection pattern.
- To a potential adversary, the detection pattern of the microwave is unknown.
- Microwaves may be stacked to create a much taller detection pattern.
- The microwave works well in most weather conditions.
- The microwave is appropriate for long, narrow, flat zones.
- The microwave will be able to detect in snow as long as the antenna is not blocked.
- Microwaves are typically vulnerable to crawling intruders immediately below and in front of both the transmitter and receiver.
- Microwave sensors do not work well in extremely heavy fog or in a wet, heavy snow.
- Microwaves will not perform well in a rainy climate when drainage is poor.
- Microwave sensors do not work well in areas where the terrain has large variations.
- Site preparation for a microwave installation can be difficult because very flat terrain is necessary.
- Microwaves will not work well in a zone between two fences that are not at least 6 meters (20 feet) apart.
- Vulnerabilities have been noticed when microwaves are operated near runways at airports.

2.2.1.5 Installation Criteria

Installation procedures should comply with manufacturer's recommendations. To operate effectively, a bistatic microwave perimeter detection system should typically be installed at a distance between antennas of not more than 120 meters (approximately 328 feet). Successive microwave links and corners should overlap to eliminate dead spots (areas where the microwave sensor cannot detect) immediately below and in front of transmitters and receivers. The required amount of overlap of successive links is contingent on the antenna pattern, alignment, and mounting height, but it may be up to 10 meters (approximately 32.8 feet) in length for some models. Overlap should be adequate to provide continuous detection of crawling intruders over the entire sector (see Figure 4 and Figure 5).

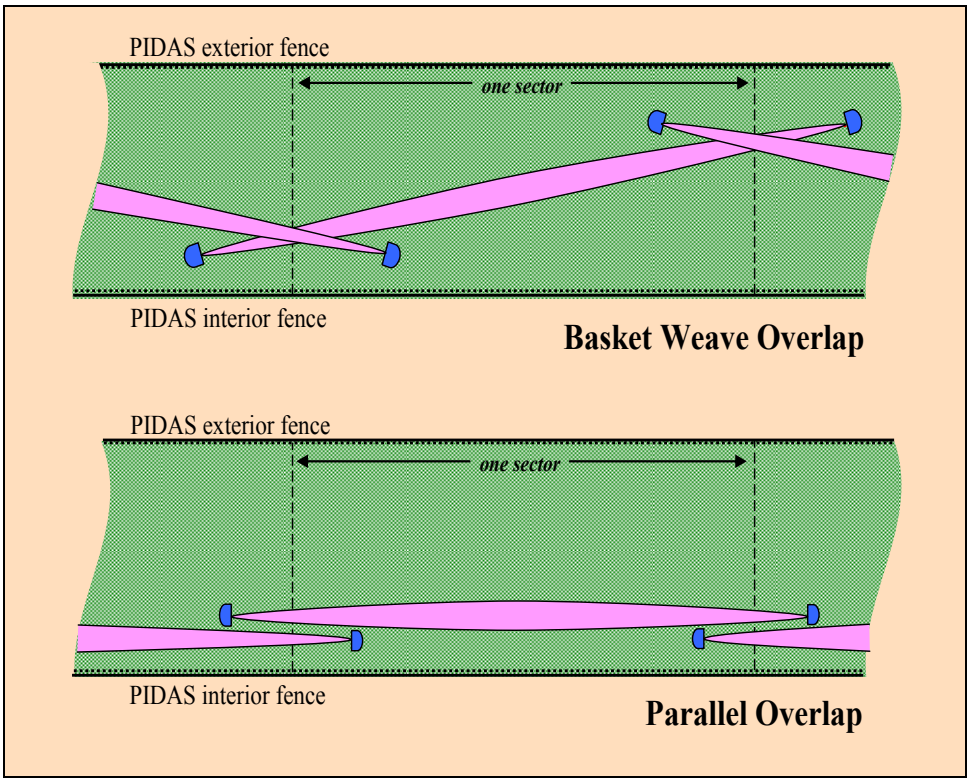


Figure 4 Examples of possible microwave sensor layouts

Figure 5 Example of a corner setup of microwave sensors that provides overlap

There should also be an area at each end of the sector where both microwave links detect a crawling intruder to ensure continuous detection between adjacent sectors.

Because the bistatic transmitter/receiver link is a line-of-sight system, variations in ground level (e.g., ditches and valleys) could allow intruders to crawl under the beam, bumps or obstructions may create shadows in the beam that the adversary could crawl behind, and variable obstructions (e.g., snow drifts or accumulations) may interrupt the beam. To prevent passage under the beam, variations in the ground should be leveled, ditches should be filled, and obstructions should be removed so that the area between the transmitter and receiver is clear of obstructions and free of rises or depressions. Overlaps should be adequate to allow the beam to expand enough to detect an intruder attempting to jump over the beam.

In zone overlap areas, the equipment for the overlapped zones should usually be transmitters or receivers to minimize the interference between the successive links. Different modulation frequencies are used for microwave links in adjacent sectors to prevent interference from other microwave transmitters.

Because standing water can be a major source of nuisance alarms, proper drainage is required to prevent standing water and to prevent erosion that may provide the adversary with low spots where crawling is more difficult to detect. Gravel is often used for the perimeter surface to allow water to drain quickly and to minimize erosion. Solid surfaces, such as asphalt or concrete, may prevent erosion problems but may actually cause a higher nuisance alarm rate during periods of heavy rain because of the rain bouncing off the surface.

Each microwave unit should be mounted securely on rigid posts and aligned according to the manufacturer's installation criteria. The mounting pole of the microwave for the adjacent sector should not give an adversary the ability to jump over the beam. Cutting down the mounting pole or using a spike or other attachment that does not allow the adversary a solid jumping platform may be required. Figure 6 depicts a scene from a test of microwave sensors and shows the possibility of an adversary using the microwave mounting structure as an aid to jump over its own detection zone. Note that the addition of the microwave patterns shown in the photograph for illustration purposes.

Figure 6 Microwave mounting structure used to jump over the detection zone

Because of variances in the antenna patterns of different microwave systems, the height may need to be varied slightly to obtain adequate coverage to detect crawling intruders. Accordingly, the mounting mechanisms for a system should permit adjustment of antenna height and position to correct poor performance or alignment.

Conduit should be used to protect wiring; flexible conduit should be used near the sensor to allow alignment and adjustment of the antenna.

The clear area (the space between the two PIDAS fences) should be sufficiently wide to preclude the generation of alarms by legitimate movements near the microwave link (e.g., personnel walking or vehicular traffic) and to preclude system degradation caused by reflections from any structure such as the perimeter fence. The manufacturer should provide approximate dimensions of the microwave pattern. Because the beam is relatively wide, care should be taken to ensure that reflections from authorized activities do not create nuisance alarms. If the microwave link is installed inside a perimeter barrier or between a double perimeter barrier, the transmitter and receiver should be positioned so that the height of the zone of detection will detect anyone jumping or attempting to bridge over the beam into the protected area from atop perimeter barriers such as fences or walls. Typically, the distance between a chain-link security fence with an overall height of 2.4 meters (8 feet) and the center of the beam should be a minimum of 2.4 meters (8 feet). In addition, the microwave link should be positioned within the isolation zone to maximize the zone of detection and enhance assessment once detection is made. Neither a transmitter nor a receiver should be mounted on a fence.

Stacking of microwave sensors is one means of increasing the detection zone height of the system to enhance its detection capabilities. The stacking technique places a microwave link close to the ground to provide better crawl detection and one or more links higher to improve detection of jumping or bridging (refer to Figure 7; note that the possibility of crawling beneath the microwave detection zone has been reduced significantly because the microwave sensor is installed close to the ground). The stacked units may use different carrier frequencies, different antenna polarization, or multiplexing to prevent interference between the microwave links.

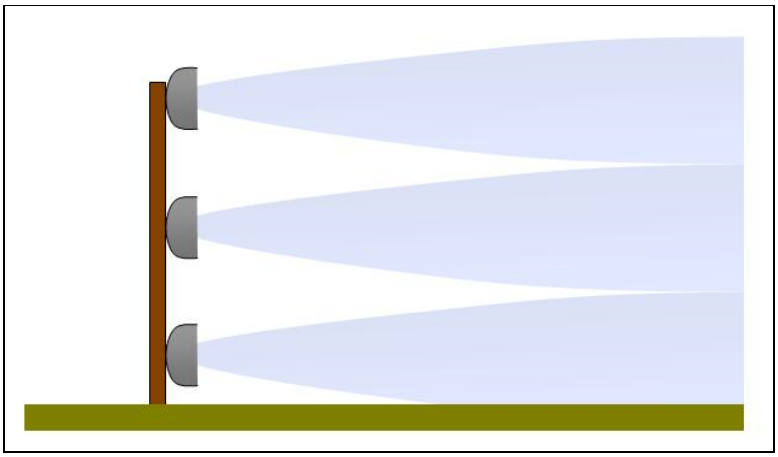


Figure 7 An example of stacked microwave sensors

2.2.1.6 Testing

Testing procedures should comply with manufacturer's recommendations. A regular program for the testing of microwave sensors is imperative for maintaining them in optimal operating order. Three types of testing need to be performed during the life of a microwave sensor: (1) acceptance testing, (2) performance testing, and (3) operability testing.

2.2.1.6.1 Acceptance Testing

When first installed, a microwave sensor should be tested in order to be formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test:

- A physical inspection ensures proper installation of the microwave unit and should do the following:
  - Verify that the installation matches the installation drawings, which should follow the manufacturer's guidance.
  - Verify sector intersection spacing.
  - Verify that the signal and power wires are routed in the conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
- A performance test establishes and documents the level of performance.

Section 2.2.1.6.2 describes the type of tests that are recommended for the microwave sensor.

2.2.1.6.2 Performance Testing

Generally accepted performance criteria for a microwave detection system are that the system should be capable of detecting an intruder weighing a minimum of 35 kilograms (77 pounds) through the zone of detection between the transmitter and receiver, including the area in front of both the transmitter and receiver. Detection should occur whether the individual is walking, running, jumping, or crawling.

Provisions should be made to ensure detection in spite of the dead spots in front of transmitters and receivers.

Procedure 1: Crawl Tests

Conduct 30 crawl tests within the detection zone/sector to verify that the probability of crawl detection is at least 90 percent at a 95-percent confidence level.

Each sector should be tested 30 times at points along the length of the microwave detection zone, although the overlap areas of two microwave sensors should be the primary focus.

Because it can be difficult to locate an adult of approximately 35 kilograms (77 pounds) and because crawling is viewed as the most favorable form of spoofing a microwave sensor, most sites use an aluminum sphere that is 30 centimeters (approximately 11.8 inches) in diameter to simulate crawl tests (refer to Figure 8). The sphere diameter represents the cross-sectional area (at microwave frequencies) of an intruder lying parallel to the beam centerline. Pulling the sphere across the zone at slow speeds can determine whether the microwave sensor is capable of detecting a small, stealthy individual. Because the radar cross-section of the sphere does not change with its orientation and because the physical demands on the tester are much less than performing actual crawl tests, the sphere test can yield more repeatable results that eliminate variability because of the size and skill of actual crawling individuals.

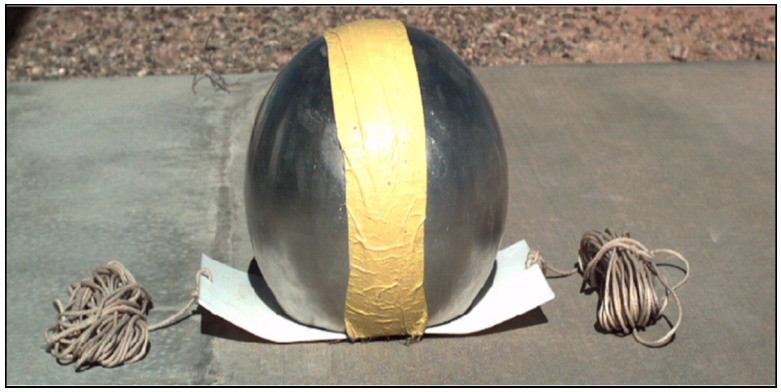


Figure 8 Aluminum sphere used to simulate crawl tests of the microwave detection system

If the aluminum sphere is not detected until after it has been pulled across the centerline of the microwave detection zone, the sensor may need an additional adjustment to address an area of weak detection. A small individual can perform actual crawls in limited locations to supplement the sphere drag test, perhaps testing in areas where the sphere was not detected until after it had crossed the beam centerline.

The aluminum sphere should be mounted on a nonmetallic platform or base that does not raise the height of the sphere or increase the radar cross-section. The base is usually a sled but sometimes has wheels that help prevent the sphere from becoming dented. As the sphere becomes dented, the radar cross-section increases and no longer accurately represents a small individual. The cord used to pull the sphere across the zone should be nonmetallic so that it does not affect the beam. Nylon sash cord can be used effectively. The cord should be long enough to allow the testers to be completely out of the microwave detection area (refer to Figure 9).

Figure 9 Testing of microwave sensors with an aluminum sphere

Procedure 2: Other Tests

Another method of performance testing incorporates the use of a combination of the common defeat methodologies (e.g., walking, running, jumping, climbing, crawling, and bridging) within each zone of detection to verify a system's detection capability. Each sector should be tested 30 times at points along the length of the detection zone. Walk tests may be useful for mapping out a sensor's detection pattern to identify antenna misalignments, but the detection of a walker is not normally considered "challenging" for a microwave detection system.

Run tests are suggested because some microwave sensors have a high-speed cutoff to eliminate some types of nuisance alarm sources. Jumping, climbing, and bridging tests should be performed to verify that the height and overlap of the beam are adequate. Jumps that are assisted or unassisted and that use nearby objects as a jumping platform should be performed to verify that detection is adequate. Similar to crawl tests, an aluminum sphere with a 30-centimeter (approximately 11.8-inch) diameter can be used to simulate jump tests. Although an aluminum sphere tests the microwave sensors from the ground level during crawl tests, using the same sphere for jump tests would test the microwave sensors from a third dimension as it is dropped down vertically. Each defeat methodology used for performance testing should be conducted in the different areas of the zone being tested.

2.2.1.6.3 Operability Testing

The operability test may be conducted by having an individual walk into the expected detection zone of the microwave sensor. If no alarm is received, a maintenance request should be immediately generated, and implementation of compensatory measures should be considered based on site-specific requirements.

2.2.1.7 Maintenance

Recommended maintenance procedures should include the manufacture's recommendations and the following measures:

- Check vegetation or erosion in the areas of the microwave detection pattern.

- If the sensor has not experienced any recent problems (i.e., failure to alarm during a walk test) and if the most recent performance test was successful, adjusting the alignment or sensitivity setting of the unit is not necessary.

- At least one manufacturer recommends waxing the antenna covers periodically.

- Look for any evidence of damage to the sensor or tampering with the device.

2.2.2 Electric Field Sensors

2.2.2.1 Principles of Operation

Electric field sensors (often referred to as e-field sensors) consist of posts or other supports with wires strung between them (refer to Figure 10). In its most basic form, the sensor comprises one field wire and one sense wire. An oscillating electrical signal is applied to the field wire, which establishes an electromagnetic field around the field wire. A sense wire is located close to and parallel to the field wire. Some of the field energy is coupled to the sense wire. A processor analyzes the received energy and monitors changes to the energy level. Most of the signal coupling results from capacitive coupling. The energy level coupled to the sense wire depends on the electrical ground (also referred to as earth ground), the spacing of the wires, the length of the wires, and the dielectric of the medium (air) between the wires. A human body is mostly water, and the dielectric of water is about 100 times greater than that of air. As an intruder approaches the wires, the signal coupled to the sense wire is disturbed because of the higher dielectric of the intruder's body and because the intruder is partially in contact with an electrical ground provided by the earth (refer to Figure 11).

Figure 10 Example of an electric field sensor installed in a test environment

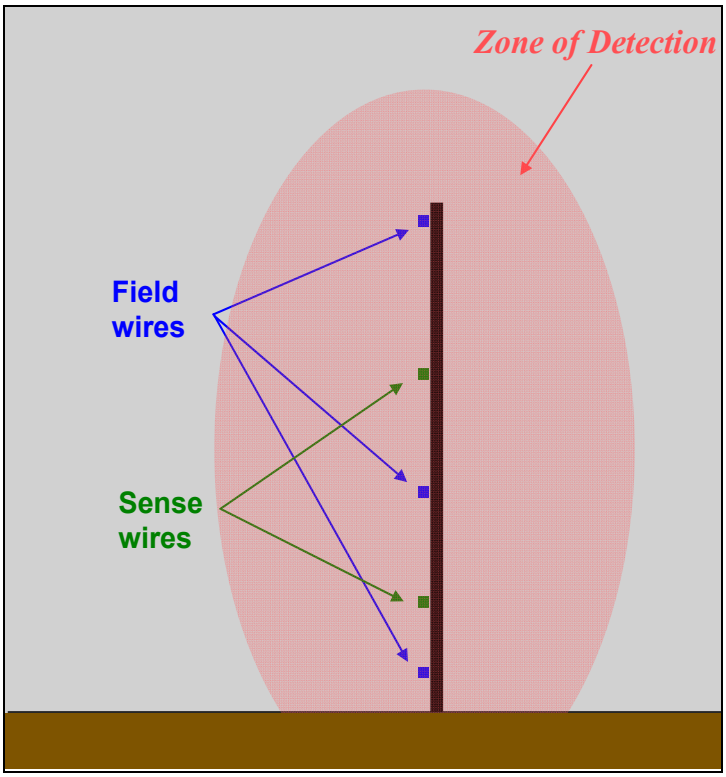


Figure 11 A cross-section of an electric field sensor's zone of detection

Older electric field sensor processors were based on detection of a sufficient change in amplitude (threshold) of the analog signal that did not occur too fast or too slowly (bandpass filtering) to be considered an intruder. Unfortunately, many environmental sources could cause disturbances that would meet these simple conditions for an alarm. Newer models employ digital processing and sophisticated pattern recognition software to generate an alarm. This change has significantly reduced nuisance alarms for new electric field sensors while maintaining good levels of detection.

Electric field sensors are volume detectors. They can usually follow the terrain where they are installed. Although their characteristic wires give them the appearance of a line-type sensor, the electric field generated by these wires extends the zone of detection well beyond the wires. Electric field sensors can have a very wide detection volume (up to 2 meters or 6.5 feet wide) and a very tall detection volume (4.9 meters or more than 16 feet) based on the installation configuration. To achieve these heights, a single electric field system can incorporate combinations of multiple field and sense wires.

2.2.2.2 Types of Electric Field Sensor Applications

Electric field sensors can be installed in a freestanding configuration on their own posts. They can also be installed on chain-link fences, on the top of building roofs, on the side of building walls, and on the top of concrete walls if special supports are incorporated (refer to Figure 12). Various wire configurations can be used to accommodate these mounting situations to yield the desired detection height and volume. Because of their adaptability to various vertical and horizontal surfaces, electric field sensors may work in areas that are not compatible with the use of other sensors.

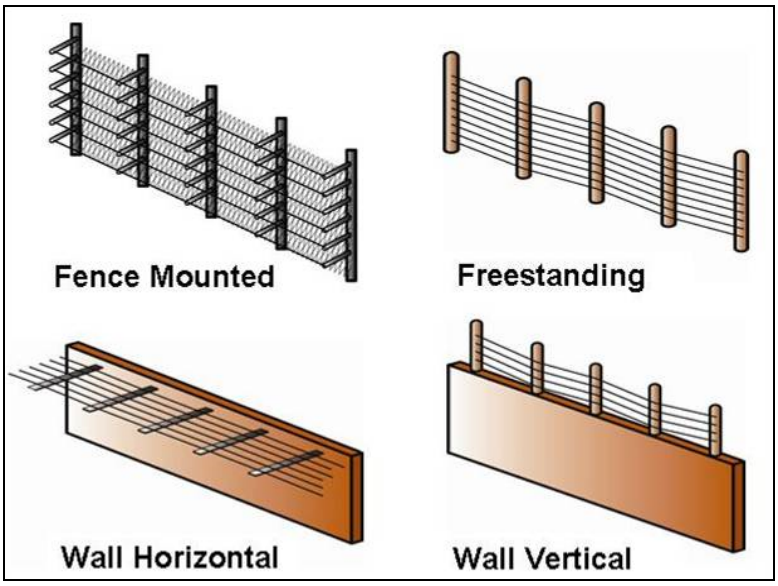


Figure 12 Various configurations for electric field sensors

2.2.2.3 Sources of Nuisance Alarms

Proper installation of electric field sensors is critical to minimizing nuisance alarms. Any ungrounded metal object in the vicinity of an electric field sensor that can change potential can cause a nuisance alarm. For example, a chain-link gate may have grease in the hinges that partially insulates it from the rest of the fence, but small wind-induced motion may occasionally result in contact between the gate and the metal of the hinge, which can cause a nuisance alarm. Attaching the sensor ground and all metal within the vicinity to a common electrical ground (earth ground) can reduce nuisance alarms.

Weather-related sources of nuisance alarms include rain and wet or melting snow. During the start of a heavy rain, a few nuisance alarms should be expected. However, the newer electric field processors can quickly recognize the pattern of rain and, after recognition, will ignore it while still maintaining detection levels. During snowstorms, even with the bottom wire covered with snow, the sensor should still detect acceptably. The potential for nuisance alarms exists during periods of very heavy, wet snow or when the snow is melting and possibly creating conduction paths to ground.

Small animals that touch the wires and larger animals that approach the wires may cause alarms. The use of nuisance control fences can significantly reduce these alarms. A single bird landing on a wire generally will not cause an alarm, but a flock of birds may. The wires of an electric field sensor are small enough that larger birds generally do not land on the wires.

Wet plants or wet weeds that touch the wires can also cause alarms. Using nuisance control fences (to reduce blowing debris) and maintaining a sterile area (to prevent plant growth) near the wires can significantly reduce these nuisance alarms (refer to Figure 13).

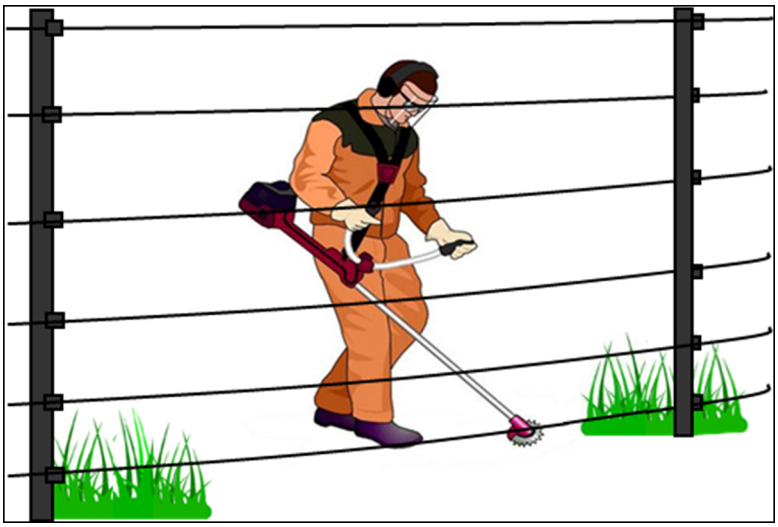


Figure 13 Prevention of plant growth near wires

2.2.2.4 Characteristics and Applications

Electric field sensors have the following characteristics and applications:

- Electric field sensors operate well in most environments.
- Configurations can be tuned to have a very large and relatively even detection volume; such configurations can make an electric field sensor very difficult to defeat or circumvent.
- A variety of mounting configurations can be used (e.g., the sensor can be mounted on an existing chain-link fence (with some reduction in detection volume), or it can be mounted on its own posts in a freestanding configuration (preferably between two fences)).
- Electric field sensors can be installed on walls and roofs, thus making it easier to maintain a continuous line of detection if a building is located within the perimeter.
- Electric field sensors can follow uneven terrain with posts spaced approximately every 6 meters (20 feet); the wires can be routed up and over gentle hills and valleys.
- The installation of electric field sensors usually requires a factory-trained installer or experienced alarm technician.
- As the horizontal parallel wires of an electric field sensor naturally form a type of fence, this configuration presents an operational barrier to the entry of authorized vehicles or personnel. If personnel or vehicles require access through the perimeter of a protected area, a different sensor (other than the electric field sensor) must be incorporated to allow for continuous and even detection through the entry area.

- Because this sensor is a volumetric sensor, large moving metal objects near the sensor can cause nuisance alarms. If the electric field sensor application includes an area where the frequency of vehicles passing close to the sensor could cause numerous alarms, a different sensor type should be considered.

- An intruder slowly attempting to crawl under the bottom wire is a potential defeat method. The bottom wire height should be evenly parallel to the ground and low enough to detect all crawlers. There should be no areas (e.g., a ditch caused by erosion or other low depression) where the wire height may create an area of vulnerability.

2.2.2.5 Installation Criteria

An electric field sensor installation requires many components (sense wire, various insulators, posts, and support hardware) (refer to Figure 14 for details).

Because proper system installation is vital for proper performance, installers should be factory trained or experienced technicians and should follow the manufacturer's installation instructions.

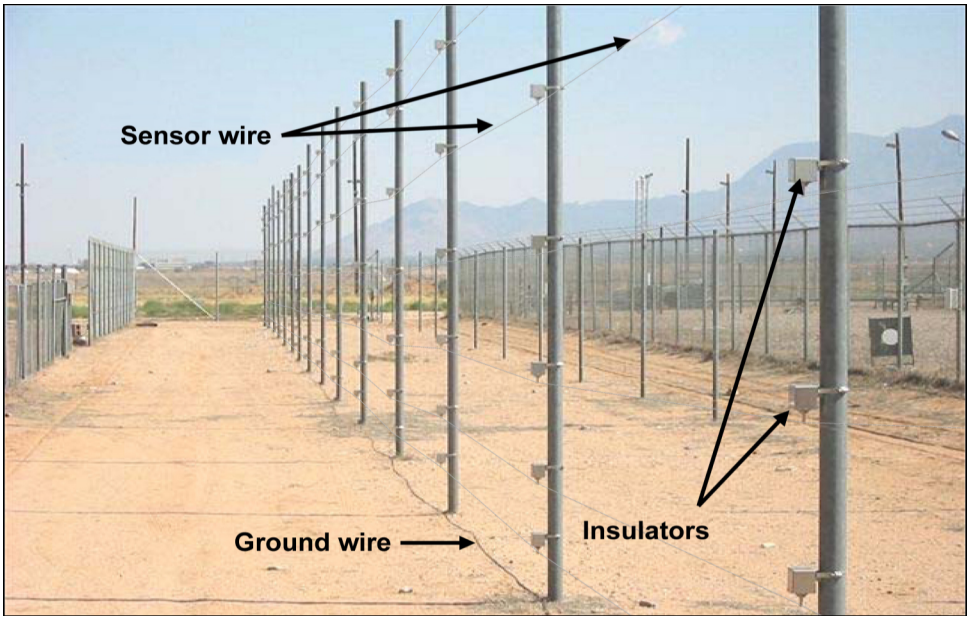


Figure 14 Main components of an electric field sensor installation

The single most important detail in the installation process is that every piece of equipment or hardware must be connected to a common ground. This includes any electrically conductive structures or objects that are near the sensor system. The manufacturers of electric field sensors provide installation instructions that specify grounding procedures that include the installation of a common ground wire and copper-clad steel rods that are driven into the ground.

Installed configurations may be freestanding (where the wires are mounted on their own dedicated poles) or may be attached to an existing sturdy fence. A freestanding installation is usually considered preferable; installation on a chain-link fence will effectively cut out half of the detection volume (that half on the side of the fencing that does not contain the electric field sense wires).

An electric field sensor system may also be mounted or attached directly to the wall or roof of a building. If the wall or building is not constructed of a material that can provide an adequate electrical ground (earth ground), a grounded metal screen can be installed under the sensor that will provide the needed ground reference.

A cleared area must be created where the sensor system will reside. Ideally, this area should not allow access by passing pedestrians or animals. Weeds near an electric field sense wire must be eliminated or kept well trimmed.

2.2.2.6 Testing

Testing procedures should comply with manufacturer's recommendations. Three types of testing must be performed during the life of an electric field sensor: (1) acceptance testing, (2) performance testing, and (3) operability testing.

2.2.2.6.1 Acceptance Testing

When first installed, an electric field sensor should be tested before it is formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the electric field sensor and should do the following:
  - Verify that the installation matches the installation drawings, which should follow the manufacturer's guidance.
  - Verify sector intersection spacing.
  - Verify that signal and power wires are routed in conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
- A performance test establishes and documents the level of performance.

2.2.2.6.2 Performance Testing

System or component modifications (e.g., processor replacement or adjustment, wire spacing, height adjustments) or any change to the electric field sensor (or in the vicinity of the sensor) that might affect the detection capability would require performance testing to verify system performance.

The performance test should include a visual inspection of the electric field sensor and of the general area where the sensor is installed. The test should record all relevant processor readings and compare these to the last recorded readings. It should measure the lower wire height at all the posts and midway between the posts and then should compare these values to previous values documented when the sensor system was judged to have been performing optimally.

Because an electric field sensor is a volume detector, it will detect the approach of an intruder at some distance from the sense wires and an intruder penetrating the wire array. Although these systems or sectors of these systems may detect an approach at some distance, in some cases the zone of detection may be such that detection occurs upon penetration of the zone between or near the sense wires. The performance test must confirm that penetrations or attempted penetrations of the wire array that forms the electric field sensor system are detected at the required level. To ensure the overall effectiveness of an electric field system, performance testing should incorporate the use of a combination of common defeat methodologies (e.g., crawling, walking, jumping, climbing, bridging) applicable to an electric field system within each zone of detection. Each sector should be tested 30 times at various points along the length of the electric field detection zone.

If a facility uses various defeat methodologies for performance testing, it should use each defeat methodology in the different areas of the zone being tested. If each of the 30 tests results in a detection, the electric field sensor sector has been confirmed to have at least a 90-percent probability of detection (P_D) at a 95-percent confidence level. Particular attention should be given to any low depressions and to the areas where sectors overlap (one of the sectors must alarm in this area).

Because an electric field sensor is most susceptible to defeat by crawling individuals, the 30 test attempts may include more crawl tests than the other defeat methodologies. For crawl tests, the tester should lie down flat on the ground outside the detection volume of the sensor with his or her head toward the wires. The tester should weigh 35 kilograms (77 pounds) or more. The tester should crawl slowly (approximately 5 to 15 centimeters (2 to 6 inches) per second or in accordance with manufacturer specifications) under the sense wires, keeping the motions as smooth as possible and stopping when a detection occurs (see Figure 15). The crawler must fully penetrate the wire array to a point beyond the detection volume on the opposite side of the sensor to declare a nondetection.

Figure 15 An example of the crawl test procedure

For fence-mounted electric field sensors, the tester cannot possibly exit the detection volume because of the physical barrier of the fence. In this case, the sensor is not considered defeated simply by the tester's head or arm penetrating the plane of the wire array without a detection. The tester should continue to move his or her body through the wire array, attempting complete penetration. In addition, because an intruder must take some action to also penetrate the fence (such as cutting a hole in the fence or standing up to climb the fence), the intrusion test should include a reasonable simulation of the motion and tools required to simulate an intruder climbing over the fence, cutting through the fence, or going under the fence.

2.2.2.6.3 Operability Testing

Operability tests should be conducted by walking to the immediate vicinity of the electric field sensor wires and attempting to penetrate the zone of detection until an alarm is communicated and is received in the alarm station.

During operability tests, the area in which the system or components are being tested should be surveyed for evidence of damage to equipment or possible tampering that may have occurred.

2.2.2.7 Maintenance

Maintenance procedures should comply with manufacturer's recommendations. The required routine maintenance is mainly associated with inspecting the components and inspecting for ungrounded metal objects, plant growth, or debris, or a combination of these near the area. The sense wires of an electric field sensor are tensioned so that they vibrate at a frequency that is outside the signal frequency of interest. Verifying the tension of the sense wires and the inspection of system components should be part of the regular maintenance and may be combined with the scheduled testing of the sensor. An increase in nuisance alarms indicates the need for physical inspections.

Routine maintenance inspections should do the following:

- Inspect for weed growth, sterilize the soil, or remove any growth near the sense wires.
- Inspect for and remove any debris that could cause nuisance alarms.
- Inspect the wire for proper tension and for any poor or broken connections.
- Inspect and clean dirt or debris (e.g., insects, spider webs) from insulators, as necessary.
- Inspect all mechanical parts for damage.
- Inspect all sensor electrical ground (earth ground) connections.
- Inspect nearby metallic objects for good ground connections.
- Confirm wire heights by looking for eroded or low areas where the sense wire height may be too high. Document the maximum bottom sense wire height determined to be acceptable to provide adequate detection.

2.2.3 Ported Coaxial Cable Systems

2.2.3.1 Principles of Operation

A ported coaxial cable system (commonly referred to as "ported coax") is a terrain-following, volumetric, covert IDS that consists of two buried, ported coaxial cables and a processing unit (refer to Figure 16). The processor contains a transmitter, a receiver, various amplifier and filter circuits, and a microprocessor with associated hardware and software. This system is an active electromagnetic sensor using two identical "leaky" coaxial cables (i.e., the shielding of the cable

has holes or “ports” in it) buried parallel in the ground. The transmitter portion of the processor is connected to one cable, and the receiver is connected to the other.

Because the outer conductor of the cables is ported (i.e., it contains closely spaced small holes or gaps in the shield that allow radiofrequency (RF) energy to radiate), any electromagnetic energy injected into the transmitter cable is radiated into the surrounding medium, and some of this energy is coupled into the receiver cable through its ported shield. Thus, a static field of coupling is established between the cable pair. An intruder entering the established field perturbs the coupling, and the change in received signal is digitally processed. Changes in this electromagnetic field that exceed threshold levels cause an alarm.

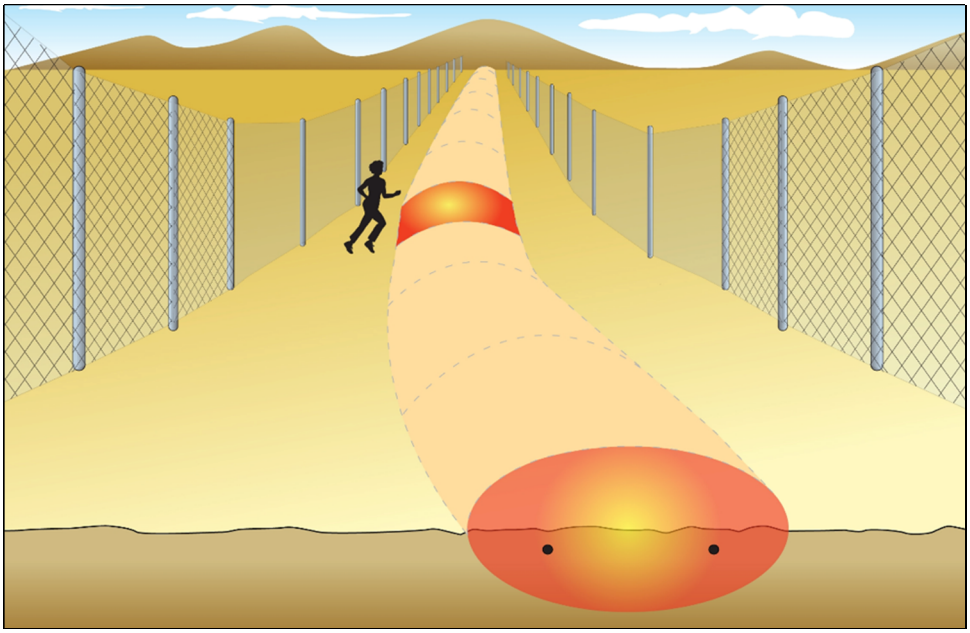


Figure 16 An illustration of the covert zone of detection for a ported coaxial sensor

Ported coaxial sensors are sensitive to changes of dielectric or conductivity within the detection zone and are insensitive to seismic noise. The cross-section of the detection zone is somewhat elliptical and can be up to 1 meter (3 feet) high and 3 to 4 meters (9 to 12 feet) wide. Detection is achieved both above and, to some extent, below the ground (refer to Figure 17). Tests have shown that both the detection zone size and detection sensitivity vary along the sensor cables. Such variance may result from several causes, such as phase cancellations, buried metallic objects, variation in cable separation or burial depth, and variable soil composition. Therefore, it is important to identify the low-sensitivity areas and to adjust the sensitivity or the installation to achieve an adequate detection volume.

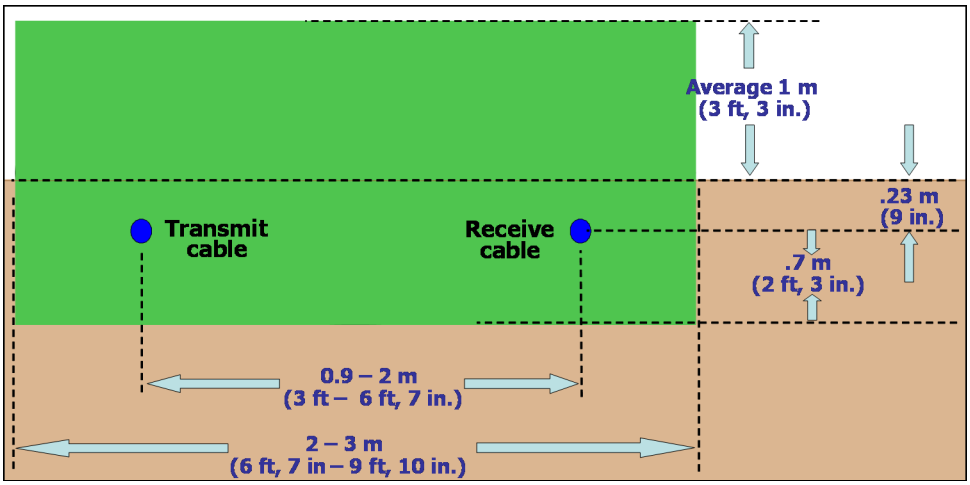


Figure 17 A typical installation and detection envelope (green) for a ported coaxial sensor

Soil characteristics affect the signal strength of the ported coaxial receiver signal. Variations in soil moisture are reflected in changes in ported coaxial signal attenuation. Wet soil is more conductive than dry or frozen soil; therefore, seasonal changes may affect ported coaxial detection sensitivity. However, even sites that have relatively large soil attenuation have implemented operational ported coaxial systems. Recalibration is often required to account for seasonal changes.

2.2.3.2 Types of Ported Coaxial Cables

Either pulsed or continuous wave RF energy can be used in a ported coaxial sensor (refer to Figure 18 for more details).

In principle, the pulsed system operates as a guided radar; therefore, it can both detect and locate the intruder (i.e., location along the cable length). Because of the ranging capabilities of this type of system, detection zones can be set in the software, enabling the configuration of more than the traditional two sectors per processor. This is possible because of the sensor's capability to divide each ported coaxial sensor cable into small subcells, usually 1 or 2 meters (3.28 or 6.56 feet) in length. Each of these subcells can be independently adapted to the site conditions and analyzed. This capability enables the alarm threshold to be varied in each of these subcells, thus providing uniform detection along the entire length of the cable.

Continuous-wave ported coaxial sensors perform no range processing; therefore, they transmit continuously or during specified times. The frequency of operation is approximately 40 to 60 megahertz. There is only one alarm threshold per set of sensor cables, and the cables are the length of the sector. The continuous wave system detects the intruder but does not localize the presence along the cable length. Each processor can monitor one or two channels (or sectors) and can indicate an alarm if an intrusion occurs anywhere in the zone of detection.

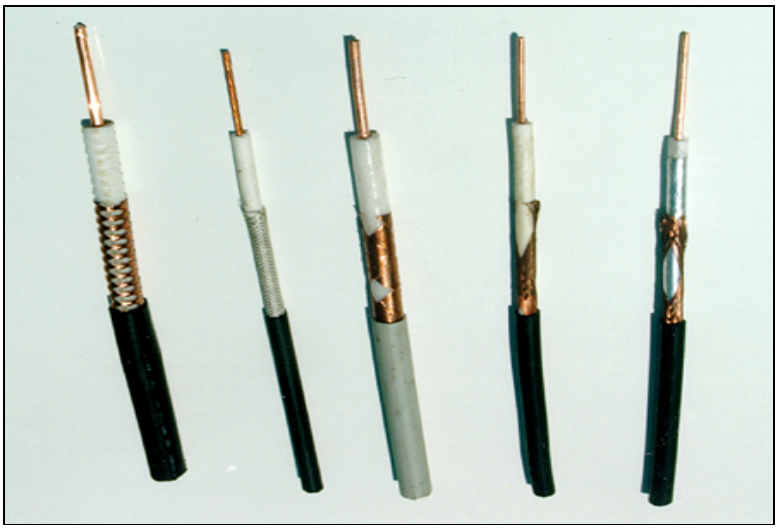


Figure 18 Examples of ported coaxial cables

2.2.3.3 Sources of Nuisance Alarms

The nuisance alarm rate for ported coaxial sensors is relatively low in a well-designed and carefully installed system, but several environmental and installation factors can affect the rate of detection (refer to Figure 19). The major source of nuisance alarms is surface water from rain or melting snow, which makes proper drainage essential. Flowing water and standing water that produces ripples when the wind blows will contribute to movement that the sensor targets.

Movement of metallic objects (e.g., automobiles and fences) or dielectric objects (e.g., animals, people, and plants) in the vicinity of the ported coaxial sensor cables can result in alarms. Small animals weighing less than 4 kilograms (9 pounds) generally do not cause alarms unless they cross the sensor cables in groups. The magnitude of the nuisance alarm rate also depends on the type of sensor, the installation method, maintenance practices, and the sensitivity setting.

Figure 19 Example of a nuisance alarm source for ported coaxial cable detection systems

2.2.3.4 Characteristics and Applications

Ported coaxial sensors have the following characteristics and applications:

- They have volumetric, covert detection capabilities. To bypass and defeat the sensor, the intruder must guess the location of the detection envelope.

- They are often used where esthetic considerations dictate a sensor technology that is unseen by the general passerby.

- Because they are very effective in detecting a crawling intruder, they are often used as a complementary sensor to other sensor technologies (e.g., microwave, electric field, or active infrared technologies) that may have a weakness in detecting this method of attack.

- The pulsed ranging systems have the added benefit of allowing the use of a lower number of processors to monitor multiple perimeter sectors.

- Even though the detection envelope of the ported coaxial sensor can be relatively wide in volume (depending on cable spacing), it is limited in height, and any method that allows an intruder to bridge over it could result in a successful defeat of the system. If not protected, nearby fences and utility poles can be used for this purpose. For this reason, the installation of a ported coaxial sensor as a standalone system around a perimeter for high-security applications is generally not recommended.

- The installation of this system requires extensive trenching. In addition, once the system is installed, any needed maintenance of the cables or decouplers buried in the ground could require significant effort to locate and repair these components.

- Even though the system follows the terrain and does not require a straight line of sight, site preparation is very important to ensure proper drainage to reduce nuisance alarms caused by runoff.

- Depending on the location, installing a good fence system to isolate the cables from animals is also important to reduce the nuisance alarm rate to an acceptable level.

2.2.3.5 Installation Criteria

Ported coaxial cable systems should be installed according to the manufacturer's specifications. Generally, this type of system can operate in longer segments than other detection system. However, restricting detection zones to segments of 100 meters (328 feet) or less to facilitate assessment is recommended. The system follows the terrain and can be curved around corners as long as the minimum radius specifications are observed. The maximum and minimum separation of the transmitter and receiver cables can vary from approximately 2 meters (6.6 feet) to being collocated in a single trench. The clear zone available and the proximity of the cables to objects that may interfere with the sensor's detection envelope dictate the separation of the cables. The cables are generally buried at a depth of 0.23 meters (9 inches) (refer to Figure 20).

The installation of ported coaxial cable perpendicular to buried metal conduit for electrical cables or metal pipes used for water or storm drains may degrade detection capabilities or

cause nuisance alarms. Separation distances dictated by the manufacturer should be strictly observed. Soil conductivity should be considered when installing this type of sensor as it may reduce the detection volume. Soil found to have relatively high conductivity may cause the detection field to be reduced. Highly conductive soil contains concentrations of iron or salt. Moving objects in the zone of detection (e.g., foliage, flowing or standing water, grasses) may create nuisance alarms. In addition, rodents can chew through ported coaxial cables.

Figure 20 A typical ported coaxial cable system installation

Sensor locations should be carefully selected to prevent nuisance alarms from such sources as personnel and vehicular traffic. Similarly, the cleared area above the sensor should be controlled to prevent the placement of objects within the area (even temporarily) that would degrade the detection zone. The ported coaxial cables should be installed on well-drained terrain cleared of trees, tall grass, and bushes. Freezing or thawing of the ground may affect system sensitivity. Neither the transmitter nor the receiver lines should be mounted above ground.

The system should be installed relative to perimeter fencing so that the transmitter and receiver lines are positioned to prevent an intruder from avoiding detection by jumping over the electromagnetic field. Typically, the distance between chain-link security fencing with an overall height of 2.4 meters (8 feet) and the center of the detection zone should be a minimum of 2.4 meters (8 feet).

Fixed metal objects and standing water distort the radiated field, possibly to the extent of creating insensitive areas with no or very low detection. Nearby metal objects and utilities should be located outside the detection volume. This includes aboveground fences and poles and underground water and sewer lines and electrical cables installed close to the surface (refer to Figure 21).

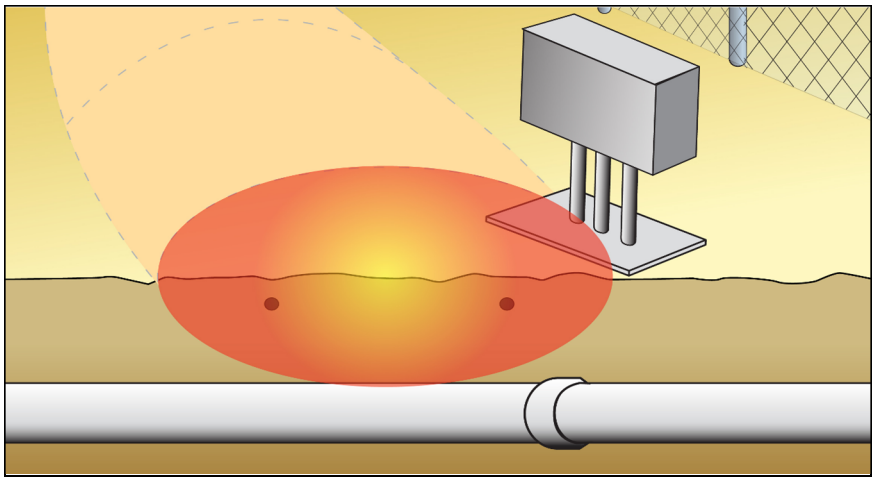


Figure 21 Example of metal objects or utilities located near a ported coaxial system

The manufacturer's instructions should be followed when installing ported coaxial cable across concrete or asphalt areas. Particular attention should be given to the binding agent and the application of epoxy over the cable groove after the cable is installed in the concrete or asphalt.

Criteria for ported coaxial cable system installation include the following:

- Ensure that the ground in which a ported coaxial cable system is buried is firm and is not subject to movement.
- Ensure that drainage is adequate because surface water (standing or flowing) can cause ported coaxial cable systems to generate false alarms.
- Rodents can chew through ported coaxial cable—be aware of their burrows.
- Avoid intersecting irrigation pipes and power lines with the ported coaxial cable, or ensure that separation distances specified by the manufacturer are observed.
- Note that the detection zone may be elongated at curves.
- In rare cases of extreme soil conditions (very sandy or highly conductive), soil conductivity tests may be warranted to ensure that the system's performance is not compromised.

2.2.3.6 Testing

A regular program of testing sensors is imperative for maintaining them in optimal operating order. All testing should follow the manufacturer's recommendations. Three types of testing must be performed during the life of a ported coaxial sensor: acceptance testing, performance testing, and operability testing.

2.2.3.6.1 Acceptance Testing

When first installed, a ported coaxial sensor should be tested before it is formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the ported coaxial sensor and should do the following:
  - Verify that the installation matches the installation drawings, which should follow the manufacturer's guidance.
  - Verify sector intersection spacing.
  - Verify that signal and power wires are routed in the conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
- A performance test establishes and documents the level of performance.

The section below describes the performance testing procedure for the recommended tests.

2.2.3.6.2 Performance Testing

A ported coaxial cable perimeter detection system should be capable of detecting an intruder passing over the transmitter and receiver wires, whether the intruder is walking, running, jumping, crawling, or rolling.

The P_D is affected by the installation configuration of the cables, the system processor settings, soil conductivity, intruder orientation and speed, and the proximity of metallic objects.

Testing should ensure that the device is capable of detecting the defined target with a site-specific P_D of 90 percent and a confidence level of 95 percent. The system should detect a person crawling, running, or jumping through any area of the detection volume. For this reason, performance testing should include these defeat methodologies. Testing has shown that using a "duck walk" profile (walking in a crouched position) to pass through the detection volume produces the smallest disturbance to the system (refer to Figure 22). Sensor parameters should be set to detect this type of intrusion.

Figure 22 The duck walk test method for a ported coaxial system

2.2.3.6.3 Operability Testing

Operability tests should involve simple walk tests. The tester should walk through the expected detection zone of a ported coaxial sensor and confirm that the alarm has been received at the alarm station. Operability tests should include a search for any evidence of tampering or damage to the sensor.

2.2.3.7 Maintenance

Because the ported coaxial cables are buried and largely inaccessible after installation, maintenance to the system is minimal and involves the processor and the environment where the system is installed. Periodic checks should be conducted at least every 6 months and should include the following:

- If applicable, check terminations and decouplers between sectors of sensor cable that are located aboveground for signs of wear or leakage.
- Inspect the processor enclosure for any physical damage, water damage, corrosion, and ingress of insects.
- Inspect the cable connections (coax, signal, or power) to ensure that they are tight.
- Check the processor electrical ground (earth ground) connection for continuity and corrosion.
- Check the input power for proper voltage. Check the battery status, if applicable.

- Inspect the areas above the sensor cable for vegetation, debris, water accumulation, erosion, and settling of trenches. Correct as necessary.

- Verify processor parameter settings to ensure that no undocumented changes have been made.

2.2.4 Active Infrared Sensors

2.2.4.1 Principles of Operation

Active infrared sensors are infrared beam-break sensors that detect the loss or significant reduction of infrared light transmitted to a receiver. Infrared light is invisible to the naked eye, although some digital or video cameras can detect it. In its simplest form, an active infrared sensor consists of a single infrared transmitter that illuminates a single infrared receiver. In most security applications, an active infrared sensor comprises two columns of multiple infrared transmitters and multiple infrared receivers. This arrangement can provide a detection volume of significant height. The actual volume of detection is defined by all the beams (cylinders of infrared light) between the transmitters and the receivers and has the diameter of the optical lenses of the receiver and transmitter. In a multibeam active infrared sensor, the actual volume of detection is composed of the numerous infrared beams that shine between the two columns (refer to Figure 23; the dotted lines represent infrared light beams). The columns can be separated by up to 152 meters (500 feet) or more for some types. The lowest beam is generally located within 15 centimeters (6 inches) of the ground to detect crawlers; the upper beams can generally be spaced further apart.

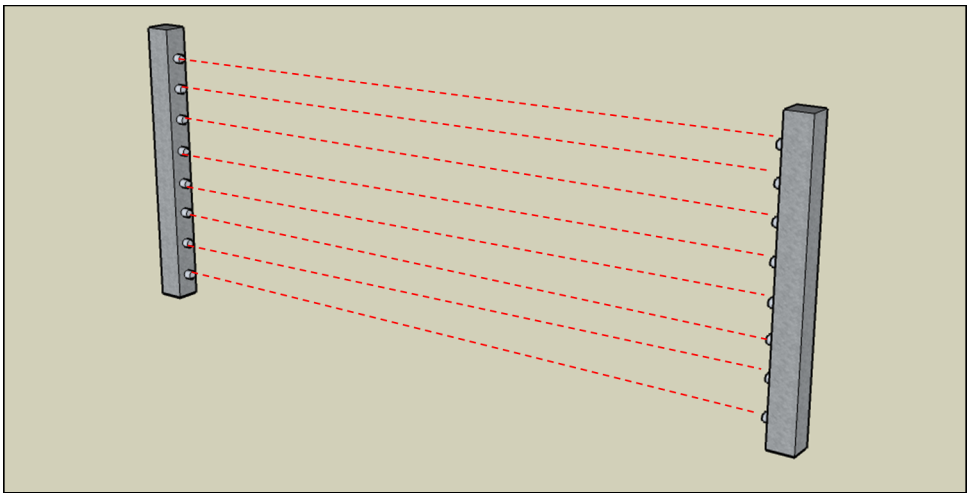


Figure 23 Multibeam active infrared sensor columns

Detection is based on blocking one or more of the beams for a specific period of time. Shorter measured beam interruption times are discounted to reduce nuisance alarms from small birds or blowing debris. Some models allow for user adjustment of this beam interruption time, whereas others automatically vary the time depending on the number of beams interrupted.

The infrared light is generally modulated and sequenced to reduce sensitivity to other light sources; this allows the sensor to operate in daylight and at night. The sequencing for some models allows the use of multiple sensor sets without mutual interference in case they happen to be within the field of view of an adjacent sensor set.

2.2.4.2 Types of Active Infrared Sensors

Active infrared sensors vary in size, beam configuration, range of operation, and operational features. They typically operate in ranges that allow them to be compatible with the sector lengths used in exterior perimeter applications. A single-beam unit will have limited application because of the small, single-beam detection volume. Many manufacturers provide sensors that can be combined to provide whatever detection height is required for an application.

Some models can communicate to a remote laptop or other computer, which allows them to be remotely configured or adjusted. Some models also allow the user to turn off the lowest beam (e.g., if the ground is covered by snow) to allow the remainder of the beams to operate normally. Most models have sealed beam assemblies or heaters that keep frost and condensation from forming on the optical covers and lenses. Some units can be sequenced so that they will operate if their transmitters are in the field of view of an adjacent sector's receivers. Licensees should consider these and other features of the different models available depending on the specific application and operational environment.

There are various designs of active infrared systems with varying transmitter, receiver, and beam configurations (refer to Figure 24 for more information).

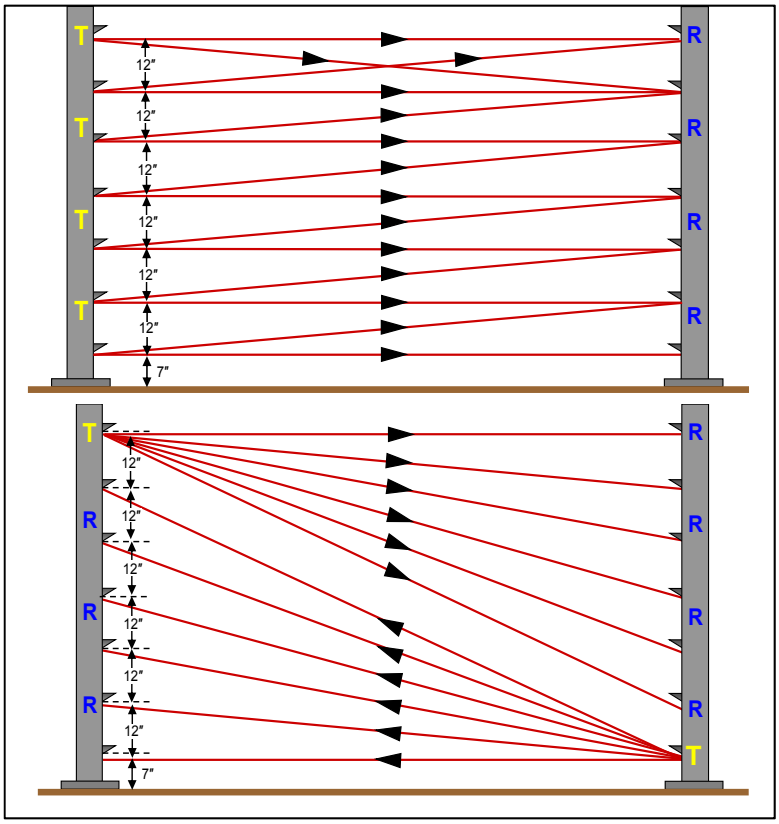


Figure 24 Active infrared sensor variations in beam configuration

2.2.4.3 Sources of Nuisance Alarms

Nuisance alarms can be caused by anything that can block or significantly obscure the infrared beam. Nuisance alarms from animals large enough to block the bottom beam can be minimized by installing the sensor between two fences. A single bird flying through an infrared beam will generally not cause an alarm, but a flock of birds may sufficiently block a beam to cause nuisance alarms.

Blowing debris that blocks the bottom beam can cause alarms. Snow accumulation to a depth that covers the lower beam will cause a constant alarm that must be cleared by removing the snow or disabling the lower beam (on sensors with that capability). A disabled lower beam could allow an intruder to crawl under the sensor undetected; once the snow has been removed, the sensor should be restored to full operation.

Heavy snow or fog that is thick enough to obscure the visibility from the transmitter to receiver may cause nuisance alarms. Bright lights (e.g., dawn or dusk sunlight during certain times of the year) that shine directly into the receiver can cause a nuisance alarm or a failure alarm. Some models have modules that contain both a transmitter and a receiver. In these models, the beam actually consists of two beams, one going in either direction. Both beams must be blocked or interfered with to cause an alarm.

2.2.4.4 Characteristics and Applications

An active infrared sensor has the following characteristics:

- line-of-sight operation
- volumetric detection that resembles line detection
- beam-break sensors (not field disturbance sensors)
- imperviousness to motion around it

These characteristics make active infrared sensors especially useful in confined areas or in areas where there is much activity nearby. Thus, active infrared sensors are successfully used in entry control portals to substitute for a sensor that would block traffic flow or would have a high rate of nuisance alarms. Active infrared sensors can operate over any surface and can "see" through chain-link fences as long as a fence post or pole does not block any beams.

Active infrared sensors are successfully used in perimeter applications. Because of their uniformity and detection height, active infrared sensors make a complementary sensor to other types of sensors that have good crawl detection but lack the significant detection height that an active infrared sensor can achieve.

Most models can operate well in a typical PIDAS sector length of 100 meters (328 feet). However, if local weather conditions have the potential to produce periods of reduced visibility, the installed operating distance should be reduced to 80 meters (approximately 264.2 feet) or less. This design practice is also good for the alarm assessment (video) system because poor visibility affects video as well. Those models with a shorter operation range can employ multiple sets of combined active infrared sensors to accommodate the required sector length.

Some active infrared sensors can be applied to special applications. They can be adapted to provide detection across doorways or windows or across critical access doors. They can be installed across pedestrian and vehicle access openings in a PIDAS. Because of their modular

nature and narrow detection width, active infrared sensors can be adapted to many areas that would be difficult or impossible for other types of sensors to monitor well.

Because the active infrared sensor detects a break in the beam rather than a disturbance in the field, a potential adversary can more readily identify its detection volume. An intruder can closely approach the sensor without concern of detection as long as the beams are avoided. This means that, if the detection height is configured to be 1.8 meters (6 feet) or less, an intruder aided by a step ladder could easily defeat the sensor by climbing the ladder and jumping over the top beam. Luckily, active infrared sensors can be configured to be 3.7 meters (12 feet) or higher. Jumping from this height becomes much more difficult; therefore, if an active infrared sensor is fairly short in height, it should be combined with a field disturbance sensor that can prevent a close undetected approach by an intruder and detect attempts by the intruder to crawl under the active infrared's lowest beam. The height of the zone of detection of an active infrared system should account for the design and configuration of physical barriers near the zone of detection to ensure that the system protects against bridging.

Because active infrared sensors are line-of-sight sensors, the ground between the transmitter and receiver columns must be relatively flat and planar (i.e., lying in a single geometric plane). An intruder can use any low areas to crawl undetected under the bottom beam. Even if the ground is flat and level, if an intruder can dig a trench without detection, it is possible that he or she could quickly create a path onto the site under the bottom beam. If an active infrared sensor is used alone, a hard surface (e.g., concrete sill or sidewalk) should be installed under the beams to prevent trenching and minimize the potential for the system to be circumvented.

Licensees should carefully consider using an active infrared sensor in locations that experience frequent deep snow, drifting snow, or dense fog. During times when the lower beam is covered and disabled, crawl defeat is possible unless the active infrared sensor is used in combination with another sensor that can detect an intrusion through the snow. In addition, the sensor may go into constant alarm during periods of dense fog. During these periods, a complementary sensor that is not normally affected by fog would be very important in the detection of intruders.

2.2.4.5 Installation Criteria

An infrared beam system(s) should be installed according to the manufacturer's specifications. A cleared area must be created around the sensor system location. Ideally, this area should be protected from passing pedestrians or animals. Isolating the detection equipment between fences gives such protection and other security benefits. It is critical that weeds be eliminated in this area to avoid attracting animals and to prevent tall plant growth from blocking the infrared beams.

The active infrared sensor should be mounted on a sturdy foundation that will not heave as the ground freezes or move in the wind. Most models have a field of view that will tolerate very small motion, but movement significant enough to misalign the beams will increase the sensor's susceptibility to nuisance alarms.

Active infrared sensors should be installed over ground that is flat and even. In a standalone configuration, the sensor should have a detection height of 3.7 meters (12 feet) or more and should be installed over a hard surface made of concrete or other material to prevent the digging of a trench beneath the lower beam. In a standalone installation, the lower beam should be no higher than 15 centimeters (6 inches), depending on the size of the optics. Therefore, a crawling intruder must interrupt the beam sufficiently (typically a 98-percent beam block) to

cause an alarm at any location between the transmitter and receiver. Some models will not have a beam this low. The alternatives include using an active infrared sensor in a complementary combination with another sensor that will detect a crawler or installing a hard surface beneath the sensor that is high enough to reduce the distance to the lower beam and to allow for crawler detection.

In locations that are susceptible to freezing, a sensor heater option is available for many models. The heater is typically controlled thermostatically and requires considerably more power than that for the sensor electronics. Care should be taken to size the wire appropriately for the electrical current requirements of the sensor heater.

To be effective, all perimeter sensors should be installed in continuous lines of detection. Sensor overlap should be provided for the active infrared sensor. The layout must be designed in a way that prevents gaps large enough for an intruder to maneuver around the beams of adjacent sectors. One method used for intersecting sectors is to “basket weave” the active infrared sensors. An intersection can also be made by overlapping the beams in parallel to enable the beams of each sector to pass very close to the transmitter or receiver column of the adjacent sector. To avoid interference, the transmitter should face the adjacent transmitter, and the receiver should face the adjacent receiver (refer to Figure 25).

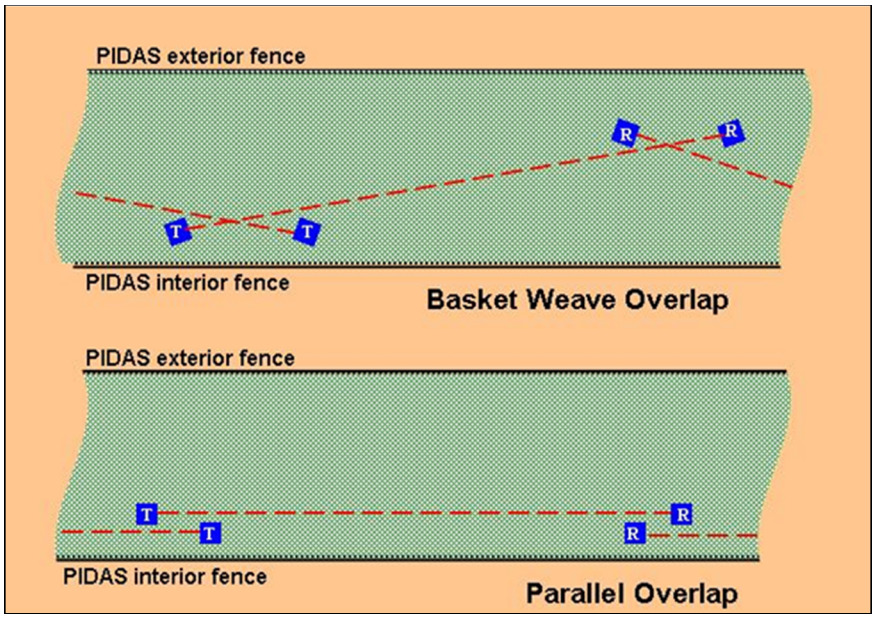


Figure 25 Active infrared sector intersection method

Another method, a variant of the parallel method, mounts the transmitter and receiver columns from adjacent sectors next to each other, leaving no gap large enough to allow an intruder to pass between them. Once installed, the active infrared sensor modules must be aligned to their matching receiver or transmitter on the opposite column. Poor alignment can result in a poorly received infrared signal level. This, in turn, can result in increased nuisance alarms.

2.2.4.6 Testing

Active infrared sensors or systems, or both, should be tested in accordance with the manufacturer’s specifications.

2.2.4.6.1 Acceptance Testing

When first installed, an active infrared sensor should be tested before it is formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the active infrared sensor and it should do the following:
  - Verify that the installation matches the installation drawings, which should follow the manufacturer's guidance.
  - Verify sector intersection spacing.
  - Verify that signal and power wires are routed in conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
  - Perform an optical alignment on all units to verify that all modules are operational and oriented correctly (i.e., the method of optical alignment is specific for each manufacturer's model).
- A performance test establishes and documents the level of performance.

2.2.4.6.2 Performance Testing

A performance test should be designed to verify the level of performance of each active infrared sensor through its range of intended function and should include the use of all defeat methodologies applicable to the system. The replacement of the electronics module, a change to the optical alignment, or any adjustment that could affect the unit's sensitivity are examples of system changes that require performance testing. The performance test should use the documented levels of performance from the original acceptance testing to verify that the sensor is still performing adequately.

The following list describes a recommended performance test for an active infrared sensor:

- Include a visual inspection of the sensor and of the general area where the sensor is installed.
- Record all relevant processor readings. Compare these readings to the last recorded readings from the acceptance test or the previous performance test. Each manufacturer's model will have different sensor settings. Make a special note regarding any significant settings that may influence the detection ability or the nuisance alarm rate of the sensor.
- Active infrared sensors can have a P_D for a walking intruder that appears to be perfect ($P_D = 1$) because the sensor is a beam-break sensor and has no direct adjustment for sensitivity. Breaking the infrared beam for the prescribed time will produce an alarm if the electronics are not defective. Confirm that the sensor produces an alarm output that

is communicated to the alarm system in response to a beam break of each beam. Cover each beam and verify that an alarm is produced. Do this at both columns.

- Because most units employ a timing feature, confirm that a fast-moving intruder will be detected when penetration occurs. A person should penetrate the sensor moving as fast as possible while avoiding the bottom beam, which sometimes has a faster beam-interruption time than that of the other beams.

- Test the area where the sensors overlap to verify that each attempt to bypass the sensor produces an alarm on either the sector being tested or the adjacent sector.

- Bypassing the beams by crawling under them or by aided climbing and jumping over them can defeat the active infrared sensor. Pay particular attention to any low places. If used in a standalone configuration, verify that the hard surface underneath the lowest beam is intact. Verify that attempts to crawl under the sensor are always detected at the location where the greatest gap exists under the lower beam. If this location cannot be readily identified, distribute the crawl test along the length of the sector being tested.

- If the active infrared sensor is used as part of a complementary sensor system and if the other sensor is used to detect the crawler or to detect climbing approaches that use ladders or other aids, test that additional sensor to verify that it functions as intended (by detecting what its complementary active infrared sensor does not detect). This objective should also be part of the other sensor's performance test plan.

- Optical alignment of an active infrared sensor is a common adjustment required of all models. A misaligned sensor will cause an increased number of nuisance alarms. If nuisance alarms are excessive, inspect for evidence of animals or debris, and check the alignment signal level if it is available on the specific model. In addition, inspect the optics for dirt or damage. If the alarms occur at certain times of the day and if dew or frost might be the cause, check that the heater is operational.

  If no cause for the increased nuisance alarms can be identified, perform an optical alignment. After alignment, slowly obscure each beam, and identify the one that requires less blockage than the others before alarming. This will indicate that either the transmitter or the receiver module is defective, especially if the beam has already been aligned.

2.2.4.6.3 Operability Testing

Operability tests are simply "walk tests." The testing individual walks through the detection zone of the active infrared sensor and verifies that the alarm arrived at the alarm display center. Incorporating this testing with an inspection of the perimeter security system is recommended. This inspection should note the status of the perimeter fence and other physical barriers and all physical security equipment nearby. The inspection should look for evidence that any component has been tampered with or damaged. Appropriate actions for repair should be taken if necessary, and indications of tampering should be reported, investigated, and documented.

2.2.4.7 Maintenance

Active infrared sensors should be maintained in accordance with the manufacturer's recommendations. Routine maintenance should involve a physical inspection of the sensor and the cleared area where the sensor is mounted. Maintenance includes periodic cleaning of the sensor's optics. The physical inspections can be combined with the scheduled testing of the sensor; however, an increase in nuisance alarms indicates the need for physical inspections. Increased nuisance alarms should be investigated as soon as noted.

Routine inspections should include the following:

- Inspect for any weed growth, and sterilize the soil or remove any growth near the sensor.
- Inspect for and remove any debris that could cause nuisance alarms.
- Inspect the lens or lens covers for any dirt or debris, including insects or spider webs, and clean them as needed.
- Inspect all mechanical parts for any sign of damage or tampering.
- Look for any areas of erosion or damage to the hard surface under the lower beam (if used) that could eventually increase the gap beneath the active lower beam of the infrared sensor.

A performance test should follow any major replacement of the electronics or adjustment of the sensor. All maintenance actions should be recorded.

2.2.5 Taut Wire Sensors

2.2.5.1 Principles of Operation

An installation of taut wire sensors consists of multiple strands of twisted wires strung between dedicated posts, known as a freestanding installation (refer to Figure 26), or attached to an existing fence (refer to Figure 27; note the application of taut wire to the outriggers in this test application). The twisted wires are generally made of a high-tensile strength barbed wire (not a farm-grade barbed wire). These wires function as a spring over a wide temperature range. A switch or sensor is attached to each wire and located in the middle of the wire spanned between two anchor posts. The distance between anchor posts can be up to 100 meters (328 feet) depending on the type of sensor and the sensitivity required. The number of wires and their spacing are critical to the effectiveness of this type of sensor.

Figure 26 A freestanding taut wire installation for environmental testing

Figure 27 A taut wire sensor system installed on an existing fence

Taut wire sensors will register a detection and alarm when one or more sensors detect a deflection of the wire(s) in a horizontal direction. This horizontal deflection is caused either by a certain amount of pressure applied somewhere along a wire's length (refer to Figure 28; note the deflection of the switch (sensor)) or by a wire being cut or broken.

Within the categories of intrusion detection sensors, a taut wire system is a terrain-following, point-of-detection, visible sensor.

Figure 28 Taut wire push test

2.2.5.2 Types of Taut Wire Systems

The major difference between the various taut wire systems is the type of sensor/switch that is used to detect a deflection in a wire. The two most common switches on the market today are mechanical and electromechanical. The mechanical switch is a device that enables the manipulation of the threshold of detection only through the adjustment of tension on the individual wires. The electromechanical switch can control the threshold of detection through the use of software that adjusts the detection threshold for each wire's tension, which allows for easier adjustments for greater ease of implementation and use. Types of taut wire electromechanical switches available on the market include strain gauge, piezoelectric, fiber optics, and resistive rubber.

2.2.5.3 Sources of Nuisance Alarms

The primary advantage of a taut wire sensor system is that, if the system is correctly installed and maintained, there are few sources of nuisance alarms. This statement should not be interpreted to mean that taut wire is an ideal sensor for most applications (refer to Section 2.2.5.4).

One possible source of nuisance alarms, though fairly rare, is a serious ice storm. A heavy buildup of ice on the wires can physically damage the system.

In some areas of the country, facilities experience a wide variety of temperature fluctuations from -20 degrees Fahrenheit (F) to 100 degrees F over the course of a year. This large temperature fluctuation can change the tension of the wire, causing sensitivity concerns and possibly requiring additional maintenance because of the stretching and shrinking of the wire. A

facility in this type of location may need to readjust or retension the wires on a seasonal basis to provide a uniform P_D.

A highly corrosive environment (e.g., an environment near the ocean) can cause increased maintenance and reliability concerns if the taut wire system is not stainless steel or aluminum. In addition, during high winds, a large piece of heavy debris (e.g., heavy cardboard, a sheet of plywood) striking the wires could cause a nuisance alarm (refer to Figure 29).

Figure 29 Examples of sources of nuisance alarms for taut wire fencing

2.2.5.4 Characteristics and Applications

Taut wire fence sensors have the following characteristics:

- They have a very low nuisance alarm rate; small animals (e.g., rabbits, rodents) and weed vegetation do not typically cause alarms.
- They follow the terrain (to a degree).
- They are not affected by most weather conditions (except for heavy ice buildup).
- They work effectively during fog conditions.
- They can be installed on the outside of the inner perimeter fence to validate an alarm condition in conjunction with a different sensor type.
- They can be installed along outriggers of a fence.

- They can be installed along the edge of roofs as both a barrier and a sensor.
- They can be applied in highly corrosive environments if all components are manufactured with stainless steel and aluminum.
- They can be mounted on an existing chain-link fence with minor modifications.
- They can be combined with fence disturbance sensors as an outrigger system used to detect climbing intrusions while the fence disturbance sensors detect cutting intrusion attempts (less expensive than a full taut wire sensor installation).
- Optimal performance is achieved when the taut wire sensors serve as part of a multisensor PIDAS.
- Depending on the sensor and the intermediate and anchor post configuration, an intruder could bridge a taut wire system using a ladder without causing a detection.
- Although difficult, clamping and cutting the wires or slowly separating the wire to create a passable opening could allow an intruder access without detection.
- If noncorrosive components are not used, wires and components could corrode in a highly corrosive environment; such a condition could affect the friction between wires and their mountings, thereby decreasing the sensitivity of the system.
- Tunneling or digging under the taut wire may be a concern if an adequate concrete curb or a sensor designed to detect a crawling intruder (i.e., a ported coaxial sensor) is not installed beneath the lowest wire.
- If anchor or sensor posts, or both, are poorly installed, slight movements of the posts can cause a significant nuisance.
- A taut wire sensor system should not be the only sensor system in a PIDAS.
- A taut wire sensor can be installed on gates, but this type of installation is challenging. The use of another technology (e.g., an active infrared sensor) is much preferred.
- As with most sensors, a taut wire sensor system should not be installed on the outside of the outermost PIDAS fence because it could be easily bridged.
- A taut wire system should not be installed on the inside of a PIDAS fence because an intruder could climb the outside of the fence and then jump down without detection.

2.2.5.5 Installation Criteria

Manufacturer's specifications should be followed for installation. A taut wire system may be installed as a freestanding system (i.e., the wires are mounted on their own dedicated posts), or the system may be attached to an existing sturdy fence. For a freestanding system, it is critical that the outermost anchor posts for each taut wire system be installed with sufficient bracing to withstand the tension created by the wires. The bracing should not enable an adversary attempting to climb the post to bypass the IDS.

The wires of the taut wire system are securely attached to each anchor post in various ways, depending on the manufacturer's specifications. For short sectors, springs are usually incorporated at the anchor post to provide enough movement at the sensor to enable an alarm.

A sensor post is installed at the midpoint of the sector length, usually at 50 or 100 meters (164 or 328 feet), depending on the system manufacturer. Sensors/switches will be mounted along this pole, and the wires are attached to these switches.

Additional posts, referred to as intermediate posts**,** are installed about every 3 meters (approximately 9.8 feet) between each anchor post and the sensor post. A slider coil the length of the post is installed at these locations to provide a support to the sense wires and to maintain the spacing for the wires. The installer slides a fixing bar down between the post and the slider coil, which allows the wires to remain in position but still move freely.

The anchor post will generally be a sturdier post than the sensor and intermediate posts in the system.

If barbed wire is used, the installer should be certain that a barb from the barbed wire does not catch on any of the coils; the wire must remain "free" between the anchor post and the sensor post. One or more individual barbs from the barbed wire may need to be removed to prevent excessive friction.

Depending on the threat facing the facility, concrete curbing may be installed beneath the bottommost wire to discourage intruders from digging under the taut wire fence.

Typical installation guidelines require approximately 45 kilograms (100 pounds) of tension on each wire. A typical taut wire system will alarm when 11 kilograms (25 pounds) or more of pressure is exerted on at least one wire. This pressure can result from a person pulling on a wire in any direction; a wire being climbed on; or a wire being cut, which releases the tension on one side of the sensor.

A taut wire system follows the terrain only to a certain degree. Over the length of a taut wire unit, the change in the elevation of the wire between all posts can be no more than a total of 15 degrees, with the wire always remaining parallel to the ground. This includes vertical and horizontal changes. If the angles change beyond the 15 degrees, the friction between the wires and the coils holding them becomes so great that the wires cannot move freely enough to detect an alarm condition.

2.2.5.6 Testing

Taut wire sensors or systems, or both, should be tested in accordance with the manufacturer's specifications.

2.2.5.6.1 Acceptance Testing

Acceptance testing is the process that a site must go through after an installer has completed the installation of a taut wire sensor system but before the system is accepted and used operationally.

Acceptance testing for a taut wire system consists of the following parts:

- Physical Inspection. The newly installed system should be thoroughly inspected to ensure that it has been installed in accordance with the manufacturer's specifications and the detailed engineering drawings for the site-specific design/installation of the taut wire system. A facilities engineer must ascertain that the installer implemented commonly accepted practices that resolve the following questions:

  – Was the system wired correctly?
  – Are poles installed at 90 degrees?
  – Are wires parallel with the ground and each other?
  – Are voltages correct?

- Performance Test. A complete and positive performance test of the newly installed system should be conducted.

2.2.5.6.2 Performance Testing

Performance tests for a taut wire system should be performed on the wires on each side of a sensor because the lowest sensitivity of the system will be located at the furthest point away from the sensor post. Testing should be concentrated at or near the anchor post. Other tests can and should be performed at other locations along the wires to verify uniform sensitivity. However, testing of the wires should not be done within approximately 10 feet of the sensor because it could damage the sensor.

Two types of tests can be performed on the sensor without damaging the system. Each of these methods tests whether the deflection of the wires from a person either climbing the wires or placing a ladder against the wires will cause an alarm. The sense wires should not actually be cut.

The ladder test involves an individual placing a ladder against the wires and climbing the ladder to a point where sensor activation occurs. The alarm should generally occur before the knees of the tester are near the top of the fence, but the test should be terminated as soon as an alarm is received to prevent damage to the sensors. To facilitate this, a local alarm should annunciate during testing.

To test the individual wire deflection, the tester can use a yardstick to measure the distance that each wire can be moved before an alarm occurs. To facilitate this, the yardstick should be hung from above the wire being tested (refer to Figure 30). The distance that any single wire should be able to be deflected before receiving an alarm is based on site-specific requirements; however, a deflection of no more than 7 to 10 centimeters (3 to 4 inches) should be tolerated.

Figure 30 Measuring deflection on a taut wire sensor

For taut wire systems using electromechanical devices for monitoring the wires, any software setting or sensitivity parameters that are adjustable in the processors should be measured or verified and documented. In addition, any processor box located at the fence should have a tamper switch that is tested as part of the semiannual performance test.

Deflection results should be documented to allow the monitoring of system changes or degradation over time.

During periods of extreme cold weather, mechanical sensor switches may take some time to return to the normal neutral position after activation. Multiple tests of the same zone should consider this time issue.

2.2.5.6.3 Operability Testing

The standard operability test for this system consists of pulling up or down on one of the wires of a particular sector until an alarm is received at the alarm monitoring station.

Because of the number of sensors (i.e., wires) that make up the taut wire system, some method should be used to ensure that a different wire is tested each time. This ensures that, over time, all of the wires and sensors will be tested for operability.

2.2.5.7 Maintenance

Maintenance of the taut wire system is essential for consistent performance. During the weekly operability testing of the system, the tester should be observant of any abnormalities that may exist. At a minimum, the inspection should do the following:

- Remove any foreign objects that may have blown into or otherwise become lodged on the wires.
- Remove any vegetation growing onto the wires.
- Inspect the ground beneath the system for signs of erosion or digging by animals.
- Inspect the condition of the slider coils, and ensure that the fixing bar is in place and is secure.
- Ensure that the wires are not jammed or snagged at the slider coils or sensor post and that no barbs are within 5 to 7 centimeters (2 to 3 inches) of the slider coils.
- Inspect the condition of the sensors to ensure that components are not cracked or damaged and that the wires are securely attached.
- Inspect wires for condition, spacing, and tautness.
- Perform any other inspections or maintenance specified by the manufacturer.
- At least once per year or whenever physical inspection warrants, verify the tautness of the wires using a dynamometer to ensure that tension is within manufacturer's specifications.

2.2.6 Fence Disturbance Sensors

2.2.6.1 Principles of Operation

A fence disturbance sensor is designed to be mounted on a chain-link fence to detect disturbances of the fence (e.g., the noises or motions generated when an intruder attempts to climb over or cut through the fence fabric). Figure 31 illustrates the deflection caused by an intruder climbing on chain-link fence fabric.

Figure 31 Deflection caused by an intruder climbing on chain-link fence fabric

A climber generates two types of disturbance while climbing the chain-link fabric: (1) a slow, low-frequency motion of the fabric movement and (2) a higher frequency impulsive shock or noise caused by pieces of the fence striking or rubbing against each other. Cutting the fence fabric also generates an impulsive shock. Some types of fence disturbance sensors have dual processors so that they can distinguish between the slow, low-frequency motion of the fabric and the high-frequency shock noises.

When a significant disturbance to a fence occurs, a switch will activate or a signal will cross a threshold, thus causing an event.

To generate an alarm condition, most fence disturbance sensors require a specified minimum number of events to occur within a specified time. For example, a facility could specify that an event must be detected five times within half a minute before an alarm is generated. The threat, the goals of the physical protection program, and the physical characteristics of the fence (i.e., height and wire mesh size) should drive the selection of these parameters. A lower number of required events would increase the P_D but would also increase the nuisance alarm rate. Requiring a higher number of events to generate an alarm would cause the opposite (i.e., a lower P_D but improved (lower) nuisance alarm rate).

The actual number of events over a specific period of time required to generate an alarm at a particular facility is generally considered sensitive information because knowledge of these parameters would give an adversary the advantage needed to possibly defeat that system.

2.2.6.2 Types of Fence Disturbance Sensors

2.2.6.2.1 Mechanical Fence Sensors

Mechanical fence sensors operate on the principle that fence movement will cause a switch to open or will close a set of contacts. One of two approaches is generally used. First, mercury switches are used to detect side-to-side movement or tilting of the fence, and signal processors use count and time criteria to differentiate between intrusions and nuisance indications. The second method uses a mass on a set of contacts. The system detects impulsive fence movements of sufficient magnitude to cause the mass to move off the contacts momentarily. Generally, this method also uses count and time criteria to generate an alarm indication. Such sensors are positioned on the fence at regular intervals.

2.2.6.2.2 Electromechanical Fence Sensors

Electromechanical fence sensors use individual point transducers to detect fence motion. The point transducers produce an analog signal instead of a switch closure and use an electronic signal processor to extract alarm information from the signal. Like mechanical fence sensors, these sensors are positioned on the fence at regular intervals. For high-security applications, the transducers are placed on every pole or on the fence fabric itself between each pair of poles.

Two types of electromechanical transducers are used: (1) geophone and (2) piezoelectric transducers. The sections below describe the principles of operation for each type.

Geophone Transducers

A geophone transducer uses the principle of a conducting loop moving in a fixed magnetic field to generate a voltage. Either the coil or the magnets are mounted on a spring structure so that, when the body of the geophone moves, relative motion is established between the coils and the magnets, thus causing a voltage output.

Because geophones are sensitive to movement along one axis only, they are mounted on the fence in an orientation that enables them to be sensitive to the vertical movements of the fence. This orientation helps to eliminate nuisance alarms caused by wind-induced fence movements.

Piezoelectric Transducers

Piezoelectric transducers detect fence motion by using crystals that exhibit the piezoelectric effect. When the crystal is deformed, a voltage appears across the crystal. The crystals are mounted in a housing in an orientation that enables the detection of fence motions. The transducers are sensitive along a major axis and are generally mounted in an orientation that enables them to be most sensitive to vertical fence motion.

2.2.6.2.3 Strain-Sensitive Cable

A strain-sensitive cable is a transducer that is uniformly sensitive along its entire length. It is specially designed to produce an output voltage when the cable is moved. An electric cable uses a polarized dielectric to become microphonic. Another cable type uses special construction to enhance voltage output caused by the triboelectric effect. The triboelectric effect is an electrical phenomenon in which certain materials become electrically charged by friction

after being rubbed together. A third cable type resembles a distributed geophone with magnetic material surrounding sense wires in one cable. Each cable type is fastened directly to the fence using wire ties to directly couple movement of the fence fabric to the transducer cable (refer to Figure 32).

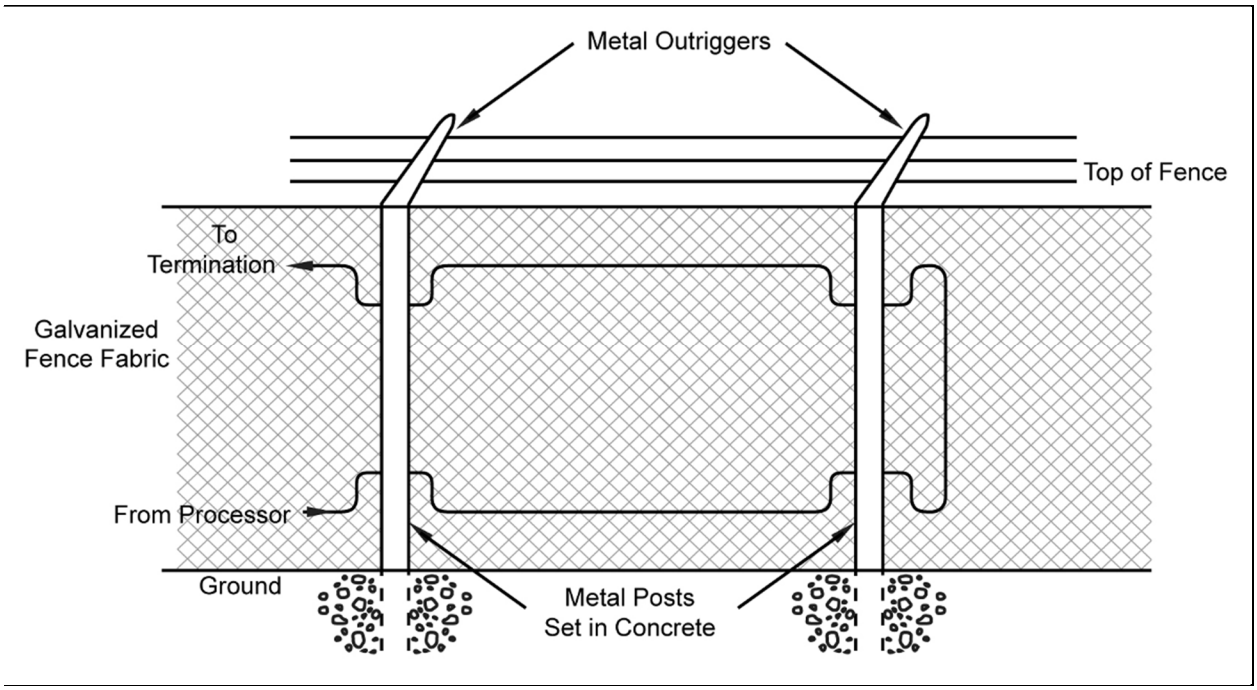


Figure 32 Typical installation of strain-sensitive cable

2.2.6.2.4 Fiber-Optic Cable

Fiber optics is a class of optical technology that uses strands of optically pure glass as thin as a human hair to carry digital information over long distances. A light source, such as a light-emitting diode (LED) or laser diode, is coupled to one end of the fiber, and a receiver (such as a photo transistor or similar device) is coupled to the other end of the fiber. The two major categories of fiber-optic sensors are continuity sensors and microbending sensors. The major advantages of fiber-optic cable include immunity to radio and electromagnetic interference and durability in conditions of changing temperature and humidity.

Because the fiber does not have to be straight to reflect the light from one end to the other, it can be installed in various configurations on a fence or can be buried in the ground to sense a disturbance. The light diffraction (speckle) pattern and the light intensity at the end of the fiber are a function of the shape of the fiber over its entire length. Motion, vibration, or pressure of the fiber induces modal differences causing a phase shift in the light. Sophisticated processors can detect these phase shifts or minute changes in the light patterns traveling down the cable. The processor can characterize these changes as those being produced by an intruder cutting or climbing the fence. When the right criteria are met as set in the parameters of the processor, an alarm will be generated.

Some processors can allow long lengths (up to tens of kilometers) of nonsensing cable (single-mode fiber) to be placed between it and a length of sensing cable (multimode fiber).

This configuration allows the processor(s) to be located in a central location a long distance from the fence being protected.

2.2.6.3 Sources of Nuisance Alarms

The tension of the fence fabric and the general condition of the fence can affect both the performance and the number of nuisance alarms that will be experienced. Tight fence fabric enhances the transmission of noises along the fence and, therefore, makes the slight noises caused by a climbing or cutting intruder easier to distinguish. Loose fabric may allow the fabric to flap against the post or other fence parts causing increased noise and increased nuisance alarms.

Many factors can affect the rate of nuisance alarms for fence disturbance sensors, including rain, hail, melting ice, wind, wind-blown debris, lightning, and the physical condition of the fence on which they are mounted. The magnitude of the effects of each of these sources depends on the type of sensor, the installation method, sensor maintenance practices, and the adjusted sensitivity or other settings.

Some fence disturbance sensors cannot be used near an electrical high-power line. Radios may also affect the geophonic type of fence disturbance sensors. Immunity to these sources is one advantage of using fiber-optic technologies.

Because fiber-optic cable senses vibrations, nuisance alarm sources can be similar to those of seismic sensors. The sensor will likely detect anything that causes a noise or vibration in the fence structure or fabric. New digital processing algorithms incorporated into most processors have some capabilities to filter out extraneous noise such as that produced by wind or other vibrations. As with other fence disturbance sensors, the general condition of the fence is very important for the proper performance of this technology.

2.2.6.4 Characteristics and Applications

Fence disturbance sensors have the following characteristics and applications:

- Some cable types give the location along the fence disturbance sensor where the detection occurred; this characteristic allows for a quicker and more accurate assessment of an alarm.

- Most fence disturbance sensors are relatively inexpensive to purchase and install, particularly because most facilities already have some sort of fence installed as a boundary marker.

- A fence disturbance sensor can be applied with excellent reliability to protect an asset located indoors. One example is a sensor applied to a cage that is built around the asset.

- An adversary who climbs or cuts a fence very slowly may be able to spoof a fence disturbance sensor; however, this can be much harder than it sounds. This scenario may be more likely if the adversary knows the event count and time constraints for alarm generation.

- A typical standalone fence disturbance sensor installation can be bridged over or trenched under.

- A fence disturbance sensor should not be used on the outer fence or as a facility's only line of detection.

- Typical rigid conduit installed on the fence will expand and contract with temperature change, which can cause nuisance alarms.

- Fence disturbance sensors (except for fiber-optic technologies) should not be used near a high-power line. Radios may also affect the geophonic type of fence disturbance sensors. Careful testing and evaluation should be conducted at the site before installation of the sensors to determine the frequencies and wattages that may be problematic.

2.2.6.5 Installation Criteria

Installing a fence disturbance sensor on an existing chain-link fence is possible; however, generally too much "noise" occurs if the fence was not installed with the original goal of supporting such a sensor. In this case, many adjustments will be required over time to achieve acceptable sensor performance. The following guidelines are suggested for preparing and evaluating an existing security fence for compatibility with fence-mounted intrusion detection sensors designed to sense motion, displacement, or acceleration forces, or a combination of these, resulting from an intrusion attempt:

- The fabric of the fence should be located on the unprotected side of the posts.

- The fence fabric should be stretched to allow not more than 6.3 centimeters (2.5 inches) of deflection when a 13-kilogram (30-pound) perpendicular load is applied at the center of the panel.

- The fence posts should not deflect more than 1.9 centimeters (0.75 inch) when a 22-kilogram (50-pound) perpendicular load is applied at a height of 1.5 meters (5 feet) above the base of the post.

- The fence fabric should not be embedded in a concrete or otherwise solid sill to preclude later tightening of the fabric, if necessary.

- The fence should not have a top rail. Top rails reduce sensor performance while aiding the climbing adversary. However, the fence should have a bottom rail.

- The fence should not have outriggers that tend to be noisy and cause unwanted nuisance alarms.

- Tension wires should be used to provide for the stabilization of the fence fabric.

- The top of the fence posts should be approximately 10 centimeters (4 inches) below the top of the fabric to prevent an adversary from using the post as a bridging aid or from leaning a ladder against it.

- Wire ties should be used to secure the fence fabric to the structural members of the fence (i.e., posts, braces, or tension wires). The wire ties should be 9-gauge or thicker zinc-coated steel (refer to Figure 33).

- The fence fabric should be secured with wire ties approximately every 30 centimeters (12 inches).

- The wire ties should form a 540-degree tightened loop that is secure enough to prevent movement between the fence fabric and the wire tie.

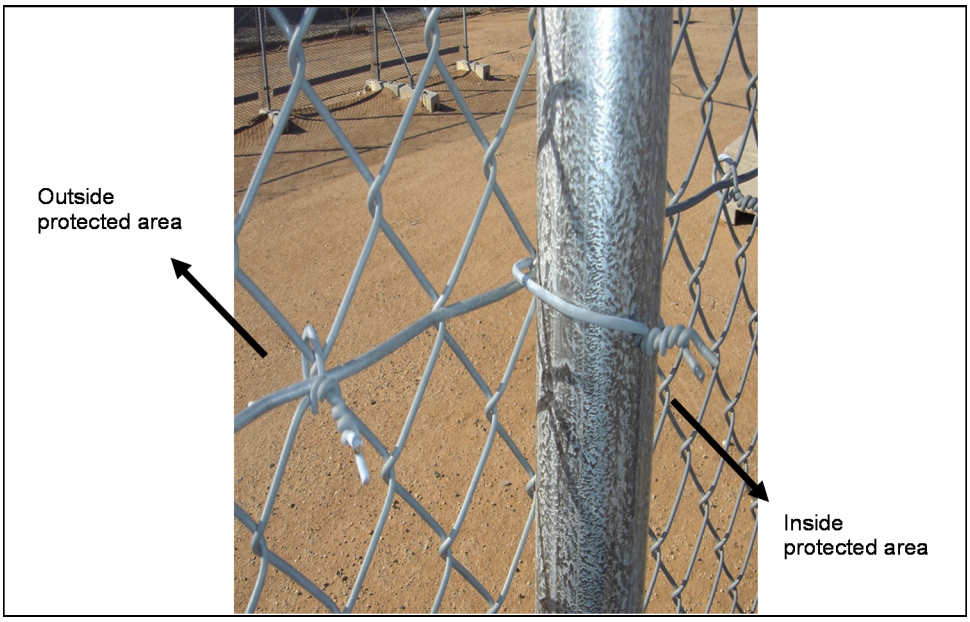


Figure 33 Example of security fence wire ties

Some fence disturbance sensors can accept input from an anemometer (windspeed indicator) so that the processing of events can be changed when windspeed exceeds a certain value. Care should be taken when using this type of system because it can automatically increase the attenuation of the sensitivity of the system as the wind increases. The wind can increase to a point at which the sensor is no longer providing intrusion detection, without the operator's knowledge. Preferably, the operator should access the sensor if the nuisance alarms increase to an intolerable level and implement compensatory measures as necessary.

Certain fence disturbance sensors will allow the sensitivity of each meter of the cable to be adjusted independently along the length of the cable to compensate for variations in the fence, such as corners, tension posts, and gates. This flexibility also allows the user to define zones in the software of the processor, potentially reducing the number of processors necessary.

Signs should not be mounted on a fence that supports a fence disturbance sensor. During windy conditions, the sign is likely to be a source of noise or to provide a larger surface and thereby increase the fence movement and noise, consequently increasing the number of nuisance alarms. If a sign must be mounted on a fence supporting a fence disturbance sensor, it should be attached with twisted metallic wire ties to secure the sign and prevent it from rattling.

If chains are used anywhere along a fence that supports a fence disturbance sensor (e.g., to secure a gate), the chain should be rubber coated and as short as possible.

2.2.6.6 Testing

Fence disturbance sensors or systems, or both, should be tested in accordance with the manufacturer's specifications. Three types of testing must be performed during the life of a fence disturbance sensor: (1) acceptance testing, (2) performance testing, and (3) operability testing.

2.2.6.6.1 Acceptance Testing

When first installed, a fence disturbance system/sensor should be tested before it is formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the sensor it and should do the following:
  - Verify that the installation matches the installation drawings, which should follow the manufacturer's guidance.
  - Verify sector intersection spacing.
  - Verify that signal and power wires are routed in conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
- A performance test establishes and documents the level of performance.

2.2.6.6.2 Performance Testing

Performance tests should be designed to verify the level of performance of the fence disturbance sensor through its range of intended function. Fence disturbance sensors are designed to detect an adversary attempting to climb over or cut through the fence.

A performance test should be conducted when the following apply:

- A processor is replaced.
- Sensor cables are replaced or repaired.
- An adjustment that can affect sensitivity is made to the processor parameters.
- The configuration of the installed sensor cables is changed.
- A change has been made to the sensor or near the sensor that might affect the detection sensitivity.

This test should include a visual inspection of the fence disturbance sensor and of the general area where the sensor is installed. The testers should refer to Section 2.2.6.7 (maintenance) and perform the required routine maintenance.

All relevant processor readings and parameter settings that can affect the detection capabilities or the nuisance alarm rate should be recorded. Each manufacturer will have different sensor settings. The test should involve a comparison of the current readings to the last recorded readings to ensure that they fall within the manufacturer's specifications.

To test the detection capabilities against a climber, the tester will physically climb the fence fabric. To preserve the integrity of the fence fabric, test devices are available that provide a consistent, simulated fence-cut disturbance without damaging the fence fabric (refer to Figure 34).

Figure 34 Use of a fence-cut simulation tool

Sufficient testing should be performed to provide the probability of sensing (P_S) at the confidence level defined for the facility. For example, a "30/30" test methodology and binomial distribution may be used to yield a 90-percent P_S performance at a 95-percent confidence level. Using this methodology, if the sensor alarms 30 times when subjected to 30 attempted intrusions, the P_S value is equal to 0.90 at a 95-percent confidence level based on the values derived from a binomial reliability table.

Performance testing of fence disturbance sensors should include the procedures described below. Performance tests should be conducted at 30 equidistant points along the length of the detection zone/sector. One or more test trials should be performed for each of the 30 test locations. Particular attention should be directed to locations where sensitivity might vary if the installation configuration varies from the norm, such as at corners or sector overlaps or where fence structure is more significant.

Procedure 1: Conduct Climb Tests

Conduct 30 climb tests within the detection zone/sector to verify that P_S = 0.90 at a 95-percent confidence level.

Each sector should be tested 30 times at points equidistant along the length of the sector. For this procedure, the adversary test subject should attempt to climb the fabric from the outer (unprotected) side of the fence (refer to Figure 35). If the test requires climbing the fence from the inner side, do not use the fence support posts to aid in climbing. A failure is recorded if the adversary test subject can reach the top of the fence and start to go over it without generating an alarm.

Figure 35 Test climbing the fence from the outer (unprotected) side

Procedure 2: Conduct Simulated Fence-Cut Tests

Using the simulated cut device, conduct 30 simulated cut tests within the zone of detection/sector to verify that P_S = 0.90 at a 95-percent confidence level.

Each sector should be tested 30 times at points equidistant along the length of the sector. For each trial, use the cut simulation tool to strike the fence (releasing the plunger from the middle notch) X[1] times at a point either 30 centimeters (12 inches) from the ground or 30 centimeters (12 inches) from the top of the fence or at a point in the middle of the fence fabric. Ensure that the test device is firmly pressed against the fabric when releasing the plunger. The strikes should be at approximately X-second intervals. A failure should be recorded if the tester can strike the fence X times within the designated timeframe without generating an alarm.

---

[1] "X" is the number for the amount of time needed to strike the fence and the required time interval to generate an alarm, which is determined by the site and is usually classified.

Procedure 3: Verify Processor Enclosure Tamper Alarm

Test the tamper alarm of the processor enclosure by slowly opening the door to the enclosure. A failure should be recorded if an alarm is not received or if the cover can be opened more than 2.5 centimeters (1 inch) before an alarm is received.

Resettling Time

When following the performance test procedures, allow sufficient time for the system being tested to stabilize or reset between each individual test trial.

Verification of Failure To Alarm

If an alarm is not received for a given trial, two more attempts may be made at the same location using the same test method. The trial should be considered a valid detection, and testing can proceed *only* if both of the additional trials result in successful alarms. If either additional trial results in a failure, testing of the system should cease, and corrective action should be taken. Following required maintenance or recalibration, the complete performance test procedure should be conducted again using the same test methodology at all test locations (if possible) to verify acceptable sensor performance. If sensing performance does not meet requirements after all reasonable corrective actions have been attempted, the test should be annotated as a failure, and compensatory measures should be considered based on site-specific requirements.

2.2.6.6.3 Operability Testing

The operability test is conducted by causing a disturbance to the fence fabric within the zone of detection to be tested. The disturbance can be caused by striking the fence with some object or simply shaking the fence until an alarm is received at the alarm monitoring station. The force exerted to strike or shake the fence during the operability test is usually outlined in the manufacturer's specifications and is derived from a reasonable representation of the force that the fence disturbance system would encounter and should detect if a human were attempting to circumvent the system by climbing the fence or cutting it.

If no alarm is received, a maintenance request should be immediately generated and implementation of compensatory measures should be considered based on site-specific requirements.

2.2.6.7 Maintenance

At least twice a year and after any major storms, each section of a fence disturbance system should be carefully examined to make certain that no parts of the sensor system have become loose or that the integrity of the fence has not been compromised. The inspection should do the following:

- Ensure that wire ties for the sensor cable have not broken or become loose.
- Ensure that all fence fabric wire ties remain tight and are securely attached to the fence structure.
- Search for any debris that has collected against the fence and remove it.

- Inspect any signs that may be mounted on the fence fabric and ensure that they are securely fastened.

- Ensure that any splices or terminations in the sensor cable remain sealed and securely attached to the fence.

Tree branches, weeds, and other objects that could cause mechanical disturbance of the fence should be removed. Gates, barbed wire, and outriggers (when used) should be mechanically sound and, where appropriate, firmly attached to other parts of the fence. Such precautions prevent clatter or mechanical disturbances within the fence itself.

2.3 Interior Intrusion Detection Sensors

When interior intrusion detection sensors are integrated into a physical security system using administrative procedures, access controls, and material monitoring, they can be highly effective against insider threats. Interior intrusion detection sensors that are correctly placed, installed, maintained, and tested can generate an alarm caused by the unauthorized presence of intruders.

2.3.1 Balanced Magnetic Switch

2.3.1.1 Principles of Operation

The magnetic switch, the most ubiquitous security device, is used for both door and window protection (refer to Figure 36). It consists of a magnet installed on a door or window and a switch unit installed on the frame. When the door or window is in the closed position, the created circuit is closed. When the door or window is opened, the circuit is open and causes an alarm to be generated.

Figure 36 An example of the application of a magnetic switch for door protection

At a cost of approximately $10, the simple magnetic switch device is used in most residential and small business security systems. Unfortunately, little knowledge is required to defeat a simple magnetic switch. In response, the balanced magnetic switch (BMS) was developed more than 30 years ago and requires a great deal more skill to defeat than a simple magnetic switch.

A BMS is a passive, visible, point-detection sensor that uses a magnet in both the switch and magnet units (refer to Figure 37). 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 unit. The component containing the larger permanent magnet is mounted on the movable part of the door or window adjacent to the switch unit installed on the frame when the door or window is closed.

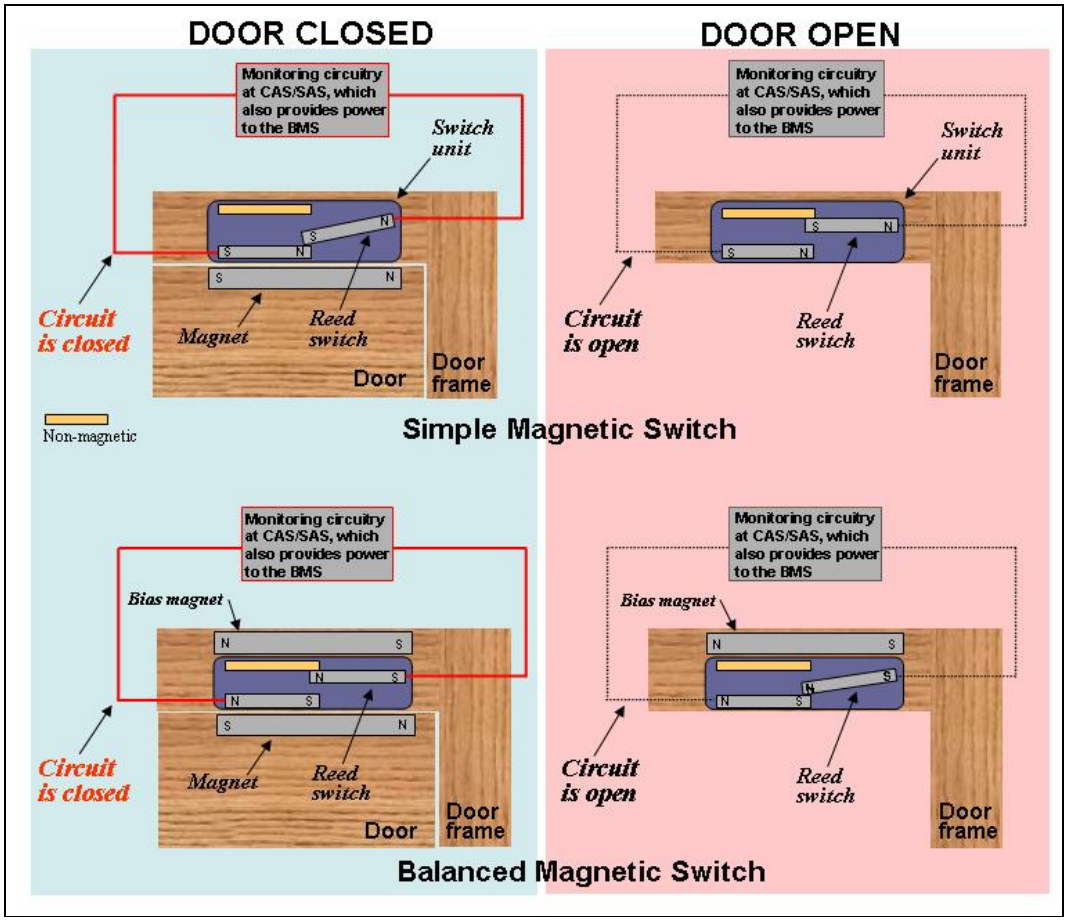


Figure 37 A schematic of a simple switch versus a BMS

With the door or window closed, the magnets are adjusted to create a magnetic loop, which causes the reed switch to experience a magnetic field of essentially zero. When the door or window is opened and the magnetic field is removed, the contacts will separate and generate an alarm indicating a security breach. In some models, this magnetic field is established by adjusting the bias magnet. In other models, the adjustment is made by varying the position of the magnetic unit with respect to the switch unit.

Any action that causes the magnetic field to become unbalanced (i.e., opening the door or window) transfers the reed switch to the "closed" position and generates an alarm. The same result is obtained if an external magnet is brought into the vicinity of the BMS, thus changing the magnetic field.

A newer BMS codes multiple magnets in each unit; thus, each BMS is matched, and the defeat of the BMS is nearly impossible. However, fixing a switch in a BMS that has a coded configuration requires the complete replacement of the BMS with another matched pair.

2.3.1.2 Types of Balanced Magnetic Switch Sensors

BMS sensors have a variety of designs. Some use multiple magnets, and some have internal electromagnets for self-testing. Manufacturers have reduced the vulnerability of magnetic switches to external magnetic fields through the following measures:

- using multiple magnets, various magnetic orientations, and magnetic shielding (e.g., Mumetal®)
- creating standoff distances
- adding magnetic tamper indicators

The newest switches on the market have very narrowly defined magnetic field paths, making them almost immune to external magnets. All provide a high level of protection for access points such as windows and doors. The type of BMS that a facility chooses should be based on the switches' ability to provide reliable functionality within the environment and the goals of the facility's physical protection program.

2.3.1.3 Sources of Nuisance Alarms

BMS sensors are very reliable when installed correctly on a properly installed door with hardware that is in good condition. A BMS alone almost never causes nuisance alarms. Most nuisance alarms generated by a BMS can be attributed to the poor condition of the door or its hardware. A worn latch or a latch that is out of adjustment resulting from excessive door movement or play are the most common causes of nuisance alarms. Excessively worn door hinges or an improperly installed BMS that causes misalignment of the switch and magnet unit can also cause nuisance alarms.

When a BMS is used on large rollup doors, a slight misalignment of the doors usually causes nuisance alarms. It is difficult over time to keep this type of door maintained in alignment for proper sensor operation. Extreme weather conditions that cause excessive movement of a door, window, or access portal can also increase the nuisance alarm rate of a BMS.

2.3.1.4 Characteristics and Applications

A BMS is passive and visible, and it detects boundary penetrations, such as a door or window being opened, through a magnetic switch. These switches are manufactured in different sizes and shapes and achieve different performance levels, depending on the manufacturer and the model.

A BMS represents a mature technology that is subject to few (if any) nuisance alarms as long as the door, doorframe, and door hardware are in good condition and the BMS was installed properly.

An externally introduced magnetic field can possibly defeat a BMS, but a BMS sensor with multiple magnets and reed switches will be much more difficult to defeat by this method. If a door magnet can be removed without detection, it may be possible to compromise the BMS. These sensors provide protection only if the intruder opens the door or window for entry. If the intruder cuts through the door, cuts through the wall next to the door, or breaks the window pane, the BMS will be bypassed. Licensees should consider bolstering the resistance to adversary penetration of these potential pathways.

High-voltage discharges from lightning, power surges, or stun guns can permanently weld reed switch magnetic contacts in a failed (closed) position, making the system useless when it is armed. If the metal contacts are welded shut, the system will indicate a secure state even when the system is breached.

2.3.1.5 Installation Criteria

The switch assembly of a balanced magnetic sensor is mounted on the inside of the fixed surface, and the magnetic assembly is mounted near the top of the movable surface near the edge that is on the opposite side of the hinge. This mounting allows for maximum detection of movement.

A BMS should always be installed on the secure side of the door. If the BMS is installed on a recessed door or outward opening door, a spacer will be needed to line up the switch and magnet units. If the doorframe is steel, a nonferrous spacer (such as aluminum or plexiglass) should be installed between the doorframe and the switch unit to prevent interference with switch operation. Likewise, if the magnet is installed directly on a steel door, it should have the same type of spacer. A spacer made from 1.2-centimeter-thick (0.5-inch-thick) plexiglass has worked well in many installations. Some manufacturers state that their switch compensates for the effects of steel. It is best to consult the manufacturer to verify the need for a spacer.

The wiring from the BMS should be protected. Installing the wiring in a conduit from the sensor switch enclosure all the way to the alarm data-gathering or multiplexer panel will protect the alarm wiring. Materials with high-magnetic permeability (e.g., Mumetal®) are preferable for the shielding; however, steel can also be used.

Sensor electronics enclosures should have tamper switches. Line supervision monitors the communication link between a sensor and the alarm control center. Supervised lines between the sensor and host alarm system and continuously monitored sensor tamper switches will help protect against adversary attacks on communication links and sensor electronics enclosures.

2.3.1.6 Testing

A regular program of testing sensors is imperative for maintaining optimal operating order. In addition, all testing should follow the manufacturer's recommendations.

2.3.1.6.1 Acceptance Testing

When first installed, a BMS sensor should be tested before it is formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the BMS sensor and should do the following:
  - Verify that the installation matches the installation drawings, which should follow the manufacturer's guidance.
  - Verify that signal and power wires are routed in the conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
- A performance test establishes and documents the level of performance.

2.3.1.6.2 Performance Testing

If a BMS has had an unexplained number of nuisance alarms or if the BMS has ever failed to generate an alarm during a daily walkthrough test, troubleshooting and repair will be required. After this repair, a formal performance test should be run. In addition, operation of the sensor tamper and communication to the alarm stations are verified during testing.

The following three basic tests constitute a performance test for a BMS:

- Evaluate the response of the switch when an externally introduced magnetic field is produced by a foreign magnet (refer to Figure 38; note that this procedure is much more difficult to accomplish than the photos would suggest).
- Establish that the BMS detects a door opening within a specified distance. A commonly used requirement is that a BMS should generate an alarm when the leading edge of the door has been moved 2.5 centimeters (1 inch) or more from the fully closed position.
- Establish that the BMS does not detect a door opening within a smaller specified distance. A commonly used requirement is that a BMS should not initiate an alarm for door movement of 1.2 centimeters (0.5 inch) or less. The importance of the condition of the door and its associated hardware cannot be overemphasized. An improperly installed and maintained door will degrade the effectiveness of the BMS.

The history of nuisance alarms and false alarms should be reviewed at this time as well. Establishing specific values for false alarm rates helps the operator determine when a sensor should be reported to maintenance personnel.

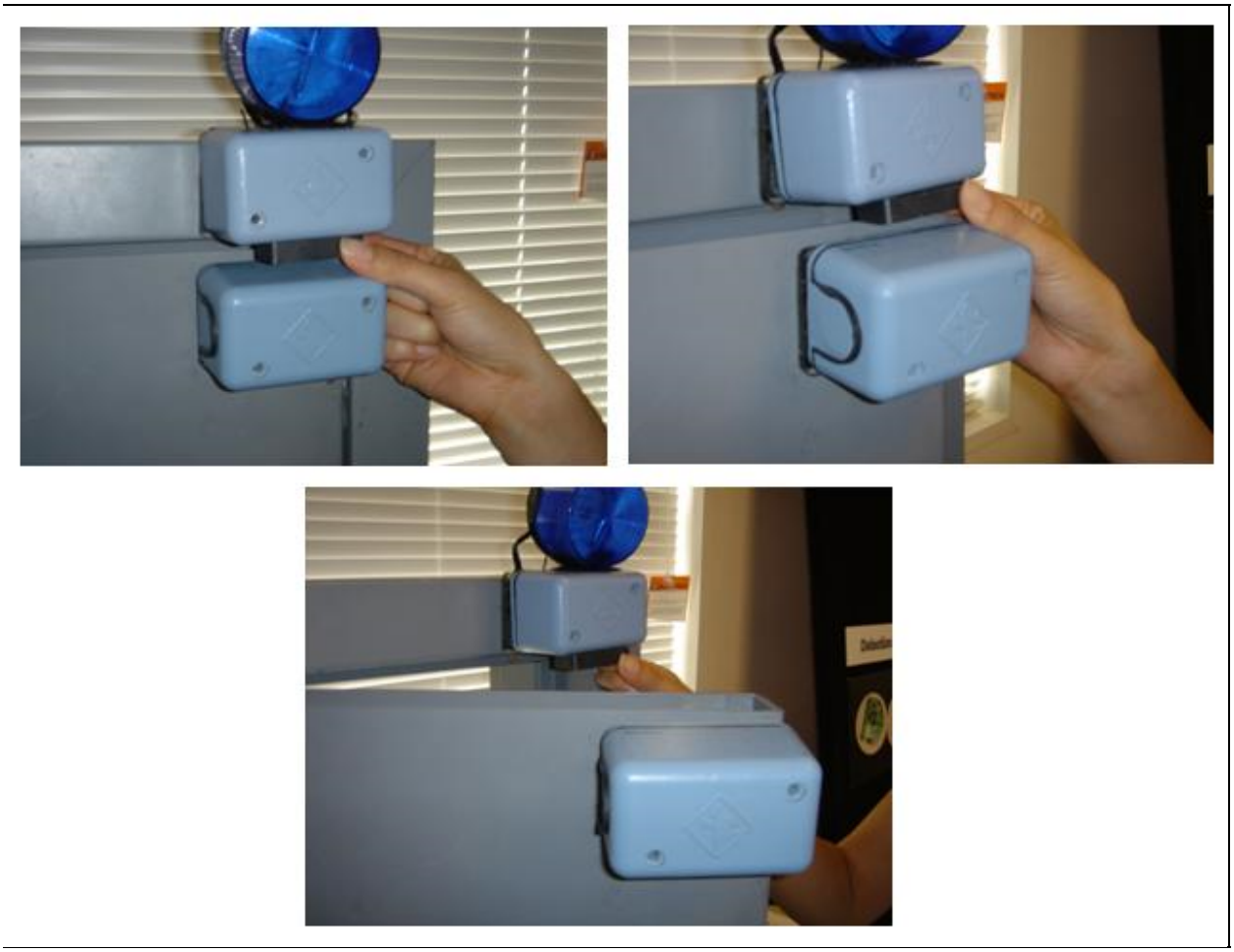


Figure 38 Demonstration of an external magnetic field being introduced to a BMS

2.3.1.6.3 Operability Testing

The objective of the operability test is to verify that the sensor is operational and that the correct alarm signal is received and displayed at the alarm stations.

The BMS operational test is simple and is performed by opening the door and verifying with the alarm station operator that an alarm was received at that particular door location. Another test is then conducted to verify with the operator that the sensor returns to the secure state and remains secure when the door is closed, latched, and pushed back and forth to account for some play in the latch. The door hardware should be in good condition. The door should open and close smoothly without rubbing or scraping on the doorframe. It should latch easily, and the amount of play in the latch should be minimal.

In addition to scheduled tests, operability testing should be performed when a protected location is placed into a secure condition from an unsecure condition (i.e., entrances have been locked, and alarms have been reactivated).

2.3.1.7 Maintenance

At a minimum, maintenance of a BMS should be performed every 6 months. The following actions should be done during maintenance:

- Verify tamper operation by accessing electronics enclosures and disconnecting communicating links of the sensors and through successful communication to the alarms stations.
- Verify tamper operation or initiation of an alarm by introducing a foreign magnetic field to the sensor.
- Verify that an alarm occurs within a specific door movement distance, which is typically before the leading edge of the door has moved 2.5 centimeters (1 inch).
- Verify that no alarms occur during any slight movement of the door when it is latched.
- Verify acceptable conditions of electrical power and communication lines.

2.3.2 Interior Microwave Sensors

2.3.2.1 Principles of Operation

Interior microwave sensors are active volumetric sensors and are typically monostatic, using a single antenna for both the transmit and receive functions; all components are enclosed in a single housing (refer to Figure 39). Microwave sensors emit an energy field.

Motion within an area protected by a microwave will cause changes to the microwave energy. These changes are a type of Doppler frequency shift. A person or other object moving within the microwave energy field will cause minute changes in the frequency of the microwave. Because the sensor “knows” the frequency at which it is transmitting, when it receives reflected energy at a slightly different frequency, it will process the difference between the frequencies. An alarm will be generated if the frequency difference exceeds a preset threshold.

Interior microwave sensors typically operate in the X band RF region (7 to 11 gigahertz) with low power output of approximately 5 to 10 milliwatts. The size and shape of this pattern can vary significantly depending on the characteristics and configuration of the microwave antenna used in the sensor design, although most interior monostatic microwave sensors have a detection pattern that ranges from approximately 9 meters (approximately 29.5 feet) up to 30 meters (approximately 98.4 feet) in length. The shape of the detection zone is governed by the design of the antenna and is roughly similar to an elongated balloon or a cigar (refer to Figure 40; the half and full envelopes indicate half-power and full-power settings). The antenna is usually a microwave horn but may be a printed circuit planar or phased-array antenna.

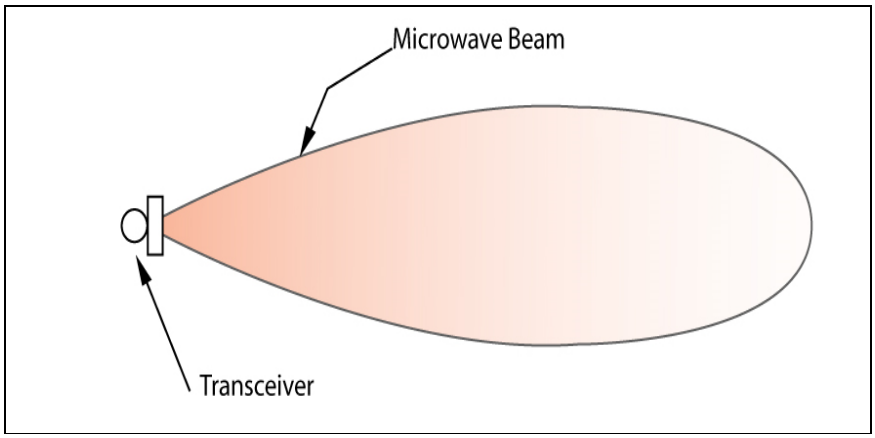


Figure 39 A common interior microwave antenna propagation pattern

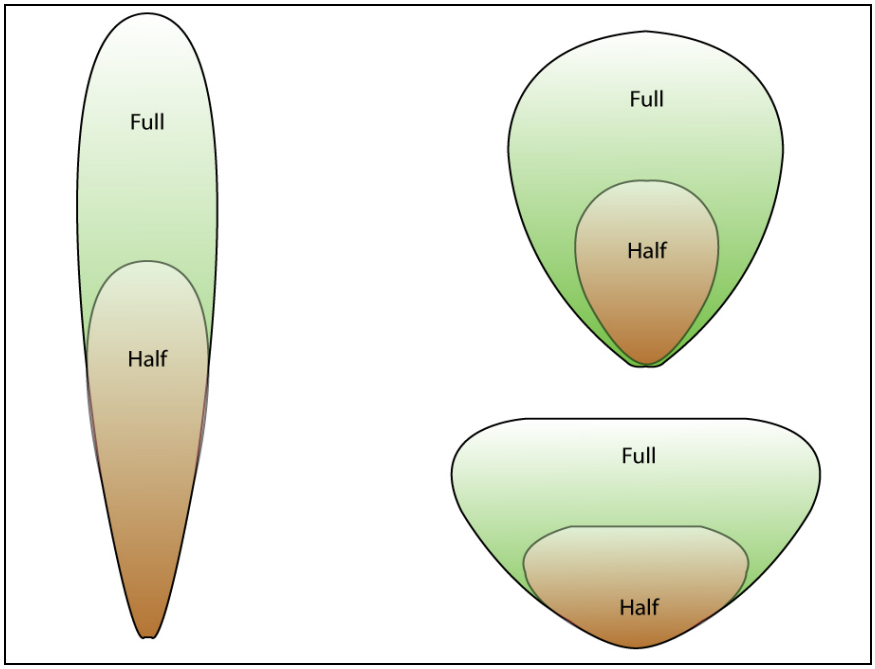


Figure 40 Examples of different microwave antenna propagation patterns

Optimal detection for interior microwave sensors is achieved when the target is moving toward or away from the sensor, not across the zone of detection. Therefore, interior microwave sensors should be oriented to force an adversary to move toward or away from the sensor to accomplish his or her objective.

2.3.2.2 Types of Interior Microwave Sensors

The two basic types of interior microwave sensors are monostatic sensors, which have the transmitter and receiver encased within a single housing unit, and bistatic sensors, in which the transmitter and receiver are two separate units creating a detection zone between them. A bistatic system can cover a larger area and would typically be used if more than one sensor is required, but such a system is more commonly used in exterior applications.

2.3.2.3 Sources of Nuisance Alarms

Because of the high frequencies of interior microwave sensors, the signal/sensor is not affected by moving air, changes in temperature, or humidity. However, the high frequency allows the signal to pass through standard walls, glass, sheetrock, and wood, which can cause nuisance alarms to be generated by movement adjacent to, but outside, the detection area. If an interior microwave sensor is installed in a room made from light construction materials and if the detection area of that microwave is larger than the room, movement outside the room will generate a nuisance alarm. The structural materials and the thickness that a particular microwave can penetrate will vary based on the manufacturer, model, and frequency (refer to Figure 41).

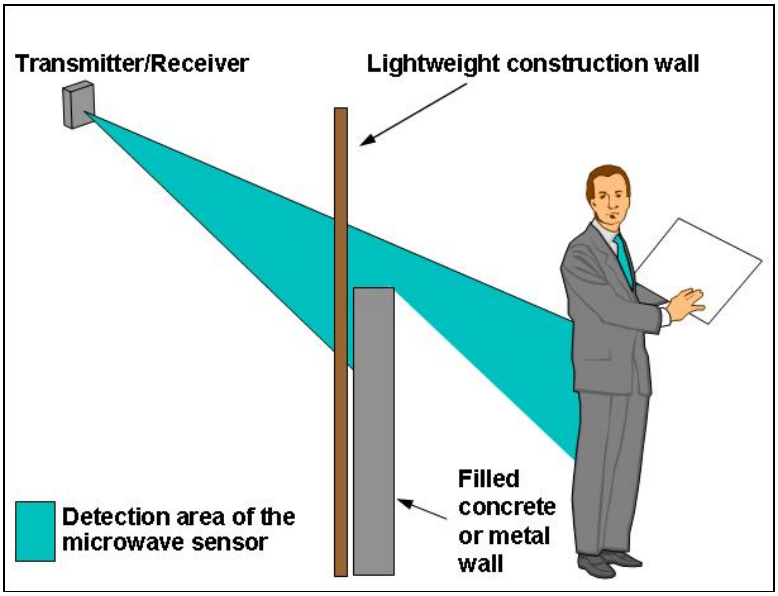


Figure 41 A microwave sensor triggering a nuisance alarm

Fans, animals, or equipment can generate nuisance alarms. A fan that is not located in the room of primary detection is also a possible source. If a fan is located within a ventilation duct, microwave energy traveling through the duct can detect reflections from the moving fan blades. Another source of nuisance alarms for microwaves is plastic drainpipes located behind dry wall. Water draining through the pipes can cause alarms.

Some interior microwave sensors can be triggered by fluorescent lights. The gas within fluorescent lights is a reflector of microwave energy when it is ionized. The light flickers at the power line frequency, which the sensor perceives as motion. If nearby microwave sensors generate nuisance alarms, a metallic screen mesh (also known as a Faraday cage) can be installed over the lights to prevent the microwave energy from passing through.

Electromagnetic sources close to the microwave frequency are another possible source of nuisance alarms. In fact, if more than one microwave sensor is installed in the same area, the sensors can potentially interfere with each other. Fortunately, interior microwave sensors that allow the user to select from several different frequencies are available. More than one microwave in the same area will require different frequencies.

Finally, signals reflected off metal objects (e.g., filing cabinets, trash cans, and electrical boxes) can "extend" sensor coverage to areas not intended to be covered and can create the potential for nuisance alarms.

2.3.2.4 Characteristics and Applications

Interior microwave sensors are most sensitive and effective when they are installed such that an adversary would walk toward or away from the sensor.

Interior microwave sensors can be used to effectively monitor interior confined spaces such as vaults, special storage areas, hallways, and service passageways. They can also serve as an early warning alert of intruders approaching a door or wall. In situations that require a well-defined area of coverage, the use of monostatic microwave sensors is appropriate.

To further enhance detection, a facility can install a complementary sensor, such as a passive infrared (PIR) sensor. A PIR sensor is considered to be complementary to a microwave sensor because it senses best when an adversary moves across the zone of detection, unlike the microwave. The use of a complementary system provides a second line of defense and gives security personnel additional information to help them accurately assess an alarm and discriminate actual or potential penetrations from nuisance events.

Interior microwave sensors are least sensitive if they are installed such that an adversary would be able to limit their movements to paths across the detection pattern.

The special properties of microwave beams allow them to penetrate most types of surfaces (but not metal). For this reason, it is possible for a microwave to detect motion in an area where detection is not desirable and not to detect motion in an area where it is desirable. For example, a large metal filing cabinet in the area of detection will shield the area behind it. Objects such as these create "dead zones" (areas where the sensor cannot detect motion), thereby creating a potential hiding place for an adversary. On the other hand, because the beam can penetrate walls, the sensor may detect motion behind a wall in another room.

Because microwave sensors operate in the high-frequency spectrum (X band), close association or proximity to other high-frequency signals can adversely affect their detection reliability. Areas that contain strong emitters of electric fields (radio transmitters) or magnetic fields (large electric motors or generators) can affect the ability of microwave sensors to function properly and should be avoided or compensated for by distinct signal separation or shielding. Self-generated signal reflection is a common problem caused by improper placement or mounting. Positioning the sensor externally and parallel to the wall rather than embedding it within the wall will help avoid this problem.

Although it is not easy to defeat a microwave sensor, very slow movement by an intruder is harder for a microwave sensor to detect. The speed required to bypass a sensor will depend on its make and model. Testing in the past has shown that some microwave sensors will have some sensitivity against intruders moving at speeds as slow as 2.5 centimeters (1 inch) per second. The microwave sensor will detect any swaying of the body, including movement of the head, arms, or legs. For a successful defeat, an intruder must be inside the zone of detection for a lengthy period to allow the time necessary to move this slowly and avoid detection, thereby increasing the chances that the intruder will be noticed.

Circumferential motion in a perfect arc with no effective motion toward or away from the sensor will not produce a Doppler shift, and therefore, no detection will occur. However, this type of movement is very difficult for an intruder to accomplish correctly and subsequently avoid detection.

The graphs in Figure 42 show the differences between the detection pattern shape and size with respect to the test subject's direction of movement into an area that is protected by a microwave sensor. The left graph shows the maximum detection pattern with the test subject walking directly toward the sensor. The right graph shows a small decrease in the detection pattern size with the test subject walking parallel to the sensor centerline. The top graph shows a much smaller detection pattern with the subject walking parallel to the sensor face. Walking in this direction creates less of a Doppler frequency shift. The Doppler shift requires a sufficient amplitude change and duration time to generate an alarm. In practical terms, this means that the microwave transmitter sends out a known frequency, and if a higher or lower frequency is returned to the receiver, the target is moving closer or further away from the sensor.

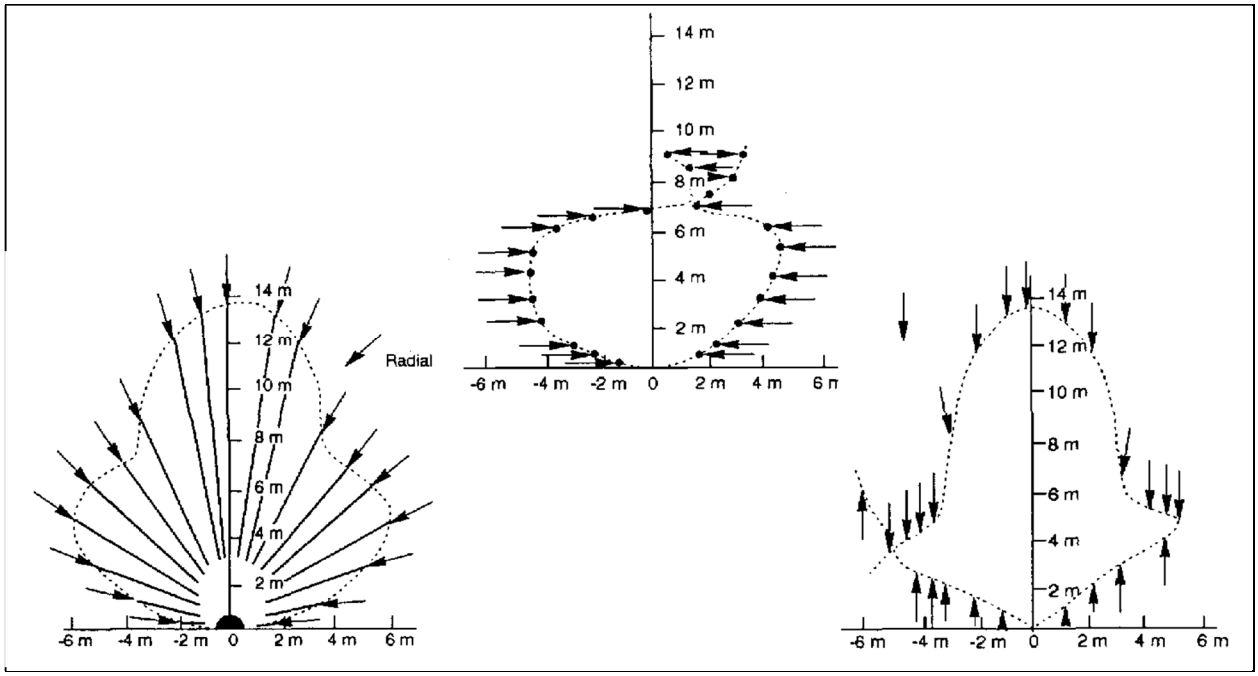


Figure 42 Differences in detection patterns from microwave sensor walk tests

2.3.2.5 Installation Criteria

Interior microwave sensors should ideally be mounted near the ceiling or directly on the ceiling. A rigid and stable mounting assembly should be used. The actual location of the sensor (e.g., ceiling, corner, wall) will depend on the particular sensor being used and on the area or target that it is intended to protect.

In surveys of the area to be protected, any object that may degrade the detection capability of the sensor should be noted (e.g., metal filing cabinets, fans, air conditioner vents). Because microwave energy is difficult to constrain, special care should also be taken when locating and directing the energy within the area requiring detection. A protected volume surrounded by

masonry or metal construction confines microwave energy and prevents detection outside the protected volume, thus preventing one common source of nuisance alarms.

Fluorescent lights located in the sensor detection envelope, especially at distances of less than 3 meters (about 10 feet), may cause low-frequency Doppler shifts originating with reflections from the ionized gas within the fluorescent tubes. Blocking the line-of-sight path by using either a 0.6-centimeter (0.25-inch) metal mesh or an RF absorber eliminates such signal interference.

2.3.2.6 Testing

A regular program of testing interior microwave sensors is imperative for maintaining optimal operating order. Three types of testing must be performed at different times in the life of an interior microwave sensor: (1) acceptance testing, (2) performance testing, and (3) operability testing. Testing should follow the manufacturer's recommendations.

2.3.2.6.1 Acceptance Testing

When first installed, an interior microwave sensor should be tested before it is formally "accepted" as part of the facility's physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the interior microwave sensor; therefore, it should do the following:
  - Verify that the installation matches the installation drawings, which should follow the manufacturer's guidance.
  - Verify that signal and power wires are routed in the conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
- A performance test establishes and documents the level of performance.

2.3.2.6.2 Performance Testing

Performance tests (refer to Figure 42) are designed to verify the level of performance of each interior microwave sensor through the range of intended function. This testing will verify the manufacturer's published detection pattern or will establish the actual detection pattern.

This test should include a visual inspection of the sensor and of the general area where the sensor is installed. Prudent routine maintenance should be performed according to Section 2.3.2.7.

All relevant processor readings should be recorded, and new readings should be compared to the last recorded readings. As in all test situations, a member of the site security force should keep the test area under visual observation, or a member of the site security force should conduct the test.

The test for each interior microwave sensor should, where possible, do the following:

- Ensure that the system meets the manufacturer's specifications and recommended detection probability.
- Verify that no disabling dead spots exist in the zone of protection.
- Verify that line supervision and tamper-indication alarms in both the access and secure modes are functional.
- Verify that the alarm station receives both line supervision and tamper-indication alarms as appropriate.

Records of initial testing capabilities, equipment sensitivity setting, or voltage outputs should be maintained to monitor any deterioration in equipment capability. Walk tests should be performed for all areas covered by the interior microwave sensor, and the results of those tests should be compared with the results of the acceptance test to check for any degradation in the coverage of the sensor.

Radial Path Testing

The following instructions describe the walk test to be conducted along the radial (parallel to the common center of the detection zone) paths, which is the most effective detection approach against a microwave sensor (refer to Figure 43):

(1) Start outside of the published detection area in front of the sensor and walk at 30 centimeters (1 foot) per second along the first radial path.

(2) Stop when an alarm occurs and mark that position.

(3) Return to the start point, wait 30 seconds for the sensor to reset, and repeat the walk test along the same path.

(4) Repeat the test on that path until the required number of tests is completed. Multiple tests along each test line path must be performed to establish a P_D. For example, the sensor would have to pass 29 out of 30 tests to establish that it has a minimum P_D of 90 percent at a confidence level of 95 percent.

(5) Perform Steps 1 through 4 for the remaining radial paths.

Tangential Path Testing

The following instructions describe the walk test to be conducted along the tangential (lateral or perpendicular to the common center of the detection zone) paths, which are the least effective detection approach against a microwave sensor (refer to Figure 43):

- Start outside of the published detection area on one side and walk at 30 centimeters (1 foot) per second along the first tangential path.
- Stop when an alarm occurs and mark that position.

- Return to the starting point, wait 30 seconds for the sensor to reset, and repeat the walk test along the same path.

- Repeat the test on that path until the required number of tests is completed. Multiple tests along each test line path must be performed to establish a P_D. As an example, the sensor would have to pass 29 out of 30 tests to establish that it has a minimum P_D of 90 percent at a confidence level of 95 percent.

- Perform the above tests on remaining paths.

- Repeat Steps 1 through 5, starting from the other side of the detection area.

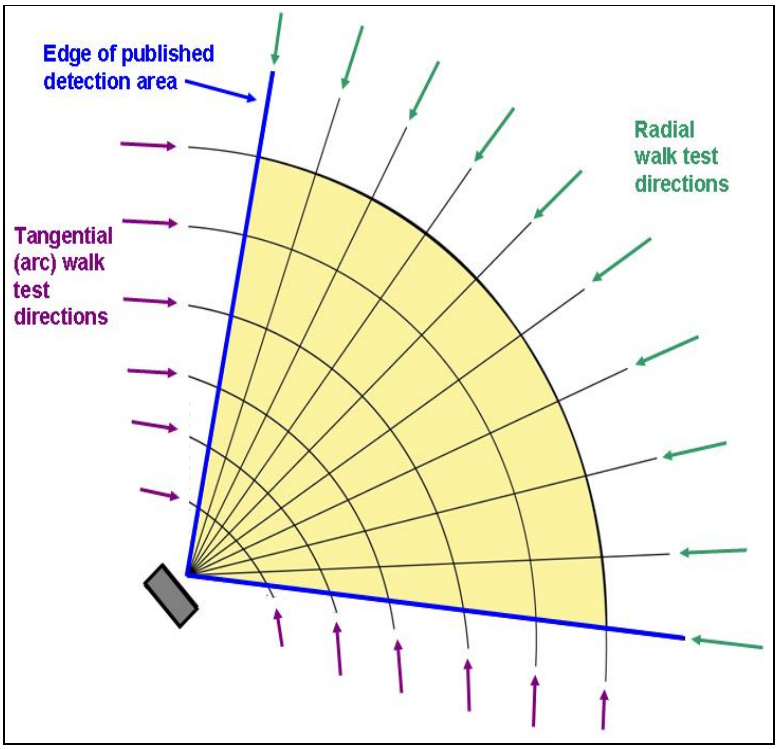


Figure 43 Recommended walk test paths for microwave sensor performance testing

Slow Walk Tests

Slow walk tests are conducted at speeds less than 15 centimeters (0.5 feet) per second. Most volumetric sensors, such as the microwave sensor, will have a speed at which detection capability decreases. If the potential to circumvent a system by crawling is a concern, crawl testing should be performed to obtain detection characteristics. Detection of a crawling intruder will likely be different than detection of a walking intruder.

If an equal number of tests for each approach is not possible, the penetration approach pattern that is most difficult to detect for a particular sensor should be attempted more frequently. The various paths should be tested in random order to reduce the possibility that environmental effects and other unknown factors influenced the test results (i.e., detection or nondetection). Using a random sequence, there is less chance that the test results would be biased.

2.3.2.6.3 Operability Testing

Operability tests for these systems consist of simple walk tests. The testing individual walks through the expected detection zone of a sensor and confirms that the alarm has been received at the alarm display center. The testing individual should look for any evidence of damage to the sensor or tampering with the device.

2.3.2.7 Maintenance

A visual inspection of the installation should be performed quarterly and immediately after major maintenance to the building in the sensor area. Mounting brackets and hardware should be inspected for stability and corrosion. Frequent visual inspections ensure that no blocking objects have been moved into a position that would render the sensor inoperative. Periodic tests, in addition to the sensor or system's invoked self-test, ensure that the sensor is operating effectively. Standby batteries should be replaced on a conservative schedule. Every service call should be entered in a log to record the date, time, corrective action, and an assessment of the cause of the problem.

2.3.3 Passive Infrared

2.3.3.1 Principles of Operation

PIR sensors are the most commonly used volumetric sensor for interior applications. Many facilities use PIRs for the protection of the interior of rooms or particular areas of a room (refer to Figure 44).

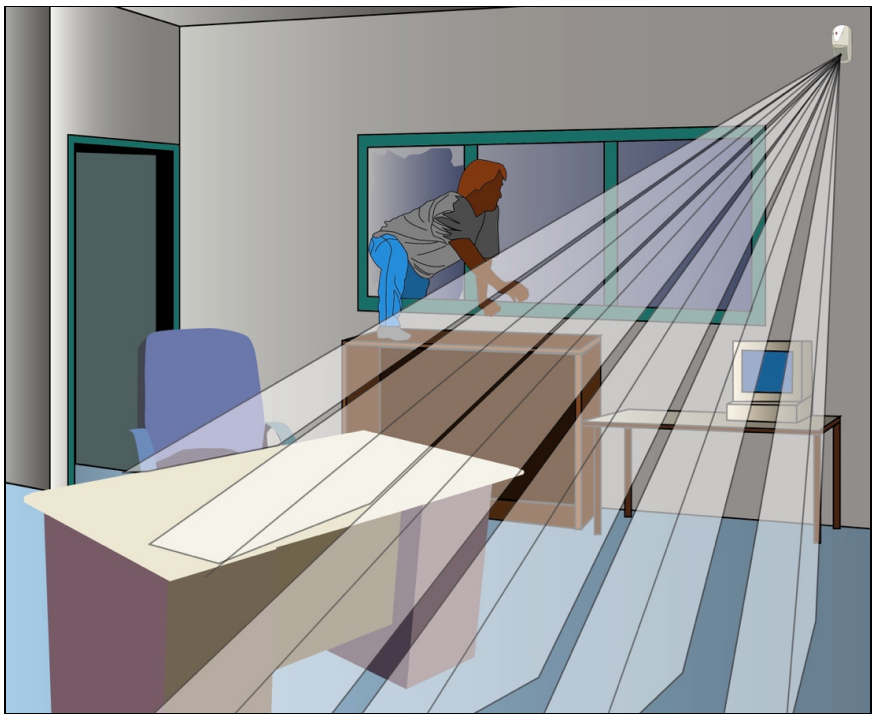


Figure 44 Detection pattern for a typical installation of a PIR sensor

A PIR sensor detects the electromagnetic radiated energy generated by sources that produce temperatures below that of visible light. A PIR sensor does not emit any energy field into the area that it is protecting and does not measure the amount of infrared energy; PIRs measure changes in thermal radiation. A PIR sensor detects thermal radiation by sensing the change in contrast between a heat source and the ambient background temperature. They are considered to be a type of visible sensor because they are in plain view within the area. They also require a line of sight between the sensor and any target to be detected. The sensor detects intrusions as a function of the magnitude of the difference between the intruder's temperature and the background temperature.

Using parabolic mirrors or Fresnel lens optics, the infrared energy is focused on the detector chip in the sensor. Using either variety of lenses, the detection pattern is subdivided into solid angular segments (refer to Figure 45). As an intruder passes across the detection segments, each segment passed through will generate an increase or decrease in temperature, which will trigger an alarm. A thermopile or pyroelectric device detects this infrared energy and converts it into an electrical signal. This signal is then processed by circuitry in the sensor, which determines whether this constitutes an alarm. The electronic processing can be a count of the number of signal pulses over the detection threshold and will generate an alarm only when a specified number of pulses occurs within a certain time period. An alarm is annunciated when the difference between an intruder and the ambient background temperature reaches a predetermined value. On some sensors, this difference can be as small as 1 degree C.

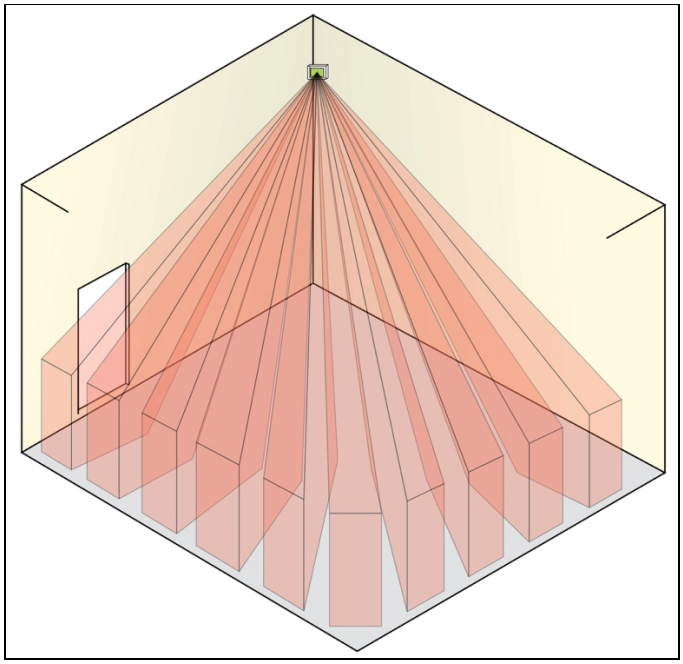


Figure 45 Example of a PIR sensor's subdivided detection pattern

Although infrared radiation is invisible to the human eye, infrared radiation emitted by an object is directly related to its temperature. The infrared region lies between 0.75 and 1,000 micrometers. The human body radiates infrared energy in the 8- to 14-micrometer region.

PIR sensors continuously receive infrared energy from all objects within a protected area. Ceilings, walls, floors, furniture, and other objects all emit infrared energy proportionate to their temperature and emissivity (emissivity defines how well an object absorbs and radiates infrared

energy). A PIR will respond only to changes in the received infrared energy. The absorption and radiation of infrared energy depend on the composition of the surface of the object.

2.3.3.2 Types of Passive Infrared Sensors

By configuring the parabolic mirrors or Fresnel lens, a single conical field (referred to as a "curtain PIR"), a multiple segment field, or a hemispherical field of view can be generated (refer to Figures 46 and 47).

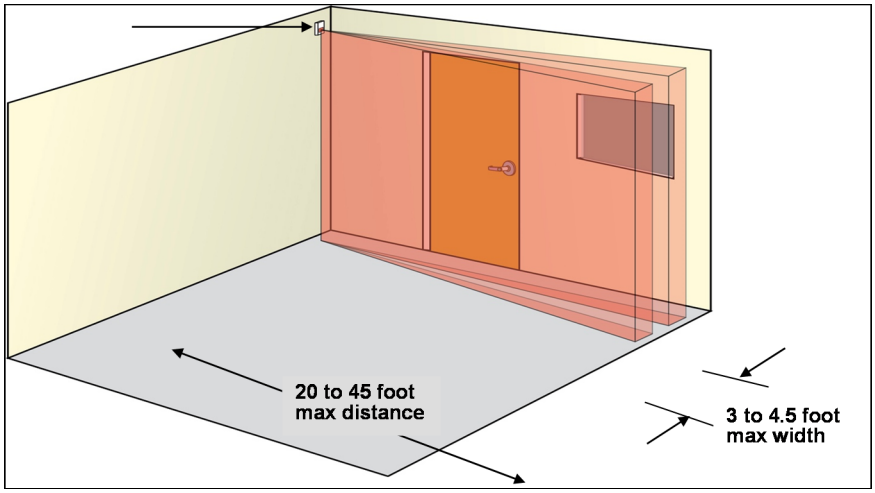


Figure 46 An example of a curtain PIR application

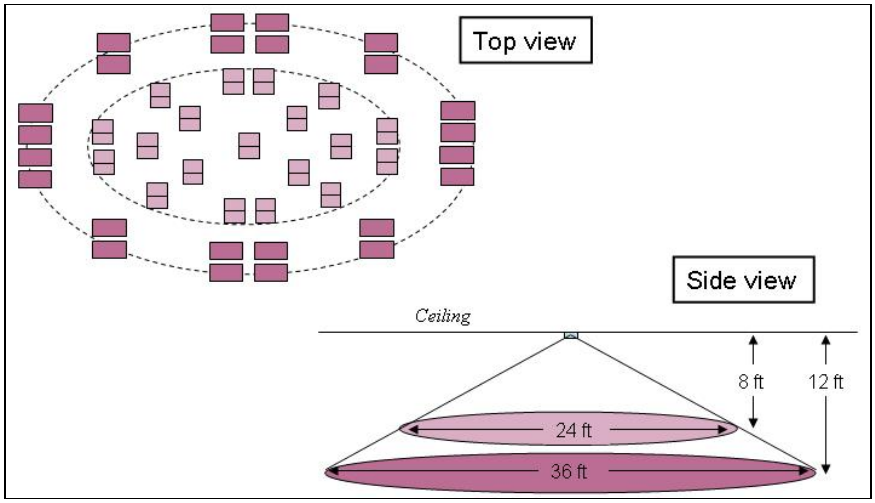


Figure 47 Illustration of the detection pattern of a ceiling-mounted PIR

2.3.3.3 Sources of Nuisance Alarms

Any object that causes an appropriate temperature differential can potentially generate a nuisance alarm in a PIR sensor. The required temperature differential can be caused by rapid changes in localized heating and cooling, which may be affected by the following:

- sunlight

- incandescent light bulbs
- radiators
- space heaters
- heating, ventilation, and air conditioning vents
- hot pipes

In practice, localized heating and cooling are less likely to generate nuisance alarms because temperature changes generally do not happen rapidly. All hot spots that generate infrared energy should be removed or shielded. Radiant energy from such sources may produce thermal gradients that change the background energy pattern. Hot spots can include open heating elements; incandescent light bulbs; convective heat currents; and direct sunlight on windows, floors, and walls.

Sunlight can enter the protected area directly through openings such as broken window panes, ventilation grids, and poorly fitted doors. Small animals or large insects moving in the PIR sensor field of view may also be detected. Devices that retain the required temperature differential and sway into the sensor field of view may generate nuisance alarms.

The vibration of a PIR sensor may generate an alarm by causing a heat source to appear as if it were moving. Insects crawling on elements inside the sensor or condensation forming within the sensor may also generate nuisance alarms.

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

2.3.3.4 Characteristics and Applications

A PIR is installed so that the detection pattern covers the area or asset to be protected. This detection pattern can be pictured as a “searchlight beam” that gradually widens as the zone extends farther from the sensor with some segments being illuminated while others are not. This design characteristic allows the beam to focus on areas where detection is needed while ignoring other areas, such as known sources of false alarms.

Changes in the infrared signature of an object (including people) are most visible when the object moves laterally through the detector’s range. Detection effectiveness is less than optimal for motion directly toward or away from the sensor. Positioning a detector so that an intruder must walk across the detector’s range is much more effective than positioning the detector so that an intruder would likely walk toward the detector.

The presence and location of a passive sensor are more difficult for an intruder to determine than the presence and location of an active sensor, which puts the intruder at a disadvantage.

In environments where explosive vapors or explosive materials may be present, passive sensors are safer than active ones because they do not emit potentially explosion-initiating energy.

Multiple passive sensors can be placed in a volume without interfering with each other (interacting) because they do not emit any signals.

Because the PIR is a line-of-sight detector, cubicle partitions or furniture can easily block the field of view.

Sources of rapid temperature changes can cause nuisance alarms. Sensitivity changes with the temperature of the detection area. If the ambient temperature is near the body temperature of an intruder, the intruder could possibly enter undetected.

Slow-moving targets can present a problem because a PIR sensor will not detect very slow motion. However, defeating a PIR sensor with slow motion is difficult to do because an intruder must keep all body movement to a minimum.

A PIR sensor may fail to detect movement in an area if the lens is masked or fogged.

2.3.3.5 Installation Criteria

Installation of PIR sensors is fairly inexpensive. The manufacturer's guidelines should be followed as appropriate.

All hot spots that generate infrared energy should be removed or shielded. Radiant energy from such sources may produce thermal gradients that will change the background energy pattern. Hot spots can include open heating elements; incandescent light bulbs; convective heat currents; and direct sunlight on windows, floors, and walls. Sunlight can enter the protected area directly through openings, such as broken window panes, ventilation grids, and poorly fitted doors.

For optimal intruder detection, the sensor should be aimed so that the path likely taken will be across the sensor 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 being protected. The detector should not be mounted directly above a doorway or a window or mounted in any position that would allow an intruder access to the sensor from below.

For high-security applications, the small LED light on the sensor that indicates a detection should be turned off when not being tested by authorized personnel.

Placing the sensor near a light source can generate nuisance alarms caused by insects attracted to the light.

All sensors should have the following:

- supervised wiring in conduit
- fail-safe operation
- emergency power in case of main power failure
- tamper indication

An end-to-end self-test is desirable. A final test should be performed after installation to verify the PIR sensor coverage area.

2.3.3.6 Testing

A regular program of testing PIR sensors is imperative for maintaining optimal operating order. Three types of testing must be performed at different times in the life of a PIR sensor: (1) acceptance testing, (2) performance testing, and (3) operability testing. Testing should follow the manufacturer's recommendations.

2.3.3.6.1 Acceptance Testing

When first installed, a PIR sensor should be tested before it is formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the PIR sensor and should do the following:
  - Verify that the installation matches the installation drawings, which should follow the manufacturer's guidance.
  - Verify that signal and power wires are routed in the conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
- A performance test establishes and documents the level of performance as described in Section 2.3.3.6.2.

2.3.3.6.2 Performance Testing

Performance tests verify that the level of performance of each PIR sensor is consistent with the documented performance achieved during the original acceptance testing.

Performance testing should be conducted whenever an electronics module is replaced, the optical alignment is changed, or an adjustment is made that can affect sensitivity. This test should include a visual inspection of the sensor and of the general area where the sensor is installed. Personnel conducting the test should refer to Section 2.3.3.7 and perform the prudent routine maintenance. Test procedures recommended by the manufacturer should be followed. As in all test situations, a member of the site security force should keep the area being tested under visual observation, or a member of the site security force should conduct the test.

The test for each area of detection should do the following:

- Ensure that each PIR sensor meets the manufacturer's specifications and recommended detection probability.
- Verify that no dead spots exist in the zone of protection.
- Verify that line supervision and tamper-indication alarms in both the access and secure modes are functional.

- Verify that the alarm station receives both line supervision and tamper-indication alarms as appropriate.

Records of initial testing capabilities, equipment sensitivity settings, or voltage outputs should be maintained so that deterioration in equipment capability can be identified and monitored.

Walk tests should be performed for all areas covered by the PIR sensor, and the results of those tests should be compared with the results of the initial acceptance test to check for any degradation in the coverage of the sensor.

Tangential (Arc) Path Testing

The following instructions describe the walk test to be conducted along tangential paths. This approach has the likeliest chance of detection because the PIR sensor is most sensitive in this direction (refer to Figure 48).

- Start outside of the published detection area on one side and walk at 30 centimeters (1 foot) per second along the first tangential path.

- Stop when an alarm occurs and mark that position.

- Return to the starting point, wait 30 seconds for the sensor to reset, and repeat the walk test along the same path.

- Repeat the test on that path until the required number of tests is completed. Multiple tests along each test line path must be performed to establish a P_D. For example, the sensor would have to pass 29 out of 30 tests to establish that it has a minimum P_D of 90 percent at a confidence level of 95 percent.

- Perform Steps 1 through 4 on remaining paths.

- Repeat Steps 1 through 5, starting from the other side of the detection area.

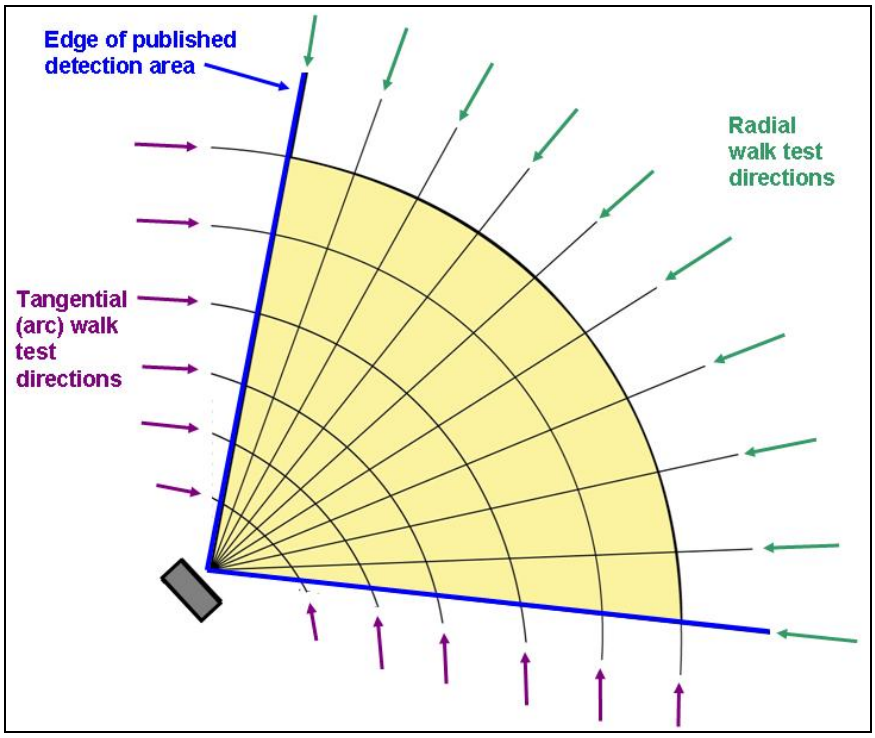


Figure 48 Recommended walk tests for the performance testing of a PIR sensor

Radial Path Testing

The following instructions describe the walk test to be conducted along the radial paths. This approach has the least likely chance of detection because the PIR sensor is least sensitive in this direction (refer to Figure 49).

- Start outside of the published detection area in front of the sensor and walk at 30 centimeters (1 foot) per second along the first radial path.
- Stop when an alarm occurs and mark that position.
- Return to the starting point, wait 30 seconds for the sensor to reset, and repeat the walk test along the same path.
- Repeat testing on that path until the required number of tests is completed. Multiple tests along each test line path must be performed to establish a P_D. For example, the sensor would have to pass 29 out of 30 tests to establish that it has a minimum P_D of 90 percent at a confidence level of 95 percent.
- Perform Steps 1 through 4 for the remaining radial paths.

Changes in the room configuration can affect PIR sensor coverage and should be checked. If the room configuration has changed significantly, a complete retest of the sensor coverage should be done to ensure the protection of the room or the asset.

The test should determine the most vulnerable area for each section and the method of approach most likely to penetrate (e.g., walking, running, jumping, crawling, rolling, or climbing). In most cases, this determination will depend on the sensor and location. The penetration approach that is most difficult to detect should be attempted more frequently if an equal number of tests for each approach is not possible.

The various approach paths should be tested in random order to preclude the possibility of environmental effects and other unknown factors affecting the test results (i.e., detection or nondetection). Using a random sequence reduces the chance that the test results will be biased.

When determining the best place to locate an asset within a room, the designer could use as guidance a sample graph like that shown in Figure 49, which shows the PIR sensor detection pattern. The asset should be placed inside the area that has a high P_D, no matter the direction from which the intruder approaches the sensor.

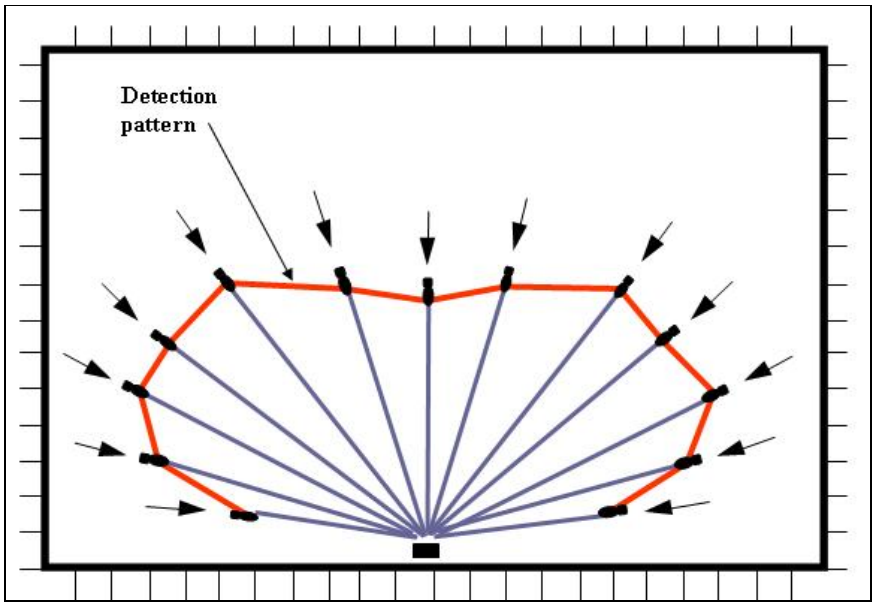


Figure 49 A typical PIR detection pattern derived from walk tests toward the sensor

2.3.3.6.3 Operability Testing

Operability testing should be conducted by crossing the zone of detection in the monitored area. The detection capabilities of each PIR should be walk tested in a different order, preferably random, on a weekly (i.e., every 7 days) basis, and the tests should be conducted throughout the week rather than all on the same day. The testing should result in 100-percent detection on all segments on a weekly basis. If the interior intrusion alarm system fails to detect an intrusion in one or more segments, corrective actions should be taken and documented. Records should be maintained to document that all required testing has been accomplished.

2.3.3.7 Maintenance

The general maintenance guidelines outlined in the manufacturer's technical manuals should be followed on a schedule determined by security maintenance personnel and security forces and by the environment in which the PIR sensor is installed.

At a minimum, the sensor optics should be periodically cleaned and frequent visual inspections performed to ensure that no objects have been moved into a blocking position that would render the sensor inoperative.

Equipment maintenance guidelines generally recommend that a facility should keep 10 to 20 percent of spare parts on hand, based on its total units. This requirement may be adjusted as maintenance data are accumulated on the failure rate of specific sensors and sensor components. If a facility can quickly obtain replacement parts from regional distributors, smaller onsite inventories would be adequate.

2.3.4 Proximity Sensors

2.3.4.1 Principles of Operation

Proximity sensors, also known as point protection/detection devices, can detect someone approaching, touching, or attempting to remove valuable items. Proximity sensors usually form the innermost level of protection after exterior perimeter sensors, boundary penetration sensors, and volumetric sensors. Because they are usually located close to a particular asset, the response force has the least amount of time to respond to an alarm once the intruder is detected. For this reason, proximity sensors should not be used as the primary detector for a high-risk item. Proximity sensors are most effective for protection against an insider.

2.3.4.2 Types of Proximity Sensors

The types of proximity sensors describe below include capacitance, pressure, strain, and switch sensors.

2.3.4.2.1 Capacitance

Capacitance proximity sensors operate on the same principle as an electrical capacitor. These types of detectors are used to protect metal containers, such as safes or file cabinets, that can be isolated from ground. An electrical capacitor comprises one or more conductors separated by a dielectric medium. A change in the electrical characteristics 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 or 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. When a person comes close to or touches the object, the dielectric is changed, which in turn changes the capacitance. The processor (part of the capacitance sensor) detects the change in capacitance and generates an alarm.

2.3.4.2.2 Pressure

Pressure sensors incorporate a sensing device that responds to deformation of the sensor caused by weight placed on it. Pressure mats consist of a series of ribbon switches positioned

parallel to each other, approximately 7.5 centimeters (3 inches) apart along the length of the mat. Ribbon switches are constructed from two strips of metal in the form of a ribbon separated by an insulating material. When an adequate amount of pressure, depending on the application, is exerted anywhere along the ribbon, the metal strips make electrical contact. They can be used to detect the presence of intruders when they approach or attempt to move protected items. For instance, pressure mats can be installed under the carpet around the protected item. Anyone who approaches the item steps on the mat and generates an alarm. The operation of a pressure mat represents the operation of pressure sensors in general. The pressure sensor output signal is routed to an alarm console to indicate an intrusion.

2.3.4.2.3 Strain

Strain sensors measure small amounts of deformation or flexing of a surface. A basic configuration of a strain sensor would involve one or more sensing devices connected to a processor. The sensing devices can use piezoelectric, piezoresistive metal foil or wire to detect surface deformation or flexing. When configured to be a strain sensor, the electrical properties (such as resistance) of these materials will change when they are bent, stretched, or compressed. The processor continually measures the electrical properties of the sensing device and will generate an alarm or other indication when a specified amount of change has occurred. Processors will typically have user-programmable controls to specify how much change has to occur in order to generate an alarm. In a proximity sensor application, the sensing device is attached to a surface that is flexed slightly when an object (such as a protected item) is placed on it. The processor is programmed to alarm if a change occurs, such as when the object is removed or tampered with.

2.3.4.2.4 Switches

Switches can be used as a proximity point sensor. A protected item is placed on the switch, actuating it so that the electrical contacts are either in an open or closed position. Alarm system electronics monitor the switch for a change in the position of the contacts. If the item is removed, the contacts change position, and an alarm is generated. Movement of the item can also generate an alarm if it causes the switch contacts to change positions. The surface and switch mounting must be designed in a manner that makes removal of the protected item very difficult while attempting to maintain the switch in the secured position.

2.3.4.3 Sources of Nuisance Alarms

Changes in relative humidity and the relocation of other metal objects closer to or farther away from a protected item affect the sensitivity of capacitance sensors. Changes in the relative humidity vary the dielectric characteristics. A rapid increase in humidity causes the dielectric (air) conductivity to increase and reduces the capacitance, thus generating an alarm. Conversely, a decrease in humidity or drying of the air reduces the conductivity. Similarly, when larger metal objects (i.e., with high electrical conductivity, such as cabinets, desks, and equipment racks) are moved close to an object that is protected by a capacitive sensor, the sensitivity of the sensor can change. If the sensitivity is increased, the chance for nuisance alarms increases. If the sensitivity is decreased, detection capability is lowered.

Nuisance alarms from pressure mat sensors can occur if the insulating or separating material that keeps the ribbon switch contacts apart deteriorates through wear or exposure to harsh conditions. Extreme heating and cooling (out of the operating range) are additional nuisance alarm sources, especially if the mat is worn and deteriorated. A mat installed near heavy traffic

areas where personnel would inadvertently step on it is an additional source of nuisance alarms. Pressure mats that are in good condition and installed properly should generate very few nuisance alarms.

Changes in temperature can affect strain sensor devices and generate nuisance alarms. Some strain sensors are configured to reduce or eliminate the effects of temperature changes. Changes in humidity can also be a source of nuisance alarms. If the protected item can absorb moisture, the weight of that object could fluctuate enough with humidity changes to cause nuisance alarms.

Switch sensors in good condition and installed properly should generate very few, if any, nuisance alarms. Primary nuisance sources include loose or damaged mounting brackets, fasteners, and mounts and damaged or worn out internal or external components of the switch itself.

2.3.4.4 Characteristics and Applications

Proximity sensors should not be used as the primary detector for high-risk items. They are typically used as a second or third line or layer of protection and are most effective for protection against an insider threat. The goal would be to detect the insider who is very close to, touching, or moving an object that he or she should not have access to. Portable high-value objects should be in a cage or safe or tied down to add delay to an abrupt theft (refer to Figure 50). Portable high-risk or high-value items should be locked in cabinets or secured by other means to delay their removal. Proximity sensors can be installed to detect attempted removal of tiedowns or opening of cabinets.

Figure 50 Example of portable high-value items

A typical application of a capacitance proximity detector would be the protection of a safe or file cabinet (refer to Figure 51). The safe or file cabinets must be set on blocks to isolate them from the ground plane. The blocks should be made of a nonconductive plastic or nonhydroscopic

material. Wooden blocks should not be used because they are hydroscopic and could absorb enough moisture over a period of time to change the dielectric characteristics enough that the protected objects become insensitive. Capacitive detectors can be used to protect paintings, tapestries, and other objects by installing a relatively large copper foil sheet or metal screen under the objects that require protection. In this type of application, the metal screen and the safe or any other metal object become part of the protected circuit.

Industrial and commercial applications commonly use pressure mats (e.g., as controls for opening doors or as safety devices for machinery). Although pressure mats are less common in security applications, they can be used along probable intruder routes or around valuable objects. They are usually well concealed under carpets or flooring to make it more difficult for an intruder to determine the location of the detection area.

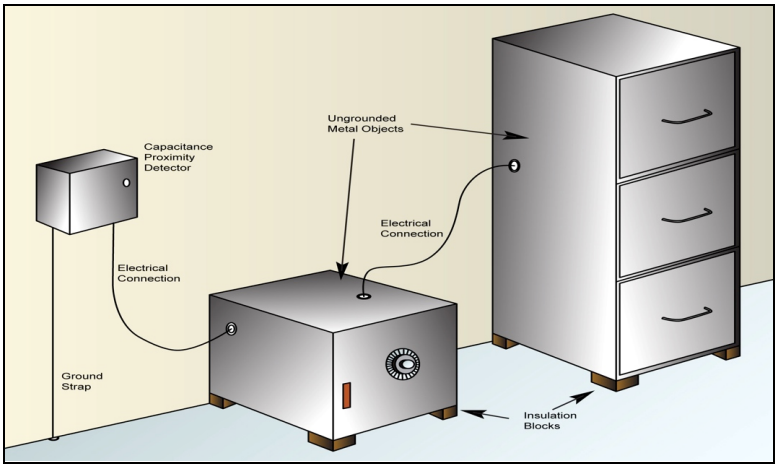


Figure 51 Example of a capacitance sensor installation

Strain sensors can be used to continually monitor the weight of an object. They can sense when an object is being lifted, moved, or tampered with (refer to Figure 52). Consideration must be given to the environment to account for potential changes in temperature or humidity. Strain sensors can also be used to detect a person's weight as they approach a protected area or item (refer to Figure 53).

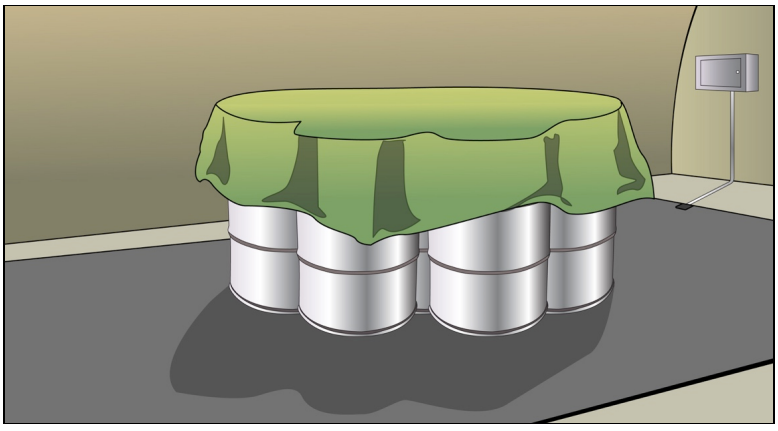


Figure 52 Example of a pressure mat

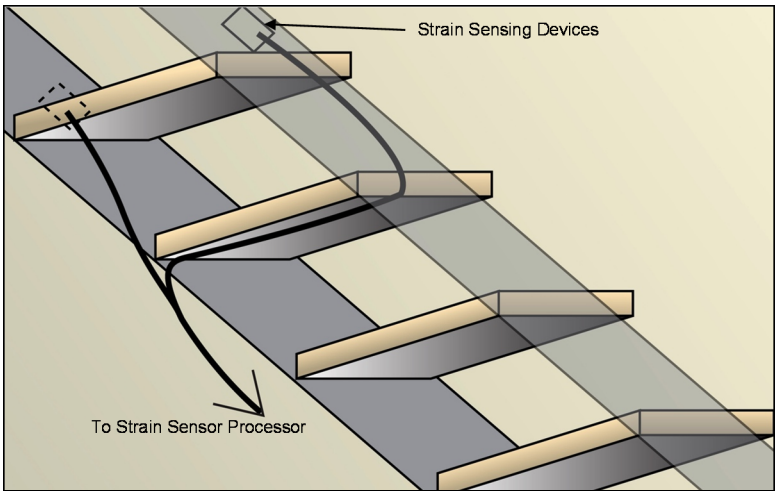


Figure 53 Strain sensor concept to detect an intruder on stairs

An adversary can defeat a self-adjusting capacitance proximity sensor by approaching the protected object extremely slowly. An adversary can detect the presence of a capacitance proximity sensor by using RF field-sensing equipment, such as the equipment used by a telephone company to find underground telephone cables. Relocating any conducting object closer to or farther away from the protected surface can cause a small capacitance change between the protected surface and ground, thus generating a nuisance alarm. These objects include persons walking near or leaning on the surface, cabinets, other objects being moved close to the surface, or loose-fitting components of the protected object itself. A capacitance sensor may not work well (i.e., may generate many nuisance alarms) if the protected object is in an area that experiences high traffic close to the object when the sensor is in the secured condition.

Sudden changes in the relative humidity affect the sensitivity of a capacitance proximity sensor. Changes in the moisture content of the air will vary the dielectric characteristics 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.

A pressure sensor is vulnerable to bridging by an intruder placing a board on bricks to walk over it or by an intruder jumping or stepping across it. A pressure sensor is also subject to considerable wear from normal traffic and should be tested periodically to ensure that the sensor is operating effectively. A mat sensor could be used to let occupants in the room know that someone is at the door, but it can be easily bridged if installed incorrectly (refer to Figure 54).

A strain sensor responds to any action that causes the surface on which it is mounted to flex. Heavy machinery in the building or nearby heavy vehicular traffic can cause surfaces to vibrate and generate nuisance alarms. Although the sensor operates at frequencies as low as direct current (dc), limiting the low-frequency response avoids alarms caused by long-term drift and slow deformation of the structure over time.

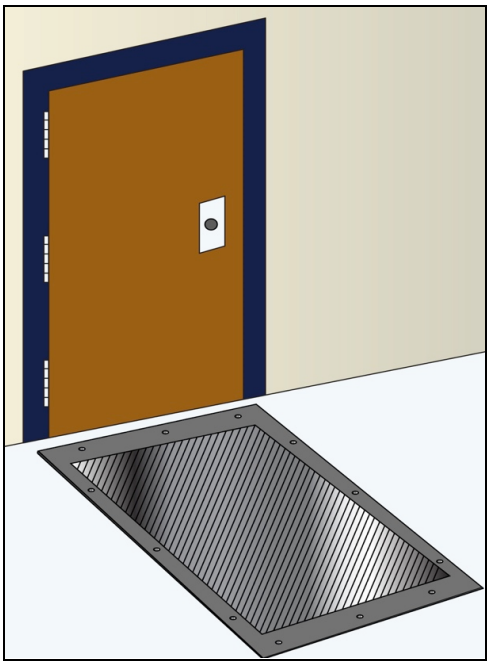


Figure 54 Example of a mat sensor near a door

2.3.4.5 Installation Criteria

For installation and setup of proximity sensors, the manufacturer's instructions and recommendations should be followed. The sensors should be equipped with a tamper-indicating device that is continuously monitored by the security system. These tamper-indicating devices are typically switches that detect the removal or opening of a cover or door that allows access to the sensor electronics. All wiring for these systems (alarm, power, or tamper) should be in conduit, and the alarm and tamper signal wiring should be supervised. Backup batteries or standby power is recommended. Once installed, performance testing is necessary to confirm the desired detection capability of the proximity sensor. Testing should include attempting to defeat the sensor using defeat methods for the sensor technology. Short-term trial operation (i.e., several days to several weeks) will help determine any initial and common nuisance alarm sources. An end-to-end self-test is also desirable. The sections below describe general installation criteria for each type of proximity sensor.

2.3.4.5.1 Capacitance Sensor

The capacitive sensor requires a ground plane, which could consist of cables, conductive mats, or conductive foil under, near, or around the protected object. The protected object must be isolated from the ground plane using nonhydroscopic materials. Both the protected object(s) and the ground plane must be connected to the processor unit, which is typically mounted on a wall close to the protected object.

2.3.4.5.2 Pressure Sensor

The pressure sensor is usually concealed from an intruder as a doormat or by placing it under the floor covering. The sensor pad can be installed in a depression in the floor. If the pad is placed under a protective cover such as a rug or a rubber doormat, the protective cover must be fastened down around the edges to prevent the pad from moving or being removed.

2.3.4.5.3 Strain Sensor

The strain-sensing device should be mounted at the point where the largest deflection is most likely to occur. If that point cannot be defined, the best procedure is to mount the strain sensor in the center of the surface. The sensor should be bonded to the surface as rigidly as possible to force the sensor to elongate or contract when the surface flexes and to ensure that it will not separate or slide along the surface. The strain sensor may require site- or object-specific design and fabrication of the mounting or attaching surface.

2.3.4.5.4 Switch Sensor

The switch sensor may require site- or object-specific design and fabrication. Basic installation criteria include a way to secure the object to the placement surface, protection of the switch and switch wiring from tampering, protection against the removal or moving of the protected object by making it very difficult to do so while keeping the switch in the secured position, and connection of the switch contacts to an alarm communication system.

2.3.4.6 Testing

Testing should follow the manufacturer's recommendations.

2.3.4.6.1 Acceptance Testing

When first installed, a proximity sensor should be tested before it is formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the proximity sensor and should do the following:
  - Verify that the installation matches the site installation documentation and drawings, which should follow the manufacturer's guidance.
  - Verify that signal and power wires are routed in the conduit.
  - Verify proper power levels, both voltage and amperage.
  - Verify correct wire connections.
- Performance testing establishes and documents the level of performance as described below.

2.3.4.6.2 Performance Testing

Performance testing should include a visual inspection of the proximity sensor and of the general area where the sensor is installed. When performing testing, alignment, or adjustments on sensors, the assistance of additional personnel should be considered as these activities can be difficult for one person to manage.

For proximity sensors, performance testing should include tests to verify good detection when a protected item and any associated delay hardware are approached, touched, or moved.

Specific tests will depend on the sensor type and installation configuration. Tests should be conducted at different locations around, near, and at the protected object. Several tests at each location should be conducted to achieve a confidence level for detection. Performance testing procedures should include testing of tamper switches, backup batteries, or power supplies and receipt of correct detection and tamper alarms at the alarm stations.

Sensor-specific performance test procedures should be developed and documented. Procedures should include step-by-step test methods; pages or forms to record test results (including a sketch of the sensor detection coverage, if applicable); and a form to record the sensor model, serial number, settings, and other data as necessary. Test results and data can be compared to previous test results to determine trends or the occurrence of gradual degradation. Test results and documentation should be protected from unauthorized disclosure.

2.3.4.6.3 Operability Testing

Operability tests should be conducted on proximity devices in a manner in which the sensor is designed and installed to function (e.g., opening doors to activate sensor alarms, moving through protected areas, or being close to or touching a protected item). Certain proximity sensors (e.g., switch and strain sensors) require a protected item to be moved or a protective cage or cabinet to be opened to activate the alarm. Testing of these types of alarms may require increased coordination among facility personnel to ensure that safety and security are maintained during the testing.

During operability testing, testers can visually inspect the protected area or asset to ensure that objects that affect the detection capabilities of the sensor or that could cause nuisance alarms have not been placed in the area or near the protected asset.

2.3.4.7 Maintenance

In addition to any self-test invoked by the proximity sensor or the system, periodic operability and performance tests must be performed to ensure that the sensor is operating effectively. The installation should be visually inspected periodically, particularly after the completion of any major maintenance to the protected surfaces. Maintenance should be performed in accordance with the manufacturer's recommendations. Standby batteries should be tested on a conservative schedule and replaced when indicated. Every maintenance or repair action should be entered in a log to record the date, time, corrective action, the name of the person who performed the maintenance or repair, and an assessment of what may have caused the problem. The sections below describe maintenance activities for each proximity sensor type.

2.3.4.7.1 Capacitance Sensor

The area near the protected object requires extremely good housekeeping because a 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 dielectric of the air that is placed near the protected item must be removed. Wet mopping or liquids spilled on wooden floors under and around the protected object can significantly change the operation of a capacitance sensor.

2.3.4.7.2 Pressure Sensor

Because a mat-type sensor can be subject to considerable wear from traffic during normal business hours, frequent operability tests are important. During testing, the tester should inspect the sensor for visible signs of wear and degradation.

2.3.4.7.3 Strain and Switch Sensors

During periodic testing, the tester should inspect strain and switch sensors for loose attaching hardware, loose connections, and excessively worn parts.

2.3.5 Dual-Technology Sensors

2.3.5.1 Principles of Operation

Dual-technology sensors (also referred to as “dual-tech” sensors) are designed to lower the false or nuisance alarm rates in an interior sensor by combining two different types of sensors in one casing so that each sensor is complementary (i.e., each sensor generates a different set of nuisance alarm sources). The two sensors are connected electronically by using an “AND” gate logic function; both technologies need to sense an event within a predetermined interval before a valid alarm will be generated. If one technology has a detects an event but the other does not, no alarm will be generated. Because the two sensors will not sense an intrusion at the same instant, the system is designed to generate an alarm when both sensors sense an intrusion in a preselected time interval, usually a few seconds. This time interval is usually a parameter that the user can configure.

Reducing the nuisance alarm rate of a sensor is highly desirable. However, this feature comes at a price—making a unit less sensitive to possible nuisance alarms also makes the unit less sensitive to valid alarm conditions. For this reason, dual-technology sensors that are configured to operate in an AND gate logic are not normally recommended for high-risk or high-security facilities.

Less commonly, dual-technology sensors can be designed to operate using “OR” gate logic. With the OR configuration, either sensor technology can generate an alarm independent of the other. This configuration is similar to having two separate sensors installed in the same location. Unfortunately, two different types of sensors are not likely to both be optimally installed in the same location. For example, a PIR sensor would be best placed such that an adversary would likely walk across the detection zone, whereas a microwave sensor would be best positioned such that an adversary would likely walk toward or away from the detection unit. Therefore, in high-risk facilities, the installation of two different types of sensors in locations that are optimal to their own detection capabilities would be preferable to the use of a dual-technology sensor configured with an OR gate logic (refer to Figure 55).

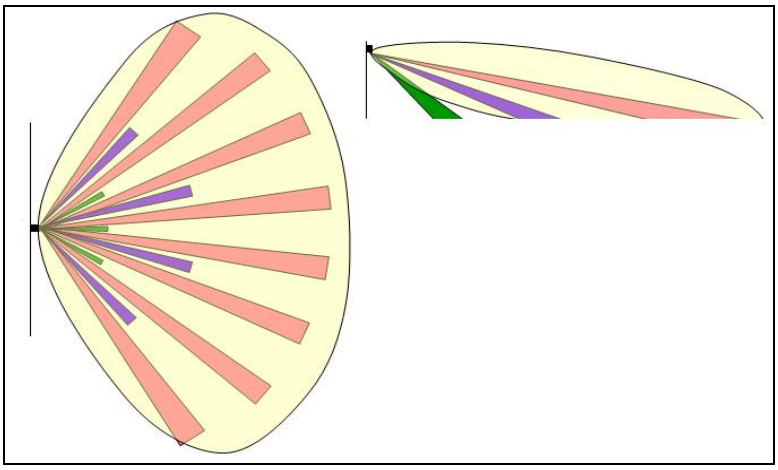


Figure 55 Example of a dual-technology sensor

In Figure 55, the image on the left depicts an overhead view, and the image on the right depicts a side view of the patterns of detection for a dual-technology sensor comprising a PIR sensor and a microwave sensor. The pale yellow illustrates the microwave detection pattern, and the remaining colors illustrate the PIR detection pattern. Most dual-technology sensors use AND gate logic for the two different sensors such that both sensors would have to sense a detection before the sensor would signal an actual alarm.

2.3.5.2 Types of Dual-Technology Sensors

Two combinations of dual-technology sensors are usually used for interior protection: (1) PIR acoustic and (2) PIR microwave. Many manufacturers build these sensors with varying technical specifications; therefore, the sensor should be carefully selected to meet the needs of the particular application. The sections below describe the different types of dual-technology sensors.

2.3.5.2.1 Passive Infrared Acoustic

The PIR-acoustic dual-technology unit uses a PIR sensor and usually an ultrasonic sensor. The ultrasonic sensor generates a teardrop-shaped pattern of acoustical energy at frequencies well above those audible to humans. The patterns are typically about 9 meters (30 feet) deep and 7.6 meters (25 feet) wide. They detect disturbances in the reflected energy from a person moving in a radial direction in the energy pattern. The shape of the PIR detection segments is similar to the ultrasonic energy pattern configuration. A person moving in the zone of detection will generate an alarm if detected by both the PIR sensor and the ultrasonic sensor.

2.3.5.2.2 Passive Infrared Microwave

The PIR microwave dual-technology unit employs a PIR sensor and a microwave sensor. The microwave sensor detects Doppler changes in the reflected microwave energy pattern produced by a person moving in the area with some radial velocity relative to the detector. This teardrop-shaped pattern typically covers an area that is about 20 meters (65 feet) deep and 15 meters (50 feet) wide. The shape of the PIR detection segments is also similar to the microwave energy pattern configuration (refer to Figure 55).

2.3.5.3 Sources of Nuisance Alarms

Because dual-technology sensors are normally configured to operate with AND gate logic, the likelihood of nuisance alarms is greatly reduced. If operated with OR logic, sources of nuisance alarms will be the sum of sources of nuisance alarms for the individual sensors.

The PIR detector in most dual-technology units can trigger nuisance alarms from heat, sunshine, incandescent lights, and other sources.

For the PIR-acoustic dual-technology sensor, air turbulence from heating or air-conditioning ducts, drafts, or other sources of moving air reduces the ultrasonic sensor effectiveness. Acoustic energy generated by ringing bells or hissing noises (e.g., noises produced by radiators or compressed air systems) contains frequency components in the operating frequency band of ultrasonic motion detectors. These sources of ultrasonic energy may occasionally produce signals similar to those for an intruder, which can confuse the signal processor and result in nuisance alarms.

One important characteristic of a PIR-microwave dual-technology sensor is that microwave energy can pass through light construction material that can generate nuisance alarms.

It is also important to remember that, for a dual-technology sensor, when two sensors are logically combined using AND gate logic, the P_D of the combined detectors will be less than the P_D of the individual detectors. The P_D of the combined sensors in a single unit will be less than if the individual detectors are mounted perpendicular to each other with overlapping energy patterns and fields of view.

2.3.5.4 Characteristics and Applications

Dual-technology sensors usually have a lower nuisance alarm rate than single technology sensors when the detectors are properly applied, assuming that each sensor has a low nuisance alarm rate. This sensor type attempts to achieve absolute alarm confirmation (i.e., no nuisance alarms) while maintaining the highest P_D possible for this kind of unit.

The main advantage of a PIR-microwave dual-technology sensor is that both the PIR and the microwave are complementary in providing long, narrow fields of detection. The combination of the technologies in the AND gate logic configuration significantly reduces the false alarm rate. These types of sensors would best be used as a proximity-type sensor system that confines detection to a small area or a single object.

A PIR-acoustic dual-technology sensor can typically cover open areas that are approximately 7.6 meters (25 feet) by 7.6 meters (25 feet). A feature of ultrasonic energy is that it will not penetrate physical barriers such as walls; therefore, it can be easily contained in closed rooms. Because acoustical energy will not penetrate physical barriers, the walls of the protected room either absorb or reflect the energy.

Ceiling-mounted transceivers generate a cone-shaped energy pattern that can cover a circular area of about 9.1 meters (30 feet) in diameter when the transceiver is mounted 3 to 4.6 meters (10 to 15 feet) above the floor. A ceiling-mounted transceiver can be mounted directly over the area requiring protection. This feature is especially valuable in areas that are difficult to protect using wall-mounted transceivers. Long-range ultrasonic transceivers are available with long, narrow energy patterns for protecting aisles and hallways. A single detector of this type can

protect a hallway that is about 21.3 meters (70 feet) long. Combined microwave and infrared detectors cover open areas from 12.2 meters (40 feet) deep and 7.6 meters (25 feet) wide up to 22.9 meters (75 feet) deep and 13.7 meters (45 feet) wide. These detectors also cover long, narrow areas up to 61 meters (200 feet) long.

When sensors are combined in an AND gate logic configuration, the P_D of 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 that has a 0.95 P_D, the resulting 0.90 P_D for the dual-technology sensor is the product of the individual probabilities. A P_D of 0.90 may not meet the required P_D for some facilities.

Assuming a single direction of intrusion, a higher P_D can be obtained from separately mounted sensors than it can from a dual-technology sensor. Ultrasonic and microwave sensors have their highest P_D for radial motion either toward or 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 that are 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 for a dual-technology sensor is achieved by treating the individual sensors separately in an OR configuration.

Vulnerabilities for a dual-technology sensor include vulnerabilities for each sensor technology. In the AND gate logic configuration, if either sensor is defeated, the dual-technology sensor unit is defeated. For this reason, a dual-technology sensor should never be used as a replacement for two separately installed sensors in high-security applications. If a dual-technology sensor is necessary in a location because of nuisance alarm issues, another sensor (dual- or single-technology sensor) should be used and installed in such a manner that each sensor unit protects the other and provides overlapping detection coverage within the area being protected.

Environments where either detector type would be prone to nuisance alarms should be avoided. If either detector is exposed to an environment where it experiences a high number of false alarms, the probability of one of these false alarms being present at the AND gate logic when a false alarm arrives from the second (and perhaps more stable) sensor is high. For example, if a PIR-acoustic detector was installed in a drafty area where the ultrasonic detector would experience a high number of false alarms because of the distortions in its projected energy pattern and the infrared detector might experience a few alarms as the result of background temperature changes caused by the drafts, the probability of simultaneous alarms from both sensors would be increased. A combination microwave and infrared detector would be a better choice for such an application because this environment would not affect the microwave detector. The drafts would still cause temperature changes that could affect the infrared detector; however, because it would be combined with the microwave detector, the probability of simultaneous false alarms would be low, and consequently, the false alarm rate would be lower.

One concern when using a dual-technology sensor that combines microwave and infrared detectors with AND gate logic is that the microwave's detection zone is usually much larger than the infrared's detection zone; therefore, no detection will occur until the intruder reaches the point at which both sensors can detect him or her.

2.3.5.5 Installation Criteria

Microwave technology is usually more sensitive in its least sensitive direction than the PIR is in its least sensitive direction. For this reason, the following considerations apply:

- Performance testing and evaluation should be similar to that required for a PIR sensor.

- Primary consideration should be given to the PIR sensor during installation of the dual-technology sensor. The most likely paths to the protected item or area should cross through the PIR detection pattern; the path should not be directly toward or away from the sensor unit.

- A dual-technology sensor should be located so that the likely path of an intruder will be across the sensor detection area and is less likely to be toward the sensor.

A dual-technology sensor should be installed using a sturdy mount. Installation criteria should consider the manufacturer's recommendations. Vibration can cause misalignment or make the sensor prone to nuisance alarms. The installer should make sure that the sensor is aligned away from possible nuisance alarm sources (e.g., heaters).

If a facility plans to use dual-technology sensors, it should install multiple sensor units such that each unit provides overlapping protection of the other.

2.3.5.6 Testing

A regular program of testing dual-technology sensors is imperative for maintaining them in optimal operating condition. Testing should follow the manufacturer's recommendations. Three types of testing must be performed at different times in the life of a dual-technology sensor: (1) acceptance testing, (2) performance testing, and (3) operability testing.

2.3.5.6.1 Acceptance Testing

When first installed, a dual-technology sensor should be tested before it is formally "accepted" as part of the physical protection system. Acceptance testing consists of a physical inspection and a performance test, as follows:

- A physical inspection ensures proper installation of the sensor and should do the following:

  - Verify that the installation matches the installation drawings, which should follow the manufacturer's installation guidance

  - Verify sensor intersection spacing.

  - Verify that signal and power wires are routed in conduit.

  - Verify proper power levels, both voltage and amperage.

  - Verify correct wire connections.

  - Perform a complete alignment in accordance with the manufacturer's manual on all units to verify that all modules are operational and oriented correctly. The method of physical alignment is specific for each manufacturer's model.

- Performance testing establishes and documents the baseline level of performance as described below.

2.3.5.6.2 Performance Testing

Performance tests are designed to verify the level of performance of each dual-technology sensor through the range of its intended function. Performance testing should be conducted when the following apply:

- replacement of an electronics module
- a change of the physical alignment or any adjustment that can affect sensitivity
- after remodeling of the building structure
- any major change in the arrangement of furniture or equipment

Performance testing should include a visual inspection of the sensor and of the general area where the sensor is installed. The manufacturer's recommended testing procedures should be followed.

Performance testing and evaluation should be similar to that for a PIR sensor. The most likely path to the protected item or area should ideally cross through the PIR detection pattern; the path should not be directly toward or away from the sensor unit. In addition to the extensive walk tests described in this report, other tests can be performed. Slow walk tests should be conducted at speeds of less than 15 centimeters (0.5 feet) per second. Most volumetric sensors will have a speed at which detection capability decreases. If the potential to circumvent a system by crawling is a concern, crawl testing should be performed to obtain detection characteristics. The detection pattern of a crawling intruder will likely be different from that of a walking intruder.

The test should do the following within each area monitored by sensors:

- Ensure that the system meets the manufacturer's specifications for P_D.

- Verify that no dead spots exist in the zone of protection.

- Verify that line supervision and tamper protection in both the access and secure modes are functional.

Records of testing results and equipment sensitivity settings or voltage outputs should be maintained to monitor any deterioration in equipment capability. Walk tests should be performed for all areas covered by the dual-technology sensor, and the results of those tests should be compared with the results of the acceptance test to check for any degradation in the coverage of the sensor or misalignment problems. Significant changes in the configuration of the room could affect sensor coverage. If room configuration has changed significantly, a complete performance test of sensor coverage should be initiated to ensure that the asset or room is protected. Because the PIR is the dominant technology in this configuration, the performance test guidelines described in the PIR performance testing section should be followed.

These tests should answer the following questions:

- Does the sensor sensitivity decrease at higher room temperatures?
- Can the sensor be covered without generating an alarm?
- Can an intruder shield his or her body temperature from the sensor?

2.3.5.6.3 Operability Testing

Operability testing should consist of a simple walk test and tamper test on each dual-technology sensor in the system. Step tests should also be conducted to verify proper sensor operability. The step test is performed starting at likely points of entry and along paths toward protected items or areas.

For example, in position locations 1, 2, and 3 in Figure 56, operational tests are performed weekly. Locations 1 and 2 begin at likely points of entry—the door and window. Location 3 is an additional test near the door. The alarm stations are contacted before each test. The test subject remains still until the alarm station operator signals that the sensor is reset and is in the secure state. The test subject takes three steps into the room and stops. The alarm station operator verifies that the station received an alarm from the sensor at the correct location. If any of these simple tests fails to initiate an alarm, the sensor should be checked for alignment problems.

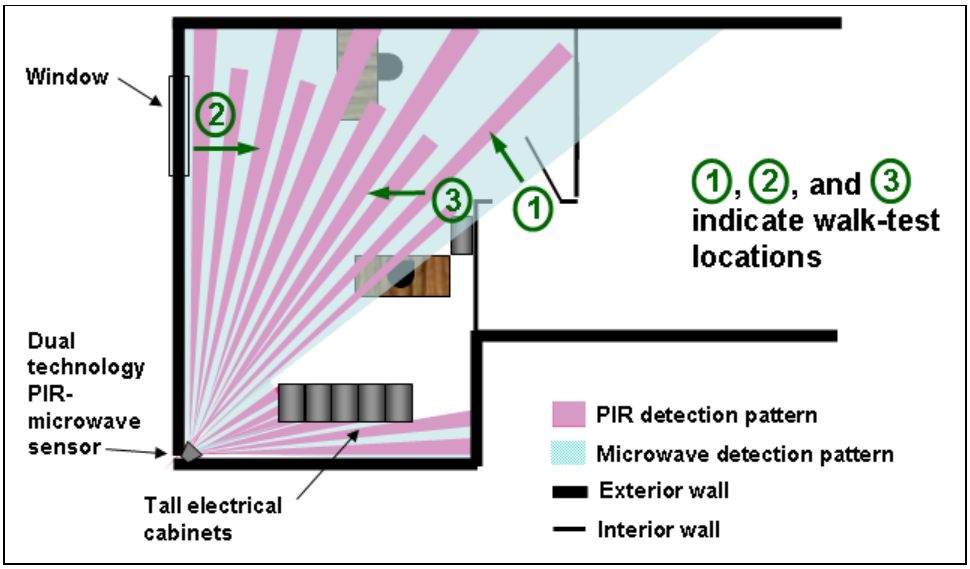


Figure 56 Walk test areas in a room covered by a dual-technology PIR-microwave sensor

Figure 56 illustrates the possible walk test locations in a room with coverage by a dual-technology PIR-microwave sensor. Note that the microwave portion of the sensor can penetrate light construction; however, because the sensor's AND gate logic requires that both sensors detect before an alarm is registered, a person in the adjoining room will not cause a nuisance alarm. In addition, note that the tall electrical cabinets block a portion of the sensor's detection pattern. This could cause a problem if the electrical cabinets are a possible target and if an intruder can hide in the location where the detection pattern is blocked.

2.3.5.7 Maintenance

The installation should be visually inspected periodically, particularly after major maintenance to the building in the sensor area. Mounting brackets and hardware should be inspected for stability and corrosion. Frequent visual inspections ensure that no blocking objects have been moved into a position that would render the sensor inoperative. Periodic tests, in addition to self-tests invoked by the sensor or the system, ensure that the sensor is operating effectively.

Standby batteries should be replaced on a conservative schedule. Every service call should be entered in a log to record the date, time, corrective action, and an assessment of the cause of the problem.

2.4 Video Motion Detection

Video motion detection (VMD) can be added to either analog or digital camera systems. VMD has been effectively implemented using daylight cameras, near-infrared (NIR) cameras, thermal imagers, and 360-degree-view cameras.

2.4.1 Video Motion Detection Systems

The primary function of a VMD system is to relieve operators from the stress of monitoring screens of closed-circuit television (CCTV) information that may not change for long periods. The VMD system will be monitoring all the cameras in its system, and reacting only when there is suspicious activity in one of the scenes. During the long periods of inactivity, the operator can continue with other tasks secure in the knowledge that the system will immediately respond to any suspicious activity. Even a moderate-sized system with eight cameras would be very difficult for an operator to monitor. If the monitors were set to sequence, activity on seven cameras would be lost for most of the time, and the system would be totally ineffective in detecting intruders. With more cameras in a system, the task of detecting intruders becomes impossible, and technology must take over the strain.

In VMD systems, the processor is continuously monitoring all the cameras in the system. During this time, the operator may select or sequence cameras using the conventional switching system. The system may include an additional monitor connected to the VMD system that will normally show a blank screen. When a camera captures an activity that the VMD system interprets as an intruder, the alarmed camera is immediately switched to the blank monitor (if used) and an alarm sounds to alert the operator. The operator immediately focuses attention on the camera covering the alarm. The detection of an intruder can also set a video recorder to real-time recording, set a matrix switching system to sequence through a specific series of cameras, or set off other such events. The operator can analyze the scene and take appropriate action.

However, an intruder could generate an alarm and be out of view of the camera before it is displayed. Therefore, the operator would see only a blank screen and not know how to react. To overcome this, VMD systems should capture, at the time of detection, an alarm image sequence containing one or more freeze frames. This may be displayed as the first view on the previously blank screen. The operator may then examine in more detail the scene at the instant the alarm annunciated.

VMD technology is best used in conjunction with other sensors. VMD developers are continually improving algorithms for use of the technology in a large range of applications. The use of VMD in interior applications has always been effective. As digital VMDs advance, they are becoming increasingly popular for use in exterior environments. VMDs can greatly reduce the time required to determine the alarm source, thereby increasing the chance of stopping the intruder. However, either overloading the operators with too much information or masking intruder movements is a concern. Masking intruder movements may involve various methods that would cause an alarm to annunciate and the respective camera to show on the monitor.

While assessing the initial alarm, the operator may not be able to act on other alarms received quickly enough to initiate a security response.

As described in the previous paragraph, VMD is best used in conjunction with other sensors. One of the newer technologies that have emerged is the combination of VMD with PIR sensors. PIR intrusion sensors detect the change in the temperature of a particular part of the viewed area, whereas VMD senses a change in the contrast within the camera scene from the normal quiescent video image. Using this combination of sensors should reduce the number of nuisance alarms because both sensors need to make a detection before an alarm initiates. Programming can allow a PIR sensor to give priority to a camera for viewing an alarm.

2.4.1.1 Principles of Operation

VMD requires the addition of hardware modules or alarm processing hardware and software, or a combination of both. The technology is modular so that it can be implemented at either the camera or at the alarm station. In one configuration, VMD software can be downloaded into specifically configured digital cameras with embedded digital signal processor (DSP) chips and memory so that the detection function occurs at the camera. When a VMD event occurs, the camera sends an alarm message to the alarm stations and then increases the frame rate of the video subsequently transmitted. Prealarm video can be stored in the digital camera's memory, and the DSP transmits it to the alarm stations when an alarm event has occurred. Many VMDs are effective for interior use because nuisance alarm sources like snow, rain, fog, and clouds are not present.

VMD technology has experienced significant advances since early 2000. Lower performing modules that provide simple movement detection are available, whereas higher performing equipment uses sophisticated algorithms to detect and categorize a moving target. With the exception of the "object-left-behind" algorithm discussed later, the VMD analysis algorithms are generally activated when movement occurs in the camera's field of view.

Early VMD equipment consisted of a module inserted into a camera's video transmission circuit. It highlighted the portion of the video image where motion was detected. Some units highlighted an area of the video image when a certain percentage of pixels in the camera's field of view changed. The simplistic video processing in these early VMD modules produced many nuisance alarms which made the technological enhancement not very usable for reliable intrusion detection purposes. Early VMD modules responded to essentially anything that moved, including insects walking on the front cover glass of the camera enclosure. As technology advanced, areas within the camera's field of view could be set as an active detection area, ignoring movement in all other viewed areas. With increased sophistication of activity-related detection algorithms, different portions of the viewed area could be activated for different detection events. For example, one area could be set to alarm on any movement while another area could be set to alarm for movement occurring from right to left, not from left to right.

In recent years, progressive VMD vendors have incorporated significant sophistication into the algorithms that analyze motion. Users can calibrate the camera's field of view with respect to object size for purposes of classification; object-type determination (i.e., human, vehicle); and speed, size, direction, and location. For example, during camera field-of-view calibration, one approach is to have a person stand in the camera's field of view at three or four locations from near-field view to far-field view. At each location, the operator calibrates the software to an individual's height and saves that height calibration information for each location for use by the detection and classification algorithms. The analysis software can then accommodate

differences in object size with respect to location in the camera's field of view and distance from the camera. A human occupies many more pixels in the camera's field of view when he or she is closer to the camera. To compensate, VMD software can scale the detection algorithm's function for identifying human movement throughout the camera's field of view.

The technology makes decisions about what is moving and the nature of the movement occurring in the camera's field of view. Once the pixel movements are identified, the pixels in movement are "blobbed together" as a group of pixels in movement. The system analyzes the blob of pixels to determine whether it falls into the classification criteria needed to generate an alarm. It then analyzes the motion, direction, and speed of motion (among other factors). If the attributes of the motion pass the algorithm analysis tests for being a valid intrusion motion, an alarm signal is transmitted to the alarm station's alarm display, and the alarm station video monitor displays the video of the intrusion event.

VMD is an electronic method used to detect a change in the field of view of a camera. In its simplest form, the system detects this change by storing one frame of the video information and then comparing the next frame with the stored frame to decide whether a change has occurred. The change detected would be a difference in the video voltage, indicating a change of brightness within the scene. The system would initially ignore this as an alarm until a further frame confirmed that a change had occurred. If the subsequent frame confirmed this as a change of brightness in the scene, an alarm would be generated. This should activate an alarm and cause the switcher to select and view the camera that detected the motion. A simple detector could be used in an environment in which all conditions were absolutely stable and the only possible change in brightness would be caused by an intruder. However, the intruder could be a mouse or a person. The system could not differentiate between the two. In addition, by the time the alarm is displayed on a monitor, the cause of it could be out of view. If the scene were being continuously recorded, the event could be reviewed; however, this review may occur too late for operators to take effective action.

As previously noted, movement is detected by measuring the changes in video level (brightness) between successive frames. If a person in a dark suit passes through a very bright scene, the change in brightness will be dramatic and immediately evident to the processor. However, a person in a grey suit in a grey scene with little contrast will cause only a small change in the brightness levels. If the sensitivity of the system were set to detect the latter event, it would be over-responsive to insignificant changes in a bright scene. This is less important for indoor systems, but it is a significant factor in external systems where large changes in light may occur. In addition, if the object is smaller than the cell, the brightness change will be a function of both the size of the object and the contrast between the object and the background. This becomes especially critical when detecting a person in the background when he or she may be only 10 percent of the screen height. The person's image may encompass only 0.25 percent of the screen area. If the person is substantially smaller than the cell, the sensitivity would have to be very high to detect this change, but it would cause many nuisance alarms for larger subjects smaller than a person, providing greater contrast.

A cell is a single detection block that is analyzed electronically for brightness changes. A cell may be a single pixel, a block of pixels, or the whole screen. A zone is a group of cells that have been defined as an active area. The next move toward reducing nuisance alarms is to build in the computing power to process each cell individually and create algorithms that will intelligently analyze certain situations. In this way, decisions can be made according to the direction of movement. For instance, one cell may be declared as a prealarm cell and another as a detection cell. Prealarm cells do not generate alarms; instead, they instruct the system to

associate detection in this area with detection in another. Activation of detection cells alone may not generate an alarm. A combination of successive detection in adjacent cells should trigger a logical action dependent on the program. For example, if a detection cell is activated after initiation of a prealarm cell, an alarm will be generated. By processing separate cells and having the power to define better algorithms, other problems can be overcome. For instance, light changes may be ignored if all cells are affected to the same extent.

In some VMD equipment software, it is possible to calibrate the alarm algorithm to allow detection of movement at the ground level to exempt movement that occurs aboveground from classification as an alarm target. This assumes that detection of an intruder either walking upright or crawling is the target of interest. However, if an intruder swinging into an area on a rope is a concern, the robustness of a VMD system's detection algorithm would have to be tested to ensure that the equipment could detect the motion of a target in particular size ranges.

Vendors have established many detection rules for their VMD hardware and software configurations. The specific rules, their functionality, and their reliability vary widely from vendor to vendor and from application to application. The licensee should thoroughly test the technology supplied by a vendor of interest in the specific applications envisioned before it commits to the installation of a particular technology.

2.4.1.2 Types of Video Motion Detection Technologies

VMD functionality is available in three configurations: (1) software running on a personal computer with video capture cards, (2) standalone single- or multiple-channel hardware/software modules, or (3) software embedded within a digital camera with an onboard DSP chip and associated memory.

The first configuration is normally at the video head end located at or near an alarm station. Either analog or digital cameras can be connected to the VMD computer, depending on a particular vendor's camera options. The second configuration can be located at either the camera or alarm station location. Either analog or digital cameras can be connected to these VMD modules. The third configuration is located within the digital cameras at the camera locations.

Some vendors have advanced VMD capabilities that include a tracking function. A movable (pan-tilt-zoom (PTZ)) camera is set to view a static scene. When alarm-generating movement is detected, the camera moves and zooms in on the target and tracks the target within the limits of the camera's movement and zoom capabilities. The function has been applied to static or preset locations in a camera tour of several fields of view, and the tracking function can be triggered at any one of the camera's tour stop locations. At least one vendor has VMD equipment with the ability to track movement while the camera is in motion. While the camera is panning, the VMD software identifies relative movement within the camera's field of view and then proceeds to track that movement.

Electrical connection of cameras to VMD equipment is simple and straightforward. Bayonet Neill-Concelman coaxial cable connectors are used to connect analog cameras to a VMD processor, whereas Ethernet connections are used to connect digital cameras to a network of high-bandwidth digital switches. High-bandwidth digital networking and trunking to support digital video transmission between camera locations and the alarm stations are beyond the scope of this discussion. However, note that in many cases, the transmission of high-bandwidth video signals is not viable using Ethernet systems designed for message transmission

(i.e., e-mail and Internet access). Specialized network configuration expertise is required for the design and installation of a digital Ethernet network to support efficient and reliable high-bandwidth video transmission.

2.4.1.3 Sources of Nuisance Alarms

Commercial VMD technologies have varying degrees of performance; however, performance testing of the technology has identified conditions that produce challenges. Indoor environments tend to produce significantly fewer challenges than outdoor environments. Large changes in lighting conditions, reflections from shiny objects, shaking cameras, out-of-focus cameras, a low-contrast scene, a target color near the same color as background, a target not occupying enough pixels in the field of view, movement of large items in the field of view (e.g., trees or large birds), heavy blowing snow, and driving rain have been identified as sources of nuisance alarms. Available equipment has a wide range of intruder detection and nuisance alarm performance attributes. Therefore, the licensee must thoroughly test the VMD equipment to ensure that the equipment performs to expectations before it purchases and installs the system.

When used indoors where environmental variables are significantly fewer, VMD technology produces fewer nuisance alarms. Indoor lighting in most locations is fairly constant throughout the day and generally the camera-to-target distance is much shorter than that encountered in outdoor applications. Cameras do not tend to shake and vibrate in indoor applications, and animals are not present to trigger alarms.

2.4.1.4 Characteristics and Applications

Combining the use of VMD with assessment cameras in indoor applications provides sensor functionality without the use of a physical sensor. VMD applications do not have the phenomenology associated with a physical sensor to create a detection alarm. The camera and VMD software do not sense the presence of an intruder within a sensored space. Software analyzes the changing attributes of a video image, and the results of that analysis determine whether an alarm condition is present. Current video analysis software only approximates a portion of the detection and assessment capability of the human mind. Although VMD software has significantly improved since 2000, it is definitely not superior to human visual acuity and cognition. However, VMD software does provide surveillance 24 hours a day, 7 days a week, to respond to predefined targets and attributes of movement within a scene. Humans do not have the capability to continuously focus on a scene for extended lengths of time. VMD technology provides continuous observation and alerts the alarm station operator, which allows a human to make the final decision regarding the presence of an intruder.

As with a physical sensor, VMD provides an indication that there is a change in the area under observation when an alarm is generated. The change creating the alarm is visual. Diagnostic information is also provided to the operator with a VMD alarm; physical sensor alarms do not provide this information. The VMD software places a box around the identified target in the assessment video to draw the operator's attention to a particular location in the video scene. The operator can then focus on the box in the video to assess what triggered the VMD alarm.

When designing for VMD sensor installation, knowledge of preferential sensitivities associated with the technology should be understood. The technology is more sensitive to movements across the camera's field of view. Movements toward or away from the camera are less sensitive to detection. Movement across the camera's field of view changes more pixels in the

image with the same amount of movement than movement toward or away from the camera. Therefore, when VMD is used as a detection sensor, the camera should view the scene such that the detection pattern is across the camera's field of view. Cameras that view scenes that experience large changes in scene illumination should not use VMD. For example, if a camera is oriented so that it views the inside of an exterior door, opening the door on a sunny day will cause a large change in scene illumination and may either cause a nuisance alarm or may not detect personnel entering through the door because of the significant perturbation presented to the classification and detection algorithms.

VMD tends to be more sensitive to black pixel and white pixel movements. Because these colors are at the extremes of the color spectrum, less decisionmaking about pixel movement is necessary than for the movement of pixels in the middle of the grey scale or with muted colors. Because of the sensitivity to white and black pixels, the scene's area of interest for VMD detection must not include an area that experiences moving shadows or moving sun glint. If VMD is applied in an area that has windows (particularly if the windows are facing east or west), the low sun angle entering the windows can cause people to cast shadows inside the building. If the area of interest includes an area where moving shadows are cast, the movement of these shadows may cause unnecessary activation of the detection and classification algorithms and create the possibility of nuisance alarms.

The use of VMD with cameras that shake or vibrate is problematic. From the VMD software's perspective, all the pixels in the camera's field of view appear to be in motion. This motion results in significant image processing and analysis. If, by chance, some patterned motion occurs within the random movement of all the pixels in motion, the detection algorithm will generate an alarm because this patterned motion appeared as "motion with purpose" in the video stream.

As described earlier, some VMD software algorithms can adapt to slow scene changes. Exterior applications where outdoor illumination in lighted areas may vary by 4 to 5 orders of magnitude, in particular, need this adaptive response. Adaptive algorithms can compensate for very slow movements. A very determined intruder could gain entry into an area by moving very slowly. In addition, some VMD systems are not sensitive to movements of pixels of a color similar to the background color. If this is the case, intruders could cloak themselves in fabric of a color similar to the background or floor and very slowly gain access.

Similarly, if a thermal imager is the video source for VMD analysis, intruders could shield themselves with highly insulating garments and then cloak themselves under another thick insulating material so that the thermal imager does not view the movement of humans because everything in the field of view of the thermal imager appears to be at the same temperature. Such cases would require complementary sensors with orthogonal detection criteria.

Performance objectives should be understood and tested on any VMD system before its procurement and installation. Testing should include a person crawling, walking, or running, or performing all three actions. These tests should be performed under the lowest expected contrast lighting condition. The following factors should be considered before selecting a VMD:

- consistent and controlled lighting (no flickering)
- camera vibration
- objects in the field of view that could cause blind areas
- moving objects (e.g., fans, curtains, and animals)
- the change in sunlight or shadows entering through windows or doors

2.4.1.5 Installation Criteria

As described in the nuisance alarm discussion above, cameras for VMD should view a detection area such that intruder movement is across the camera's field of view rather than up or down. Cameras should be installed so that they are looking at an area of interest at an angle. Mounting cameras on a ceiling so that they are looking straight down is problematic for some VMD algorithms because looking straight down at the floor causes the top and bottom of the camera's far field of view to be at the same distance from the camera. Algorithms normally expect the top of the camera's field of view to be further away from the camera than the bottom.

The background of the scene should be a neutral color rather than a very light or very dark color. A scene with a very light or very dark background color makes it easier for an intruder to blend in with the background.

Cameras for VMD sensors should be installed on solid structures that do not shake or vibrate. This minimizes the amount of computations that the VMD algorithms must make and improves the system's ability to detect an intruder.

For indoor locations, installing visible light cameras with area illumination rather than thermal imager cameras is preferable from a detection perspective.

VMD technology should not be implemented in locations where shadows move across the detection area. Because of the sensitivities of VMD detection algorithms, moving shadows in a camera's field of view can generate unnecessary alarms.

Cameras should not be installed such that they view the inside of exterior doors. Opening a door during bright sunlit days will cause large bright spots in the camera's field of view and may prevent the VMD algorithm from detecting human movement in that area.

During installation, VMD technology should be integrated with either a digital video recorder (DVR) or network video recorder (NVR) for instant playback of the alarm video. When the camera video images are processed through a VMD module or processor before they are recorded on digital media, the recorded video will be "marked up" (i.e., the recorded video will have alarm boxes around the area where the VMD camera observed movement). This markup of the recorded video allows the operator to focus on the portion of the video image where movement was detected rather than having to search for that location in the video that is not marked up. Most VMD cameras can transmit and produce images to be monitored at monitoring locations (i.e., alarm stations) within 2 seconds from detection, which is generally an acceptable standard of performance.

2.4.1.6 Testing

Testing should follow the manufacturer's recommendations. Testing a VMD sensor is very similar to testing a physical sensor. Targets of interest move through the scene at a range of speeds and at varying aspect ratios. If a human is the target of interest, target movement includes the following:

- walking and running at various speeds

- walking and crawling at normal and extremely slow speeds through a VMD camera's field of view

Tests should also include a human performing a belly crawl with a fabric cover that is approximately the same color as the background or floor.

A regular program of testing VMD sensors is imperative to maintain optimal operating order. Three types of testing must be performed at different times in the life of a VMD sensor: (1) acceptance testing, (2) performance testing, and (3) operability testing.

Alarms should be produced deliberately during all types of tests.

2.4.1.6.1 Acceptance Testing

Acceptance testing for the VMD assessment system is the most encompassing because baseline performance and operability are determined and documented. Acceptance tests will uncover operational and functionality issues that must be addressed to ensure that the system operates in accordance with design specifications. Acceptance tests should be performed to ensure that the VMD software produces alarm messages in response to tamper or defeat attempts. Use the following guidelines for acceptance tests:

Testing the Camera-to-Alarm-Station Connection

- Ensure that each camera produces a VMD video image on the monitor.

- If camera images have graphic legends displayed on the monitor, ensure that the graphic legends are labeled correctly for the VMD camera channel that is being tested.

- Ensure that VMD intrusion alarms in assessed areas trigger the appropriate camera's video to appear on the alarm station monitor. For example, while communicating with an individual in the alarm station using a two-way radio, an individual in the field triggers an intruder alarm in each VMD-sensored zone. The individual in the alarm station must ensure that the VMD video resulting from the alarm has a box around the intruder and is from the correct camera for the zone in alarm. The individual in the alarm station must also ensure that the assessment video appears on the alarm station monitor within the timeframe specified by the manufacturer (2 seconds is generally an acceptable standard) and that the playback of recorded video is from the correct camera.

Testing for the Correct Error Message by Simulating Potential Problems

- Disconnect power to individual cameras at field camera junction boxes, and ensure that a "loss of video" alarm occurs for the VMD camera disconnected.

- Cover the front of the camera enclosure with a black plastic bag or densely woven cloth, and ensure that a "loss of video contrast" alarm occurs for the VMD camera being tested.

- Shine a bright light into the front of each camera, and ensure that a "loss of video contrast" alarm occurs for the VMD camera being tested.

- Turn off the lights in the area viewed by the camera to produce a dark, low-contrast image, and ensure that a “loss of video contrast” alarm occurs for the VMD camera being tested.

- Disconnect the video signal cable from each analog camera, and ensure that a “loss of video” alarm occurs for each VMD camera channel disconnected.

- Disconnect the fiber-optic video transmission cable (fiber) for each camera, and ensure that a “loss of video” alarm occurs for the VMD camera channel disconnected.

- Physically move or rotate the VMD camera so it is no longer viewing the intended scene, and ensure that it generates an error message.

Testing for Proper Ethernet Connections

- Disconnect the Ethernet cable from each digital camera, and ensure that a “loss of video” alarm occurs for the VMD camera channel disconnected.

- Disconnect the camera Ethernet cable to Ethernet switches carrying video signals, and ensure that a “loss of video” alarm occurs for all VMD cameras connected to the switch.

- Disconnect the power cable to Ethernet switches that connect video signals to the VMD hardware, and ensure that a “loss of video” alarm occurs on all VMD camera channels connected to the switch.

Testing for Multiple Intrusion Alarms in Multiple Zones

- Simultaneously create intrusion alarms in two, three, four, and five adjacent and nonadjacent perimeter zones. Ensure that the alarm assessment video queues up the recorded (prealarm) video and that the recorded video is displayed for each of the alarming zones.

Miscellaneous Testing

- In areas with sunlight during daylight periods, ascertain that alarms are not generated as the sunlight and the shadows it creates move across the VMD-sensored area. In addition, under the same conditions, ensure that shadows created by people walking adjacent to VMD-sensored areas do not generate alarms.

- At 6-month intervals, disconnect the secondary power source operation to test the primary power source to the security system and ensure that the security system continues to function without creating detection alarms or system failure.

2.4.1.6.2 Performance Testing

Performance degradation is usually caused by changes of lower severity in the issues noted above. Usually the performance or functionality degrades, but the functionality does not cease completely. Physical changes in the baseline scene will also affect VMD performance. For example, if a piece of furniture or equipment is permanently added or removed from the scene, the baseline scene must be recalibrated to reset the detection algorithms to the new baseline condition. Some VMD software readily adapts to changes in the baseline scene over a period

of time. However, to ensure proper performance, a manual recalibration of the camera viewing the changed scene should be performed.

To optimize digital network bandwidth utilization, digital video processing at the camera generally involves video image compression. Video compression reduces scene resolution to minimize the amount of information transmitted from the camera to the alarm station. The amount of compression applied affects the amount of fine detail taken out of the video images. An application of greater than 20-percent compression begins to significantly affect fine detail in the transmitted image. Performance degradation with increased compression is noticeable initially at the camera's far field of view, and as compression is increased, the degradation begins to affect more and more of the camera's scene toward the camera. Compression causes the edges of objects to become fuzzy. Because VMD software analyzes the edges of groups of pixels in movement, compression that causes images to become fuzzy significantly complicates and degrades the functionality of the algorithm analysis.

2.4.1.6.3 Operability Testing

Camera degradation or failure, video transmission system degradation or failure, video system power or secondary power source failure, system grounding or ground loops, or lightning-induced events generally cause VMD operability issues.

Changes to the detection rules for a VMD scene or changes to the VMD calendar or time clock scheduler can also cause operability issues.

Physical changes can also affect VMD operability. Examples of these changes include an out-of-focus camera, a camera being moved from its initial VMD calibrated position, loss of scene contrast, degradation or failure of camera electronics, loss of or significant change in area illumination, or a bright light appearing in the camera's field of view.

2.4.1.7 Maintenance

Specific maintenance for VMD cameras should focus on the camera and video transmission system and should follow the manufacturer's recommendations. Because software that analyzes camera video is essentially the heart of a VMD sensor, the software will likely undergo continuous upgrades as technology advances. Therefore, the software will likely require updates during the life of the VMD camera.

The camera lens and enclosure front cover glass should be cleaned, and the lens focus should be adjusted, as necessary.

On a yearly basis, each camera's image output should be viewed at both alarm stations to ensure that the picture is clear and crisp and is not washed out or of low contrast. The absence of a clear, crisp picture would indicate degradation in the camera's electronic circuitry. For analog cameras, absence of a clear, crisp picture could indicate degradation in the video transmission network or video amplifier modules.

In addition, the tests described above should ensure that all the alarm security features are still active and operate properly.

Uninterruptible power supply batteries for modules providing backup power to the security system should be replaced at 3-year intervals.

3 WATERBORNE SENSORS

3.1 Waterborne Sensor Systems

This section provides information on waterborne sensors for facilities with water intakes (refer to Figure 57).

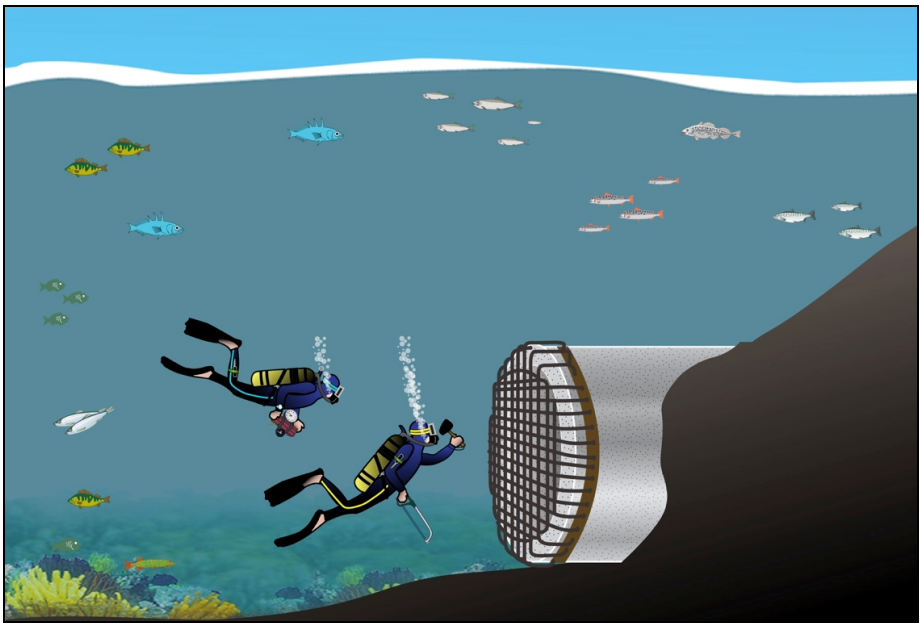


Figure 57 An example of a fiber-optic grid covering a water intake channel

3.1.1 Fiber-Optic Grid

3.1.1.1 Principles of Operation

Fiber-optic grid sensors are a commonly used application for intrusion detection in a waterborne environment. Fiber-optic grid sensors can accommodate various waterborne applications and configurations with minimal impact to the operational capabilities of the structures or systems to which they are attached. When evaluating the detection capabilities of fiber-optic grid sensors, the security industry measures quality by sensing bends and breaks in fiber-optic grids. Typical security configurations use single-mode diameter fiber illuminated with approximately 1,500-nanometer wavelength light, but any fiber diameter or signal wavelength is acceptable as long as bends and breaks can be sensed quickly (i.e., within a few seconds or less, the minimum requirement depends on the overall security system configuration). Maximum fiber length typically is a few kilometers, but some vendors claim maximum lengths of many times that length. What constitutes a “bend,” which results in signal attenuation without total signal loss, will depend on the characterization of potential nuisance alarms (e.g., a fiber run outdoors that commonly bends in a strong wind will result in more typical signal attenuation than a fiber run indoors; therefore, the sensing system should be adjusted accordingly).

Once the fiber-optic grid is arranged to ensure that an adversary must break it to enter the facility being protected, the fiber is then connected to sensing electronics. These electronics

check fiber continuity by providing an optical signal into the fiber and measuring its output on the other end to ensure that the signal is not greatly attenuated or removed altogether. Some sensing systems are capable of detecting the location in the fiber line where the event is occurring and the bend or break event itself, but this capability costs more and is often not necessary for adequate protection.

Most fiber-sensing systems will close or open a dry contact closure relay upon sensing a bend or break event, but output is adjustable depending on application needs.

Security professionals especially prefer fiber-optic cable from a tampering perspective because its modification requires very specialized tools and delicate procedures. On the other hand, electric wire typically just needs a few clips and an extra loop of wire to create enough slack to penetrate without detection.

3.1.1.2 Types of Fiber-Optic Grids

In protecting an area or surface, several vendors have had success creating fiber-optic nets, and some have embedded the fiber in a plastic or metal grate for added strength. The increased rigidity adds confidence that any break in the fiber is intentional, not accidental or caused by the environment.

A fiber-optic net can be easily wrapped around the object or surface being protected, or it can be stretched taut across an opening that needs to be controlled. Because of its flexibility, a fiber-optic net is easier to disturb and bend and, therefore, requires very little force to cause an intrusion event.

A fiber-optic grate is a rigid structure typically installed across controlled openings. Destruction of the surrounding medium almost always causes any break or bend sensed because the fiber detects that the rigid structure is being breached.

Both fiber-optic nets and grates can be treated to prevent biofouling (underwater growth, including algae, barnacles, or simple electrochemical corrosion) if they are deployed in a marine environment. Figure 58 depicts a fiber-optic grid that has been tested underwater for about 6 weeks and shows biofouling through barnacles, which can eventually degrade the integrity of the materials.

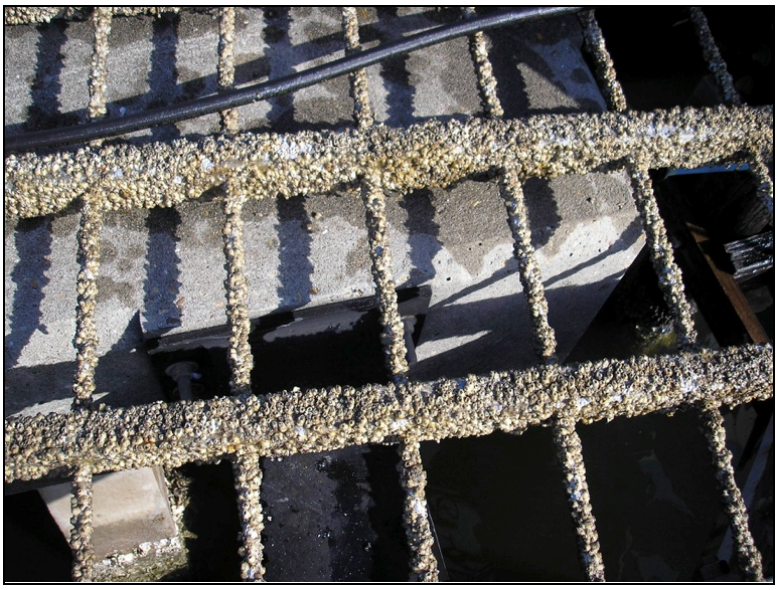


Figure 58 Example of degradation of underwater fiber-optic grid sensors

3.1.1.3 Sources of Nuisance Alarms

Of the two major types of fiber-optic grids, the more flexible fiber-optic net experiences multiple nuisance alarms in a marine environment. Marine mammals are often inquisitive and can bump the net, which results in enough signal attenuation to cause an alarm. A strong water current flowing through the net can distort it and generate an alarm. The sensing system threshold can be adjusted to allow these types of events, but such an adjustment may possibly prevent the system from sensing actual malicious bending and stretching of the net. In addition, exact characterization of marine mammal interference is difficult. Compared to the grid, the fiber-optic grate is a much more rigid structure and, therefore, is typically considered free of nuisance alarms.

3.1.1.4 Characteristics and Applications

The fiber-optic net can be used on a shaped surface that needs to be protected, an odd-shaped opening that needs to be protected quickly, or a location where weight is a major consideration. A fiber-optic net can also detect activities such as climbing and generally is more responsive than a grate to environmental influences. Fiber-optic nets work well for detection of several types of events (i.e., pushing, climbing, gathering, cutting), and a net is relatively cheap and easily replaced.

A metal or plastic fiber-optic grate creates delay (as long as an alarm is generated) and strong access denial and works where cutting is the primary activity to be sensed. Because a grate is a rigid structure, a single cut does not grant access, but it will sound an alarm, which allows operators to notice malicious activity by adversaries before they are able to pass through the barrier. A “smart fence” can tell when an intruder has broken through and can be manufactured in any reasonable size.

The following characteristics apply to fiber-optic nets:

- Nets are weaker than grates and are more vulnerable to damage in turbulent environments or in areas where heavy debris could impact them.
- Nets can be slashed, allowing swimmers to pass through the net immediately.
- Nets can create “noise” (generating frequent nuisance alarms) caused by underwater currents flowing against them or by marine mammals bumping up against them.

The following characteristics apply to fiber-optic grates:

- Grates are inflexible; therefore, if a swimmer were to cut the grate free from its support structure, it could be completely lifted away without an alarm being sensed. Adding antitamper devices can mitigate this problem.
- Metal grates can corrode quickly if they are not installed correctly (e.g., with a zinc or magnesium sacrificial bar, which must also be maintained or replaced, or both, during the life of the grate).
- Low temperatures and exposure to ultraviolet light can embrittle plastic fiber-optic grates.

The following characteristics apply to both fiber-optic nets and grates:

- Both nets and grates are susceptible to corrosion and damage through biofouling. Organisms such as barnacles could restrict waterflow.
- Both nets and grates may require regular cleaning to prevent interference from barnacles (refer to Figure 58). Anti-biofouling paints are effective against organisms adhering to the net or grate, but such paints are usually toxic to the environment.
- Both nets and grates require an assessment to confirm an alarm.
- Both nets and grates are difficult to service underwater.

3.1.1.5 Installation Criteria

Installation of a fiber-optic grid system requires the installer to work closely with the manufacturer to ensure that all potential problems are mitigated and to follow its recommendations. Installation criteria include the following:

- Install a sacrificial zinc or magnesium block on metal components.
- Test plastic material in the ultraviolet lighting conditions or temperature ranges experienced in the location where the system is to be installed.
- Use anti-biofouling coatings (if the wildlife in the area will not be affected) and determine cleaning methods and schedules.

- Add tamper-indicating conditions to ensure that the grate or net cannot be defeated without causing a tamper alarm or by being circumvented completely. For example, ensure that it is difficult to make a new opening next to a secure opening.

3.1.1.6 Testing

Testing should follow the manufacturer's recommendations. A regular program of testing fiber-optic grid sensors is imperative for maintaining optimal operating order. Three types of testing must be performed at different times in the life of a fiber-optic grid sensor: (1) acceptance testing, (2) performance testing, and (3) operability testing.

3.1.1.6.1 Acceptance Testing

Acceptance testing should answer the following questions:

- What is the vendor's prediction for long-term survivability of the grid? Although some corrosion or decay is expected over time, will the grid degrade in a timeframe that is acceptable to the facility?
- What strategies will be employed to prevent biofouling? Will the grid become overgrown with algae or barnacles?
- Could the grid be accidentally damaged, and what strategies will be used to prevent accidental damage?
- What is the projected maintenance or replacement schedule, and what are the associated costs?
- What are the tamper-indicating strategies used for the grid? Does the system generate an alarm when unplugged? Testers should simulate a disconnection instead of actually unplugging the fiber because the fiber connector ends must be cleaned before reconnection.
- What is the acceptable threshold to prevent frequent nuisance alarms? Does the system generate an alarm if the grid is rattled or hit?
- Does the grid respond to a break? Work with the manufacturer to simulate breaking the grid to generate an alarm instead of actually breaking the materials.

3.1.1.6.2 Performance Testing

Performance testing should be done regularly to ensure that the fiber-optic grid system meets performance criteria, as follows:

- Shake or hammer the grid to simulate a marine mammal or water current interference, and ensure that no alarm is generated.
- Based on the manufacturer's recommendation, simulate breaking the grid to generate an intrusion alarm instead of actually breaking the materials.

3.1.1.6.3 Operability Testing

Operability testing ensures that the fiber-optic grid system works as intended. Operability testing for fiber-optic grids involves nondestructive testing. Because cutting is the primary event to be sensed, the primary test will follow the vendor's prescribed methods to simulate cutting.

3.1.1.7 Maintenance

Maintenance should be performed according to a defined schedule. If performance or operability testing indicates degraded system performance, the maintenance schedule should be adjusted accordingly. The following maintenance is recommended (if it is not already required by the vendor):

- Clean the grid, or verify that there is no growth on the grid.
- Clear any debris from the grid.
- Check for corrosion around signal lines, connectors, and the sensor structure.

4 VIDEO ASSESSMENT

4.1 Overview

Assessment is a critical component of detection and is equally important to the initiation of response. Assessment provides a means to determine the necessary actions (responses) needed to mitigate situations that pose a challenge to physical security. The key element within the assessment process is to determine whether the alarm is due to an intruder or is a nuisance alarm. Identification also assists the security force in selecting appropriate responses within a force continuum to address security-related and potential threat situations resulting from the detected activity. Likewise, identification allows the security force to determine the absence of a threat resulting from the detected activity, such as a nuisance alarm caused by wildlife or debris. It is equally important that assessment techniques identify the stimulus that caused the alarm quickly before it disappears from view to enable a timely response that is consistent with the goals and objectives of the facility's physical protection program and protective strategy. Therefore, video assessment systems should be robust and capable of providing the highest level of protection for the specific application in which they are used.

4.1.1 Principles of Operation for Video Assessment Systems

A video alarm assessment system allows security personnel to rapidly determine, after the generation of a sensor alarm, if an intrusion has taken place within the facility. In addition to real-time observation of the location where the sensor alarm occurred, the video assessment system can record and store video of alarm events and other significant event information. This capability permits the retrieval of event images within the protected area, even under conditions of the generation of multiple simultaneous alarms or delayed security personnel attention.

The design of the video assessment system should consider the following goals:

- ability to completely assess all sensor locations
- ability to assess nuisance alarm sources
- ability to provide system response quickly (before the intruder leaves the area)

A video assessment system consists of cameras at sensored areas that display video images on monitors in the alarm stations, video switching, and recording and communication systems for transmission of the video images from the cameras to the alarm station monitors. Figures 59 and 60 show block diagrams of analog and digital alarm assessment system components. The major components of the video assessment system include the following:

- cameras and lenses to convert an optical image of an assessed scene into an electrical signal

- a lighting system to illuminate isolation zones evenly and with sufficient intensity to produce usable video images of assessed areas at night

- a video transmission system that connects the cameras to the alarm station switchers and monitors

- a video switching system that takes the video from cameras and routes it to recording and monitoring display devices
- a video recording system that records video from camera feeds for archival needs or for the recording of alarm events
- video monitors for the display of alarm assessment video
- an alarm communication and display (AC&D) controller to interface between the alarm sensor system and the video alarm assessment system to display video in the alarm stations when a detection sensor detects activity and generates an alarm

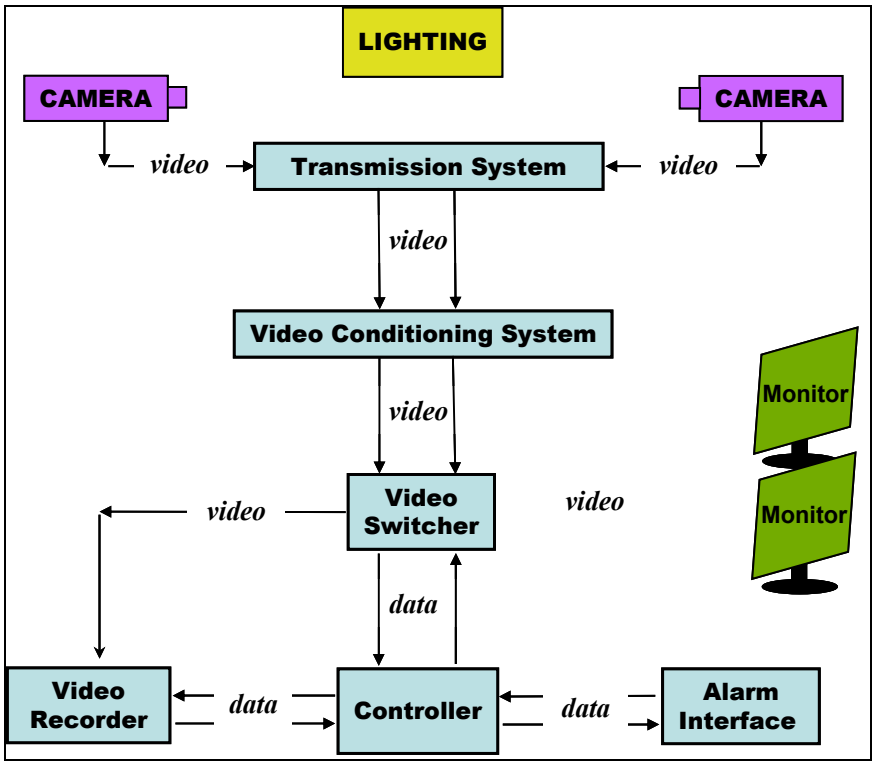


Figure 59 Diagram of an analog video system

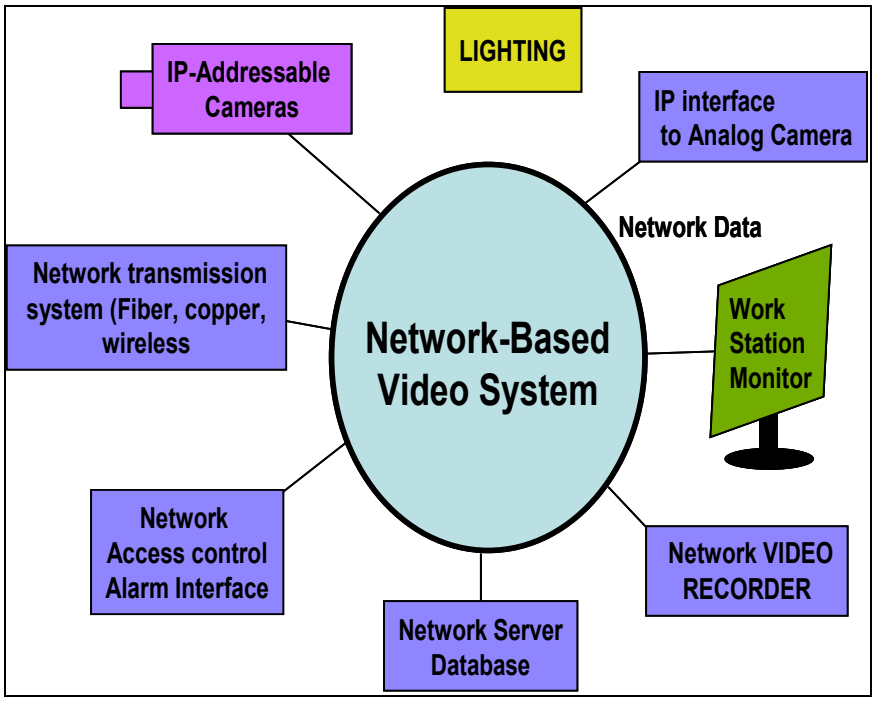


Figure 60 Diagram of a network-based digital video system

A camera converts the physical scene in the field of view of the camera into an electrical signal suitable for transmission over cable, fiber, or wireless media to a video monitor for viewing by an observer and digital video recording for playback and archival information. The video switcher directs the signal to a selected monitor for display of the visual scene observed by the camera. A selected signal can also be routed by the video switcher to and from a video recorder for playback of prealarm and postalarm video and for permanent archiving and forensic analysis.

The resolution, sensitivity, lens field of view, and aperture of the camera should be considered during the design of exterior perimeter isolation zone lengths and widths. Each video assessment system aspect should be considered individually and within a system. If assessments need to be made from recorded data, the resolution of the recording device should be considered. To compensate for reduced playback resolution of the video recorder, reductions in the spacing between cameras and maximum-assessed area lengths may be necessary. The video recording and storage device may be the resolution-limiting factor in the assessment system. If video information must be retrieved from an archived recording, the system design should consider the resolution of the archived recorder.

The installation of additional assessment cameras, associated circuitry, and hardware is necessary if sensor zones must be shortened because of terrain variations or locations of personnel access points. Each sensor zone should be evaluated individually to ensure that appropriate assessment equipment is installed and assigned to ensure optimal performance of assessment capabilities within the isolation zone. It is more beneficial to install multiple assessment cameras in an extremely long sensor zone than to risk a reduced or limited assessment capability and, therefore, reduce the overall level of protection given by the intrusion detection and assessment system. Sensor zone width also has an effect on the maximum assessment zone length; narrower widths allow assessment of longer zones.

Most of the head-end video assessment equipment can be located in or near an alarm station for convenience, a temperature-controlled environment, and an easily accessible area for maintenance. Normally, only the cameras, towers, power supplies, video transmission equipment, and signal transmission media are located external to the alarm stations.

4.1.2 How Lighting Affects Camera Sensitivity and Resolution

The design of the lighting system must consider the camera's sensitivity. A high-resolution camera will not function properly if the illumination is inadequate. These determinations must consider the relative aperture of the lens (i.e., f-stop). Generally, faster lens speeds (lower f-number) are selected when more than one option is available, even if a lens with a lower f-number is somewhat more expensive. Lenses with f-numbers higher than f/1.8 should not be used except under very unusual circumstances. Lenses with f-numbers higher than f/1.8 will require increased lighting levels or a more sensitive camera.

A camera's sensitivity or performance under low light conditions often cannot be determined from the manufacturers' specifications alone because a common standard does not exist. Some manufacturers reference scene illumination levels or illumination levels at the camera's imager that do not represent the camera's performance in security applications in which a lens and its aperture affect the amount of light appearing on the camera's imager. These variant light levels are subjective and do not allow performance comparisons. A side-by-side evaluation of cameras operating in the intended environment is the preferred method for determining whether a camera is suitable for assessing a particular area.

For a scene to be visible to the camera, it must be illuminated by sufficient natural or artificial light and must reflect a portion of that illumination for observation by the camera through a lens with appropriate field of view for assessment purposes. The light reaching the lens must then be clearly focused onto the camera's light-sensitive imager surface and converted into an electrical signal by the camera electronics system for transmission to the alarm stations.

4.1.3 Concepts of Cameras Used in Video Assessment Systems

Assessment cameras are most efficient when a smaller camera imager size and longer focal length lenses are used. To the extent that these factors can be optimized, the number of cameras, towers, and components of the camera subsystem infrastructure video transmission system can be minimized. Longer focal length lenses have narrower fields of view. This minimizes the amount of area outside the perimeter being viewed. In some circumstances, assessment cameras can view more than one sensor zone. If a video assessment system is judiciously designed, when a camera outage occurs in one zone, the camera in the adjacent zone should have the capability to assess the neighboring zone until its camera is operational again.

Alarm assessment using video technology uses cameras and lenses installed in camera enclosures and accessory equipment to create video images for an operator to observe in a facility's central alarm station (CAS) or secondary alarm station (SAS). Cameras are manufactured to widely varying requirements, performance standards, quality levels, and reliability.

Analog security cameras, an offshoot of broadcast television technology, are designed to provide a video output signal that is almost identical to that of an analog television camera. Currently, many analog camera vendors offer a large range of camera technologies at widely varying prices. As camera technology advanced, the digital video camera became available.

Many digital cameras are available to implement assessment systems using digital camera technology and digital video transmission systems.

A transmission media coaxial cable or fiber-optic cable carries the camera's electrical video signal to the alarm stations where it is displayed on a video monitor for viewing by an operator. Analog cameras produce an analog output signal in a specified format for viewing on a picture tube-type monitor or a flat screen digital monitor. Digital cameras are connected to a computer network and provide a signal to the alarm stations through the network via a stream of digital packets similar to the process that produces video on a desktop computer.

4.1.4 Testing Video Assessment Systems

The sections below discuss testing information that should be approached from a systems point of view. The sections address several kinds of testing, including acceptance, operational, and performance; integrating cameras; DVRs; lighting; and system elements. Testing should follow the manufacturer's recommendations.

4.2 Video Assessment Systems

4.2.1 Cameras

4.2.1.1 Principles of Operation

Depending on the specific camera imager technology implemented, camera imagers respond to visible and NIR illumination or thermal signatures of targets within the camera's field of view. Camera placement depends on appropriate lens selection to adequately assess a defined area, zone, or sector. The detection sensor area and the camera field-of-view area must be coincident. If a camera's field of view does not completely encompass a sensor's detection area, additional cameras must be deployed to ensure that the video assessment system can observe all of the detection area. Similar to a motion picture format, a video picture comprises 30 still pictures per second taken in succession compared to 24 still pictures per second taken in succession in motion pictures. Each picture is called a frame.

Cameras have six distinct categories: (1) black and white, (2) color, (3) day/night, (4) infrared and infrared enhanced black and white, (5) intensified, and (6) thermal. Cameras with different technologies can be used together to provide a wide assessment capability for specific applications. This is particularly true when assessment must be performed in extremely low light conditions of less than 0.01 foot-candle (f-c, 0.1 lux). For example, in unlit areas, a color camera can be used during the day, and a thermal imager camera can be used at night.

The heart of a camera is a solid-state imager. The imager has a pixel array that converts light energy to an electronic charge. Factors such as resolution, sensitivity, color versus black and white, and infrared or thermal spectrum sensitivity affect the performance of imager technology. The resolution of a quality analog color camera is approximately 470 lines. The resolution of a quality analog black and white camera is approximately 570 lines. Digital cameras have 520 to 4,000 lines of resolution. Infrared-enhanced camera imagers can provide video images appropriate for video assessment with low-power infrared illuminators. Thermal imagers have a range of 160 to 480 lines of resolution.

4.2.1.1.1 Camera Resolution

Resolution is the degree to which one can see fine detail in a viewed image. It is also a measure of spatial frequency or the number of pairs of alternate, evenly sized black and white lines that can be seen at a given linear distance (typically expressed in line pairs per millimeter). The line pairs designation is used primarily in the field of optics, but the term also appears in television literature. Different camera resolution charts have been developed for color and for black and white cameras (refer to Figure 61). Camera resolution is measured using a resolution chart that arranges groups of equally spaced black and white lines in a wedge-shaped pattern; these groups form the basis for resolution measurement.

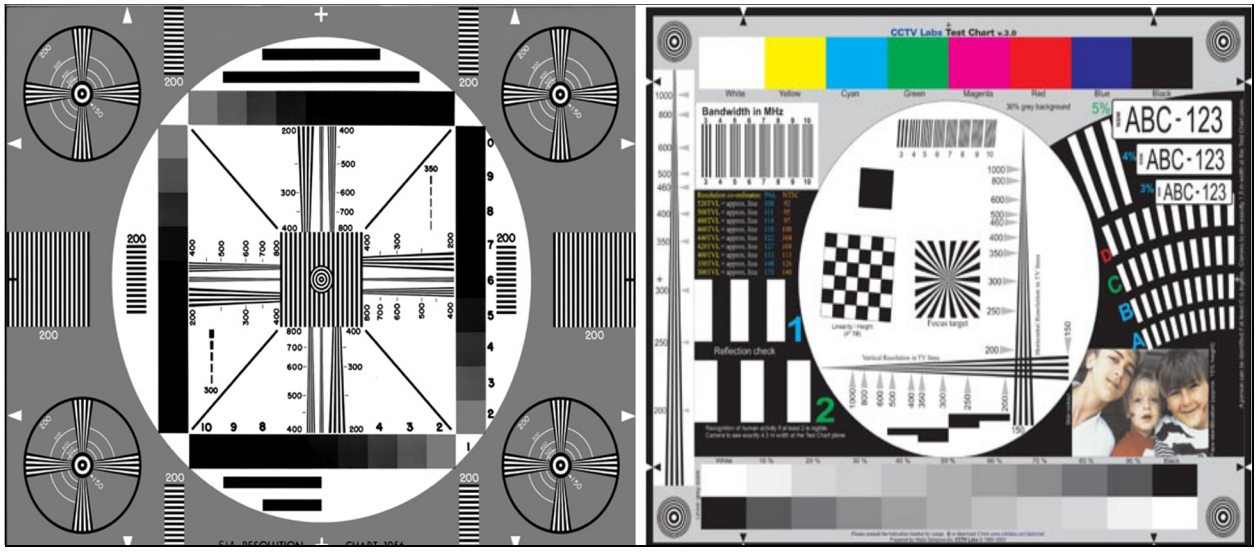


Figure 61 Examples of laboratory black and white and color camera resolution charts (graphic courtesy of CCTV Labs, available at www.cctvlabs.com)

As shown in the left picture, the chart is normally calibrated for horizontal resolution between 200 and 1,600 horizontal television lines (HTVL). The units of measure are stated as either HTVL or vertical television lines. Vertical resolution is fixed by the scan rate. Figure 61 shows a color camera resolution chart at the right.

As horizontal resolution increases, finer detail can be observed in the image. To determine camera resolution, a camera is positioned so that it views the full chart with no background visible (refer to Figure 62). When positioned correctly, the arrows at the edge of the resolution chart align with the edge of the monitor viewing area. Observing the video monitor, at some point along the vertical converging black and white lines, the lines merge. At this point, four distinct black and white transitions can no longer be discerned. The point at which the lines barely appear separate is the horizontal resolution. The resolution in HTVL is read from the numbers on the chart. For example, if four distinct lines are no longer visible at a point a quarter of the way between the 500- and 600-line calibration points, the camera would have a 525-line horizontal resolution. Figure 63 shows examples of field resolution charts; the Rotakin chart is shown on the right (Rotakin is a registered trademark of the Home Office in the United Kingdom).

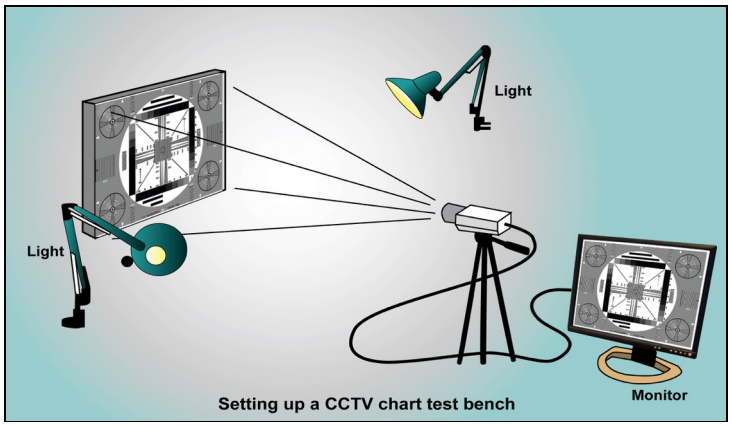


Figure 62 Example of a resolution chart test setup

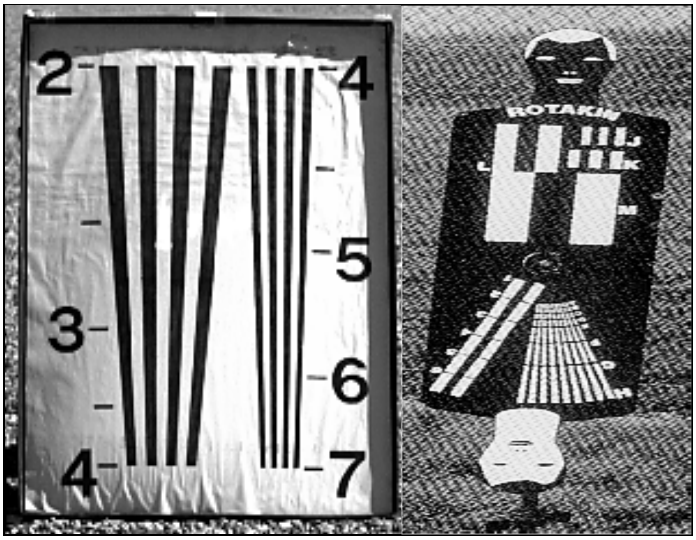


Figure 63 Examples of field resolution charts

As a point of reference for real-time assessment, the horizontal resolution of a good quality video camera is about 800 pixels. Historically, 1 percent (or 8 pixels per foot) of horizontal object resolution has been used as a basis for the resolution needed for intruder classification. This indicates that the maximum horizontal field of view should be limited to 30.5 meters (100 feet). Object resolution specification in pixels per foot must encompass all of the camera-to-monitor elements (e.g., camera, lens, transmission system, video recorder, and monitor) to determine the end-to-end resolution of the video assessment system.

For purposes of alarm assessment, the following three levels of resolution need to be considered:

(1) Detection. The ability to detect that an object is present in the camera's field of view but not to exactly identify the object (refer to Figure 64).

(2) Classification. The ability to determine whether the object in the camera's field of view is human or nonhuman (refer to Figure 65).

(3) Identification. The ability to determine the unique identity of the human in the camera's field of view based on details of appearance (refer to Figure 66).

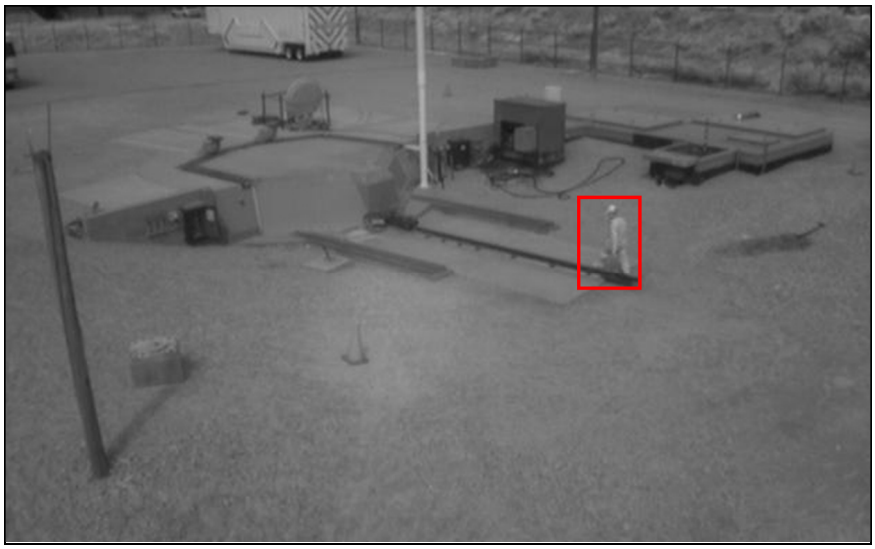


Figure 64 Example of video image showing detection

Figure 65 Example of video image showing classification

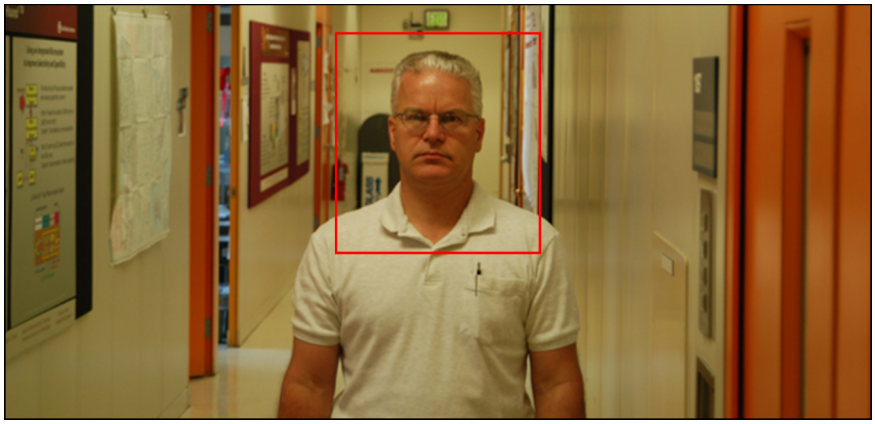


Figure 66 Example of video image showing identification

These three levels of resolution depend on the camera's resolution and the size and proximity of the object to the camera. For example, depending on camera resolution, object size, and object distance from the camera, it may be possible to identify a particular person, classify an object, or detect an object the size of a small animal. Consideration of the object or assessment target is critical in determining camera placement and the number of cameras required. In an exterior perimeter situation, a security system operator may need to classify an intruder crawling slowly through an assessment zone at night. The crawling intruder could be close to the camera or at the camera's far field of view.

The distance from the camera to the assessed area's far field of view is limited by a design criterion requiring that a specified number of lines of resolution (and thus a number of horizontal imager pixels) are occupied by a certain sized target. The amount of resolution required is determined by the level of assessment needed at a particular camera location. When assessment requirements change from intrusion detection to classification and then to intruder identification, the number of lines or pixels that a target must occupy on a video monitor screen increases.

Table 1 shows the number of horizontal pixels that are required for the three levels of assessment. In high-resolution camera imagers, the relationship between pixels and HTVL is 0.75. For example, 8 horizontal pixels on a 1-foot target are recommended for the assessment classification of a human intruder. From above, 8 pixels equal 6 HTVL on a 1-foot target. With 8 pixels or 6 HTVL on a 1-foot target at the camera's far field of view, the resultant picture quality allows the security system operator to be able to recognize and discriminate between human and animal.

Table 1 Assessment Type and Required Pixels

Assessment Type	Pixels
Detection	2 to 3
Classification	6 to 9
Identification	10 to 16

Distance from the camera, camera resolution, lighting, and other video assessment system performance characteristics contribute to how easily and quickly an operator can assess a situation. For exterior perimeter applications, having a camera resolution that allows an operator to classify a target is most likely sufficient for differentiating between an adversary attack (e.g., crawling intruders) or a nuisance alarm (e.g., an animal). At the other extreme, for some interior applications, it may be desirable to uniquely identify a human in the camera's field of view.

4.2.1.1.2 Imager Format

The camera's format designator is based on the size, or format, of the image device. The camera format is related to the size of the photosensitive surface and is a measure of the diagonal of the scanned rectangular area.

As shown in Table 2, common imager formats today are in inches. The inch measurement is a carryover from tube image cameras and relates to tube diameter, not the actual measurement of the diagonal of the imager. Early analog video cameras had 1-inch-diameter tube-type imagers. A 1-inch tube-type imager had a 16-millimeter (0.63-inch) active area. When solid-state imagers were manufactured, the sizing convention continued so that an imager with

a 16-millimeter diameter and 12.8-millimeter horizontal dimension was referred to as a 1-inch imager. Subsequently, as smaller imagers were produced, the imager format size relationship continued with the existing solid-state sizing convention.

The ratio of the imager width to height is called the aspect ratio. Standard video camera imagers have a 4:3 horizontal-to-vertical size (aspect) ratio that represents two sides of a 3-4-5 triangle. The vertical dimension is 0.75 times the horizontal dimension, and the diagonal is 1.25 times the horizontal dimension. Imagers for high-definition television cameras have a 16:9 horizontal-to-vertical size ratio where the vertical dimension is 0.5625 times the horizontal dimension, and the diagonal is 1.1475 times the horizontal dimension.

Table 2 Imager Formats, Converting Inches to Millimeters

Stated Format	Active Area	Imager Size (H x W)
1 inch =	16 mm diameter =	9.6 mm x 12.8 mm
2/3 inch =	11 mm diameter =	6.6 mm x 8.8 mm
1/2 inch =	8 mm diameter =	4.8 mm x 6.4 mm
1/3 inch =	6 mm diameter =	3.6 mm x 4.8 mm
1/4 inch =	4 mm diameter =	2.4 mm x 3.2 mm
1/6 inch =	3 mm diameter =	1.8 mm x 2.4 mm
1/8 inch =	2 mm diameter =	1.2 mm x 1.6 mm

4.2.1.1.3 Scene Contrast

Video image contrast relates to the difference between the white and black video signal levels in a picture image. High contrast indicates a large difference between the white and black levels, whereas low contrast indicates a small difference between the white and black levels. A low-contrast video image appears as shades of the same color hue. Figure 67 shows examples of high-contrast (left) and low-contrast (right) video scenes.

Figure 67 Examples of high- and low-contrast scenes

4.2.1.1.4 Sensitivity

The sensitivity of a video camera can be defined as the minimum amount of illumination required to produce a specified output signal. The following factors are involved in producing a video signal:

- illumination level of the scene
- color spectral distribution of the illuminating source
- object reflectance
- total scene reflectance
- camera lens aperture
- camera lens transmittance
- spectral response of the camera imager
- video amplifier gain, bandwidth, and signal-to-noise ratio (SNR)
- electronic processing circuitry

Camera sensitivity may also be expressed as scene illumination or the level of imager illumination that will produce a minimally acceptable video image. Normally, camera sensitivity is stated in units of lux or foot-candles. For practical purposes, experts in the field define camera sensitivity as the illumination level that produces a 60-percent reduction in camera output. Although usable camera video can be observed at levels below a 40-percent signal level, further reduction beyond 40 percent increases the amount of video signal noise and picture graininess.

Table 3 lists the reproduction from a camera specification page showing a light-sensitivity specification.

Table 3 Light-Sensitivity Specifications

Sensitivity	Full Spectrum	With Infrared Filter
Full Video, No Automatic Gain Control (AGC)	0.039 f-c (0.39 lux)	0.15 f-c (1.5 lux)
80% Video, AGC on	0.001 f-c (0.01 lux)	0.006 f-c (0.06 lux)
30% Video, AGC on	0.0002 f-c (0.002 lux)	0.0009 f-c (0.009 lux)

4.2.1.1.5 Signal-to-Noise Ratio

Camera SNR is the strength of video signal above the electronic noise level created by the camera's electronic signal processing circuits. A camera's SNR is expressed in decibels; the higher the SNR, the better the rating. With low SNR, the picture can appear grainy or snowy, and sparkles of color may be noticeable. Noisy video produces poor-quality pictures. A good camera SNR is 50 decibels or higher.

4.2.1.1.6 Automatic Gain Control

AGC is an electronic circuit in the camera that maintains a preset video output signal by increasing electronic amplification of the video signal for low-illumination scene conditions. The motor-operated automatic iris lens system controls the amount of light reaching the camera's imager. The camera's output video signal amplitude is monitored either externally by a circuit in the lens assembly or internally within the camera, and an iris-control drive signal is created to maintain the amplitude at some predetermined output level. As the video level decreases

(meaning that not enough illumination is reaching the camera's imager), the auto-iris lens is driven to increase the size of the aperture. Eventually, the iris is driven fully open, and further decreases in light level result in a reduced-amplitude video signal. At this point, the electronic amplification is increased. As the light level is reduced even further, the improvement caused by electronic signal amplification is exhausted, and a very grainy picture is presented. To prevent grainy pictures, some cameras have a cutoff circuit that causes the camera to produce no output when graininess of the picture exceeds a certain threshold.

4.2.1.2 Types of Cameras

This section discusses camera technologies for use in video assessment applications. Topics cover generic camera classifications such as color, black and white, thermal, and technical attributes of some cameras such as automatic shutter, automatic iris, and integrating cameras.

4.2.1.2.1 Color and Black and White Cameras

Although a color camera enhances daylight scenes by providing additional color information about the target being assessed, the nighttime use of color cameras, particularly when a scene is illuminated with high-pressure sodium (HPS) lamps, can be problematic. Security perimeter field tests of color cameras with HPS lights have not been favorable. At night, HPS lamps cause a gold-orange color to appear on monitor images (e.g., a perimeter floor composed of light-grey, rounded river stones appears orange). At maximum distances, it is difficult to distinguish an intruder's exact clothing color under the varying lighting conditions encountered in locations illuminated with HPS lamps. To the human eye, HPS illumination can distort naturally occurring color cues.

When comparing color and black and white cameras with the same type of camera imager, color camera resolution is about 18 percent less than that of an equivalent black and white camera imager. The black and white camera provides a brighter, sharper, higher contrast image at night because of its higher resolution and operation only in the grey scale. (See Section 4.2.1.2.2 for a further discussion.)

4.2.1.2.2 Day/Night Cameras

Some cameras produce color images during the day and black and white images at night, thus taking advantage of the best features of both. The camera has a sensor that measures the ambient light level to control switching from day to night mode. On some cameras, the ambient light level at which the switchover occurs can be adjusted. The camera electronics monitor the output video level and switches from color to black and white when the scene illumination level is less than a predetermined level. When transitioning from day to night mode (color to black and white), the camera mechanically removes an NIR filter. When the camera is in black and white mode, it responds to NIR illumination, which is blocked by a filter during the day. Removing the filter also improves picture brightness. This increases the amount of scene illumination reaching the camera imager. The nighttime black and white image has approximately 18 percent more resolution than that of the daytime color image.

4.2.1.2.3 Electronic Shutter Cameras

The pixels in camera imagers can be compared to electronic capacitors. Instead of accumulating electrical charge as capacitors do, camera imager pixels accumulate light charges over an active charging time and then send that charge information to be processed into a

complex electronic signal for the monitor to display. Some cameras adjust the amount of time that the camera imager is allowed to be exposed to a scene for producing a frame of video. These cameras have electronics that automatically adjust the amount of imager exposure time as a function of scene illumination level. Exposure time is very short during sunny environments and is lengthened in darker night environments.

4.2.1.2.4 Integrating Cameras

When scene illumination is too low and grainy pictures occur, some camera models can increase the time over which camera imagers are exposed to the scene. Known as integrating cameras, the length of time that the imager is allowed to be exposed to incoming illumination is increased to make the image brighter and improve scene contrast. These cameras slow the shutter speed to greater than one-thirtieth of a second when viewing very dark scenes to obtain enough scene illumination to produce a picture with sufficient contrast for assessment purposes. Some cameras can slow the shutter speed to as long as 4 seconds, but that length of time between frames is too long for adequate assessment. Integrating light for longer periods of time causes moving images to become blurred. For accurate assessment, the shutter speed should not exceed one-fourth of a second. An intruder running a 4-minute mile will traverse 1.7 meters (5.5 feet) in one-fourth of a second.

4.2.1.2.5 Intensified Low-Light Cameras

In a camera that has an intensifier component, photons are linearly accelerated and bombard a luminescent (green) screen. A color camera is focused on the green screen to create the displayed video signal. The intensifier responds to NIR illumination from stars, the moon, and artificial lighting. These passive cameras are only light receivers and do not emit NIR energy to illuminate the scene. The intensifier requires replacement and maintenance and has a limited life on the order of 2,500 to 3,500 hours of operation. Bright light sources in the scene can create washout smears or streaking in the camera image.

4.2.1.2.6 Thermal Imager Cameras

The thermal imager camera converts thermal radiance to a video signal. Its camera video output can be a black and white image showing the temperatures of objects as shades of grey or in a gradation of colors calibrated to temperature bands. Thermal camera imagers have resistive element pixels that respond to thermal/infrared energy in the 3- to 5-micron or 7- to 14-micron waveband emitted from warm-bodied sources. A thermal camera is a night vision device that responds to differences in temperatures against a background temperature reference. A thermal camera is a passive device and requires no illumination to produce a video image. The picture displayed is based on the difference in the temperature of objects in the scene. Cooled thermal imager cameras typically use nitrogen cooling loop Sterling pumps. The advantage of cooled thermal imagers is that they have higher sensitivity to small changes in temperature. However, the Sterling pumps must be replaced at 10,000- to 15,000-hour intervals.

4.2.1.2.7 Pan-Tilt-Zoom Camera

The PTZ camera provides alarm station operators a level of versatility in performing surveillance tasks that is not possible with the use of fixed cameras. With a PTZ camera, the operator can rotate the camera over a 360-degree field of view, move the camera up and down, and zoom in to more closely observe activities of interest. PTZ cameras come in a range of mechanical

configurations, including an exterior-mount, dome-type camera; an exterior-mount camera configuration with fixed cameras mounted on an integrated pan-tilt mechanism (lenses can be fixed or zoom); an enclosed, ceiling-mount dome indoor camera; and a nonenclosed indoor camera.

4.2.1.3 Sources of Nuisance Alarms

Sources of nuisance alarms do not apply to this discussion.

4.2.1.4 Characteristics and Applications

Several camera characteristics enhance a camera's ability to provide reliable assessment images over varying environmental conditions. These characteristics include the following:

- High sensitivity can provide the brightest and highest contrast video image under widely varying lighting conditions.
- Automatic gain control, automatic iris control, or automatic shutter control circuits maintain video image quality over a range of day and night lighting conditions. These features maintain good picture quality while bright lights (e.g., vehicle headlights) are in the scene's field of view. The imager's persistence is short enough to preclude image smearing during movement, and the image does not have a washout streak above and below a bright light in the camera's field of view.
- A history of reliability, durability, and resistance to environmental weather effects is a good indicator of the camera's future reliability.

4.2.1.4.1 Exterior Cameras

Exterior cameras should be mounted on stable towers and mounts to avoid motion or movement of the camera in the wind. A wire frame tri-pole tower (instead of a wooden pole) is unaffected by varying weather conditions.

Exterior cameras should be mounted at heights of 7.6 to 9.1 meters (25 to 30 feet) above the assessment area surface. The cameras should be tilted down to view the entire assessment area. On flat perimeter surfaces, camera downward tilting on the order of 2 to 5 degrees is recommended. With the cameras tilted down, the horizon is not in the camera's field of view, and glare at sunrise and sunset is reduced. In addition, the downward tilt reduces snow and ice impingement on the front cover glass of the camera's enclosure, particularly if the enclosure is covered with a sunshield. Exterior lighting luminaires should be at least 3 meters (10 feet) higher than the cameras. For example, if the cameras are mounted on top of 9.1-meter (30-foot) towers, lighting luminaires should be affixed to poles that place them at least 12.2 meters (40 feet) above the ground. All camera systems, associated power supplies, and connections should be protected from unauthorized external manipulation or tampering.

4.2.1.4.2 Camera Enclosures

Exterior cameras require environmental enclosures to protect cameras from outdoor temperature extremes, dust, dirt, humidity, wind, rain, and snow. The enclosures must be large enough to contain the camera, lens assembly, power supply, and (possibly) camera communication modules. The following describes two types of environmental enclosures:

(1) An integral environmental enclosure is normally cylindrical in shape and has an O-ring-sealed cover glass and rear cover. The enclosure is of rigid construction, can be pressurized with dry nitrogen, and has integral front-cover glass heaters. A sunshade protects the camera enclosure from high summer temperatures by shading the enclosure and providing a cover for the front cover glass of the enclosure.

(2) A sheet metal, formed metal, or fiberglass enclosure allows camera access through a clamshell-type cover (like the hood on a car). The cover is either hinged or removable and cannot be pressurized. The large sealing surface and enclosure manufacturing techniques normally do not provide for a dust-tight seal. The primary advantage of the clamshell-type enclosure is for ease of accessibility for camera/lens replacement and for ease of lens focus adjustment.

Accessories for exterior enclosures include heaters, insulation material, fans, defrosters, and front-cover glass washers and wipers. Washers and wipers tend to be high-maintenance items with the need for frequent washer solution and wiper blade replacement.

4.2.1.4.3 Pan-Tilt-Zoom Cameras

In addition to fixed alarm-assessment cameras, PTZ cameras have been installed in facilities as an added capability for tactical surveillance. These cameras require controller electronics and an operator joystick control to facilitate camera movements. Although PTZ cameras are not recommended for the assessment of an alarm, they are effective for monitoring temporary operations such as a construction crew working near a fence line. They can also be used as a means to facilitate a compensatory measure in the event of an assessment camera outage. A PTZ camera with the joystick control locked out can be positioned to view the area covered by a defective fixed camera.

4.2.1.4.4 Additional Considerations for Cameras

Positional errors in camera placement, mismatches in expected and actual resolution, overt or covert tampering, environmental conditions, and overall system response time can inhibit the capabilities of cameras. Section 4.2.1.1.1 describes the relationship between expected camera resolution and actual need. For example, if the security objective is to identify the target and if the chosen camera resolution can only detect the target, the camera and lens installed at that location are inappropriate for the application.

Covert video signal tampering can be accomplished in analog camera systems by tapping into video transmission cables and inserting a recorded scene or by switching video feeds to show video from the wrong zone. Overt tampering includes the following:

- using a bright light or laser to blind the camera
- covering the camera
- shooting the camera lens or enclosure cover glass with a paint gun
- cutting video transmission cables
- destroying the camera to make it nonfunctional

Placing a camera in an unprotected area could lead to undetected camera tampering and attack on the camera's video transmission infrastructure. Further, the camera tower could also be used to enable egress across a perimeter, which would circumvent detection by ground-based sensors.

Changing environmental conditions such as rain, fog, or blowing snow can be sources of video assessment system weaknesses. These conditions can cause the loss of usable images and, therefore, require the implementation of contingency plans to provide an alternate form of alarm assessment such as dispatching patrols to the area.

When designing an IDS, the design should consider the sensored areas and the video assessment of those areas together so that the detection area as a whole can be assessed. The design should ensure that there are no locations in the sensor detection area where an intruder could hide to avoid camera assessment. Cameras, mounts, and towers should be placed so that they do not interfere with or compromise sensor performance. Camera towers should not be placed so close to the sensor detection area or volume that they create nuisance alarms, decrease sensor sensitivity, or be used by the intruder as a climbing aid to bridge a sensor's detection zone. In multiple sensor configurations, the assessment camera should be able to view the combined sensored areas and volumes and all of the hardware (e.g., junction boxes or field data panels) associated with the sensor. Sensor hardware should not be large enough to provide a convenient hiding place for intruders in video assessment areas.

Wooden poles are not recommended because they will dry out and twist over time. To compensate for the twisting action of wood, cameras must be repositioned from time to time to maintain the proper view of the area to be assessed.

Video assessment in shadows surrounded by bright sunlight creates significant problems because of the high scene dynamic range in brightness levels. In these circumstances, a compromise must be made to select the area of prime interest and to ignore the unresolved areas.

If exterior cameras are positioned so that the horizon is in the camera's field of view, it is possible (particularly for east- and west-facing cameras) for the rising or setting sun to be in the camera's field of view, blinding the camera and allowing an adversary to enter the perimeter without being adequately assessed. Similarly, interior cameras with lights in the camera's field of view can experience a glare or bright spots that will wash out usable images. In addition, a camera focused under one light level and operated under a different light level or with a different lens mount or format will result in improper focus. Exterior cameras should be focused with the iris fully open at dusk to obtain optimum focus through the entire depth of field. Incorrect camera placement or lens selection can result in a horizontal field of view that is too narrow for the near field or insufficient to see an intruder or other target at the end of the assessment zone.

Outdoor cameras should be installed so that no light sources are in the camera's field of view. Direct light can cause image "blooming" or allow the automatic iris lens to close and reduce the amount of light allowed through the lens. Possible light sources include perimeter lighting, sunlight, exterior lighting on buildings, car headlights, and shiny objects that reflect light. Cameras should never be aimed such that the horizon and sky are in the camera's field of view. Because a camera is a light-averaging device, images of the ground surface (particularly at low sun angles such as at sunrise and sunset) tend to be darker and therefore harder to assess. Considerable care must be taken because camera blinding from unexpected light sources is difficult to predict before installation and is one of the most frequent problems encountered after the installation of the equipment. Illumination sources in a camera's field of view may have to be shielded or reoriented to prevent the creation of a bright spot in the camera's field of view. Perimeter isolation zones adjacent to a roadway can also be problematic. Reflections from vehicle headlights and tail lights from a roadway surface can affect the assessment capability of the alarm.

A PTZ camera should not be used for alarm assessment because of timing, reliability, and operational issues. PTZ cameras may compromise effective, timely alarm assessment and can also be pointed at the wrong location or zoomed such that part of the area to be assessed is not in the camera's field of view. Only fixed cameras with fixed or manually adjustable zoom lenses should be used for alarm assessment. This provides prealarm and postalarm video of the entire assessed zone. A PTZ camera should be used only for tactical surveillance as an added feature to augment alarm assessment cameras or for backup in case the primary camera fails.

4.2.1.5 Installation Criteria

The following considerations for camera selection are listed in order of priority:

- The main consideration in camera selection is the sensitivity required for a full-video output signal for the lighting environment in the area to be assessed. To meet the desired or required performance capabilities, the sensitivity must match the lighting design goals regardless of the imager.

- The resolution of the imager determines the number of cameras required for a given straight-line perimeter section. The greater the resolution, the greater the spacing can be between cameras. The object resolution required should be determined before a camera is selected, but in practice, the desired object resolution may be slightly modified when camera choices are limited.

- Camera format is an important consideration in the selection process. The requirements of nonstandard-sized focal length lenses should be carefully considered and evaluated before choosing a format.

- During the selection process, camera evaluation should consider the nighttime lighting environment expected at the site. The manufacturers' literature should not be the only basis for selecting a camera. The manufacturers' specifications or test conditions may not match the environment at a particular facility.

- Other considerations in the selection process should include the difficulty in performing maintenance, the packaging of the camera for the intended environment, the manufacturer's maintenance support, and the documentation supporting the equipment. Documentation should include operating, adjustment, and maintenance procedures; theory of operation; block diagrams; schematics; and replacement parts lists. Serious consideration should be given to eliminating any manufacturer's product that does not include this documentation.

The following significant factors affect the system's ability to assess exterior location video:

- perimeter layout
- lighting layout
- weather effects (e.g., fog, heavy snow)
- surface conditions (e.g., flat with no hills for hiding, evenness of scene reflectiveness, rain, drainage)

4.2.1.6 Testing

Section 4.4 contains testing information that the licensee should approach from a systems point of view. This section addresses several kinds of testing, including acceptance, operational, and performance testing, integrating cameras, DVRs, lighting, and system elements.

4.2.1.7 Maintenance

Section 4.5 contains maintenance information that the licensee should approach from a systems point of view.

4.2.2 Digital Video Recorders

4.2.2.1 Principles of Operation

Over the past 10 years, DVRs have almost totally replaced video cassette recorders for use in security video assessment applications and have significantly improved process and quality. Because a DVR records video onto arrays of hard drives, , it does not require the changing or rewinding of tapes. The most typical DVRs on the market today, depending on the features purchased, can do the following:

- Record the images obtained from 1 to 16 cameras simultaneously.
- Be set to record only when motion occurs in the camera scene, thus saving storage space.
- Instantaneously access recorded video from a particular time period.
- Store huge amounts of recorded video for weeks or even months.
- Adjust the number of frames per second (FPS) of video to store from each camera and the resolution of that stored image.

Modern DVRs are computer-based devices that can be controlled by an interactive system with the sensor alarm monitoring portion of a security system. Upon sensor alarm notification, the DVR can be directed to play back prealarm and postalarm video from the camera assessing the area covered by the alarming sensor.

Video image recording is a process that uses a personal computer to capture a video stream and store that video information to a network of computer hard-drive memories. The operator can then play back these video streams from the hard drive to the display to view the video images. The components of a video image recording system are a computer with a video-recording card, video-recording software for managing the storage and playback of the video images, and a computer monitor for displaying the video images. The video management software allows the computer to display incoming video on a monitor, record images, store incoming images to the hard drive, and play back stored images from several cameras on the monitor simultaneously.

Incoming camera analog video signals are separated into their main components (luminance and chrominance) and are then converted to a digital format for storage on a computer hard drive. Luminance contains the black and white portion of the video signal, and chrominance

contains the color portion. Digital filters are applied to each pixel (picture element) of the video image to ensure that every single pixel of video image is represented in digital format with the highest accuracy. Once the analog video signal has been converted to a digital signal, a certain amount of signal noise (white noise and other visual imperfections) results from the conversion process; this noise needs to be removed before the next step of video processing, called compression. Noise reduction software algorithms clean up the digital video information to provide better quality, improve video encoder compression efficiency, and improve the content of the stored images.

To maximize the amount of video images that a particular DVR system can store, video compression uses a coder decoder (or codec) to compress video content into a reduced size format using an encoding scheme to fit efficiently onto a hard-drive memory. For example, without compression, a 2-hour movie would need to be stored on 30 digital video disks rather than just one. Compression encoders include Motion Picture Experts Group (MPEG) format, Joint Photographic Experts Group (JPEG) format, Motion-JPEG (M-JPEG) format, H.2.64, and Wavelet. The H.2.64 compression is typically used in coding for videoconferencing and video telephony and for streaming broadcast, file download, and media storage and playback. Wavelet algorithms for video compression originated in Europe. Most DVR manufacturers have either adopted a compression scheme derived from one of the types described above or have created their own proprietary compression algorithm by combining portions of standard compression codecs. DVR manufacturers often use MPEG encoder compression because of the efficiency of video compression and the quality of the reconstructed playback image. Compression encoders analyze the video and decide which pieces of video information can be eliminated because they do not contain important visual content or they contain redundant information (e.g., an image background of all the same color).

Once the video is stored in computer hard-drive memory, retrieving images for playback requires several software algorithms to process the video images before a computer monitor can display them. The stored images must be uncompressed and reformatted to produce a series of pictures that, taken in timed sequence, replicates the initial analog images from which the stored video was obtained. Because reconstituted images can contain rough or harsh edges, a smoothing algorithm is applied to the edges of objects to make them appear more natural. Finally, a scaling algorithm is applied to adjust the picture to the size of the screen and clean up the edges of the picture. Scaling is also applied when the image size is adjusted to display images simultaneously from several cameras on the same monitor screen or to change the shape of the image displayed from its initial image size.

The standard frame rate for analog cameras operating to Electronics Industry Association standards is 30 FPS. The maximum DVR video recording rate is specified in FPS. Most DVRs can record video at rates of at least 30 FPS; however, many cannot record simultaneously at that frame rate on all channels (each channel serves one camera). The maximum recording FPS rate must be divided among all the cameras served by a DVR unit, although this does not have to be an equal number of frames for each camera. If a 16-channel DVR has a maximum recording rate of 240 FPS on average and if the DVR is recording all channels at the same FPS rate, a maximum of 15 frames can be allocated per channel. Because DVRs are computer based, the number of frames to be captured from each camera can be customized based on the camera, the time of day, or the type of received alarm that initiates the recording.

4.2.2.2 Types of Digital Video Recorders

The technology used by DVRs is evolving and capabilities and features of commercial DVR systems change radically every 12 to 18 months.

Some DVRs can control as many as 32 to 64 cameras each, although this feature is not necessarily advantageous if the system goes down. Multiple DVR systems controlling only 16 cameras each may be preferable because a significant number of a facility's cameras will not be rendered unavailable if one system becomes inoperative.

The number of video frames a particular DVR can record at any one time is also increasing dramatically. Minimal systems will record 30 FPS, whereas newer systems can record as many as 240 or more FPS.

4.2.2.3 Sources of Nuisance Alarms

Sources of nuisance alarms do not apply to this discussion.

4.2.2.4 Characteristics and Application

A DVR is generally a standalone unit. It records either analog or digital camera information and stores the information on a hard-disk drive. The DVR usually has a method of displaying the recording to a computer display that is directly attached to the DVR. The quality and number of cameras that are recorded directly affects the length of time that a DVR is capable of retaining the recordings. As a result, to increase the amount of time and the number of recordings that can be made from various cameras to one DVR, most units allow one of many software or hardware algorithms to compress recordings. Depending on the amount of compression, the compressed image may not have the same quality as the original. The advantage of DVRs is that, other than the highly reliable hard drive and cooling fans of the computer system, they have no moving parts that require increased maintenance. Because many DVRs have redundant disk drive options, the availability of DVRs for recording is very high.

NVRs work similarly to DVRs except they do not accept analog video signals as input. The NVR acts as a large database server for digital data streams and allows those streams to be sent anywhere they are commanded or programmed to send the information when an alarm event occurs. The NVR has all of the advantages of a network, including redundancy, system-level diagnostics, and system-level automatic backups of data.

Because NVRs operate on the network, the expected recording and display data loads on the network must be calculated to ensure that the network can process these high-data-rate streams without causing network bandwidth problems or delaying video or alarm data transmission. The decision to use tape or digital recorders (DVRs or NVRs) depends on the requirements for using the video in the first place. These requirements may include immediate assessment and surveillance.

4.2.2.4.1 Raw Camera Images versus Recorded Images

To determine whether the configuration of a DVR (or even the DVR itself) is adequate for purposes of assessment video playback, the output of the raw camera image should be compared to the same image played back from the DVR. Viewing the output of a DVR while a recording is taking place is not a definitive means for making a comparison. Most DVRs have a

loop-through output that connects the incoming camera input video to the video output connector. The images recorded and subsequently (and instantaneously) retrieved from the hard disks may have a significantly reduced resolution from the raw camera images. Therefore, actual playback images from the hard disk must be compared to the raw camera images when conducting resolution tests.

4.2.2.4.2 Digital Transport

A DVR can be used to copy video clips and images to portable memory devices for transport from the alarm station and for evidentiary purposes. Networked DVRs can be set up to send an e-mail with alarm video to response force personnel or offsite personnel for immediate response.

4.2.2.4.3 Memory Management

A DVR's memory management can be configured to overwrite previously saved video when the DVR reaches its maximum memory storage limit or when the oldest video has exceeded its maximum storage time limit. DVR output display configurations allow the operator to view single or multiple camera images as separate windows or panes on digital display monitors. Monitor views can be configured to simultaneously display live and recorded alarm video.

4.2.2.4.4 Video Motion Detection

VMD, a feature available in most DVRs, allows the DVR to automatically store video when a camera detects movement within its field of view. It can be set up to allow secure access to recordings using the Internet and secure communications and access controls (refer to Figure 68).

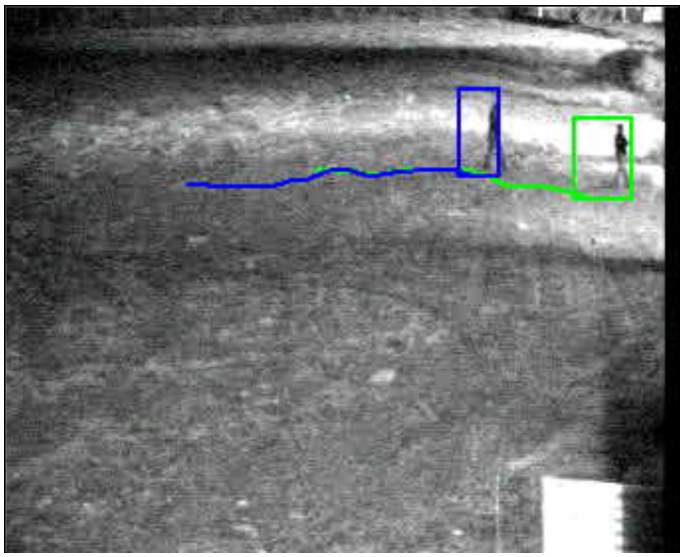


Figure 68 VMD image showing intruder tracking

The following factors determine the video storage capacity of a DVR system:

- the amount of hard-disk drive storage space
- the number of simultaneous video channels being recorded (i.e., the number of cameras)

- the FPS rate for each camera
- the resolution of the video image (pixels per frame)
- the quality of the recorded video (compression)

The file size of recorded images can be controlled by reducing the captured resolution. A DVR's resolution is represented as a pixel count or in a video format term called common intermediate format (CIF). CIF is a standard video format used to define resolution in terms of pixel count. Table 4 shows format in terms of CIF, pixel resolution of that format, and the size of an uncompressed video image with that format.

Table 4 CIF Image Sizes

Format	Resolution (Pixels)	Uncompressed Image Size (in kilobytes)
CIF	352x288	250
QCIF	176x144	63
4CIF	704x576	1,000
16CIF	1,408x1,152	4,000

Increasing the degree to which each captured image is compressed reduces the size the video files stored on the hard drives. A good camera may provide a high-resolution image, but compression of the captured image may be necessary to save storage space. To view a recorded, compressed image, the image is decompressed. However, when viewing the decompressed image, image detail can suffer. Overall image quality is a function of camera resolution, captured image resolution, and the amount of compression applied to the original digital image.

4.2.2.5 Installation Criteria

A DVR should contain a reasonably fast microprocessor that possesses the following characteristics at a minimum:

- at least 1-gigahertz clock speed or higher
- at least 256 megabytes of random-access memory
- at least a 5,400-revolution-per-minute, 300-gigabyte hard drive
- a video-recording card with at least 64 megabytes of onboard memory
- special software dedicated to simultaneously processing multiple streams of video and responding to control commands from a security alarm control and display system

The system should have at least a 17-inch monitor (preferably larger where possible) with at least a 1,024x768 pixel, 32-bit color display. A 10/100-megabyte network connection is required for streaming digital video from the video-image-recording computer to the operator's console. Existing analog cameras can connect directly to DVR analog inputs. Digital cameras can connect to recorders (called NVR) using Ethernet networks. A DVR can be implemented as a group of standalone boxes, or it can be integrated into a desktop computer-type configuration.

Most DVR systems are considered user friendly because they use simple control commands that are like those of a video cassette recorder, such as play, stop, fast-forward search, fast-reverse search, and enhanced digital control commands to play back-tabbed video associated with a specific alarm event. Because the DVR is a computer-based devise, many setup and control parameters can be customized for each application.

4.2.2.6 Testing

The sections below contain testing information that the licensee should approach from a systems point of view. The testing section addresses several kinds of testing, including acceptance, operational and performance testing, integrating cameras, DVRs, lighting, and system elements.

4.2.2.7 Maintenance

Maintenance for a DVR system is minimal. The manufacturer's suggested maintenance schedule should be followed.

4.3 Lighting

4.3.1 Lighting for Video Assessment

4.3.1.1 Principles of Operation

Lighting for alarm assessment allows security personnel to maintain visual assessment capability during darkness. When security lighting provisions are less than optimal, additional security posts, patrols, night vision devices, or other provisions are necessary for acceptable alarm assessment.

Security lighting should be used in vital areas and along perimeter fences when the situation dictates that the area or fence must be under continuous or periodic observation during nighttime hours.

When lighting is properly used in conjunction with video cameras, it may reduce the number of security personnel needed for alarm assessment. It may also enhance the protection of security personnel by reducing the possibilities of concealment and attack from a determined intruder.

Security lighting is desirable for those sensitive areas or structures within and at the perimeter that are under constant video observation. Such areas or structures include perimeter isolation zones; vital buildings; storage areas; and vulnerable control points of communication, power supply, and utility infrastructure systems. In interior areas where night operations are conducted, adequate lighting facilitates the detection of intruders approaching or attempting malicious acts within the area. Security lighting also has considerable value as a deterrent to intruders and may make the job of the adversary more difficult. Lighting is an essential element of an integrated physical security program.

A secure emergency power source, such as an uninterruptible power supply (UPS), and power distribution system for the facility should be installed to provide power source redundancy for critical security lighting and for security detection and assessment, control, and monitoring equipment. If primary power is temporarily lost as the result of power system outages or hostile activity, an emergency power supply enables critical security equipment (e.g., detection,

assessment, illumination, control, and monitoring assets) to remain operable, thus maintaining the integrity of the facility's physical protection system. Emergency power sources should be available immediately without functional interruption for critical electrical loads and should be secured against direct and indirect attack and sabotage.

Perimeter lighting needs should be based on the threat, site conditions along the perimeter, video assessment capabilities, and available security personnel. Security lighting should be designed and operated to facilitate the detection of intruders approaching or attempting to gain entry into protected areas and to discourage unauthorized entry.

An effective lighting design is of paramount importance to the proper functioning of alarm assessment systems. Just as humans need good lighting to see, most security video cameras require appropriate lighting to allow operators to efficiently assess the area when natural light is not adequate or available.

Intuitively, it would seem that a facility could order poles and an exterior luminaire to install at the top of each pole, run power lines, and then set the poles and light fixtures evenly spaced along the areas to be assessed. It might also seem that brighter lamps would require fewer poles and luminaires. However, that concept is not the optimal approach from a camera assessment perspective. To compare how lighting affects assessment, note the differences in the evenness of illumination shown in Figures 69 and 70. Figure 69 has one very bright spot that affects the camera's performance and dark spots where an adversary might hide. In the event of an alarm condition, the scene depicted in Figure 70 would allow for a more efficient video assessment to determine the cause of the alarm so that security personnel can be appropriately dispatched.

Figure 69 Example of lighting with hot spots, dark areas, and dirt ground cover

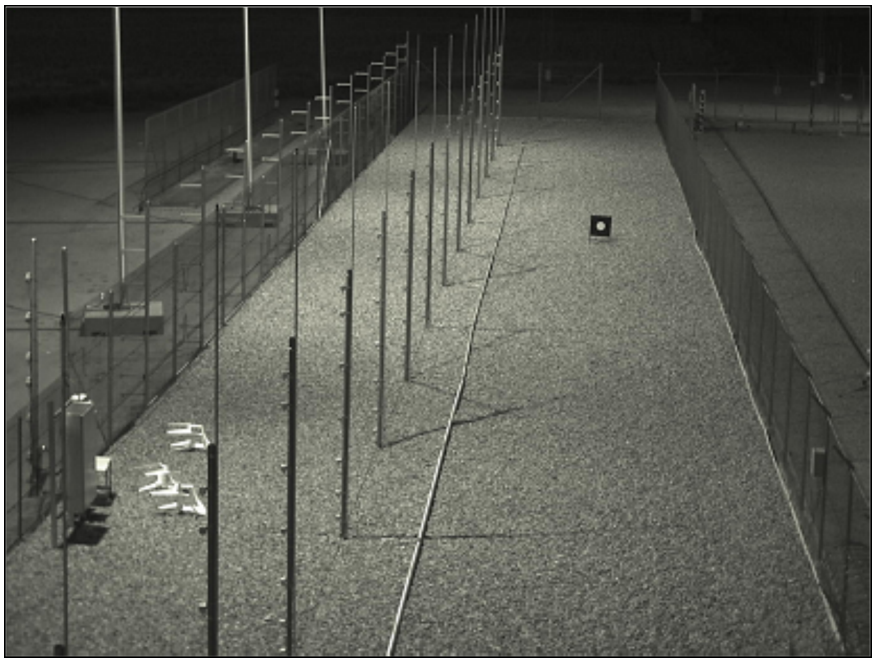


Figure 70 Improved assessment visibility with even lighting and a regular ground surface

If a facility is using thermal-imaging cameras as a means for providing alarm assessment at night, illumination in the specific areas covered by these cameras is not as critical: however, lighting may still be required to provide a means for the security force to identify and engage potential adversaries using a force continuum. If the potential exists for security personnel to use deadly force for the protection of the facility, illumination is a critical component that enables security personnel to properly identify and accurately engage the adversarial force after detection and assessment are complete.

4.3.2 Installation Criteria

Security lighting usually requires less illumination than normal task lighting, except for personnel identification and vehicle inspection at an entry control point. Each area of a facility presents its own unique set of considerations based on physical layout, security requirements, terrain, and environmental conditions.

The following information is available from lighting equipment manufacturers and vendors of lighting analysis software to assist in designing a lighting system:

- descriptions, characteristics, and specifications of luminaires and lamps
- luminaire lighting patterns
- installation layouts that show the height and spacing of luminaires necessary to achieve desired light levels
- software to produce computer-generated plots of illumination levels and lighting uniformity in a particular zone and summary statistics of the illumination profile

(e.g., average illumination level, light-to-dark ratio, and maximum and minimum illumination)

In planning a security lighting system, the site designer should consider the following factors:

- the cost of replacing lamps and cleaning fixtures and the cost of providing the required equipment (e.g., ladders and bucket trucks) for maintenance
- provision of automatic transfer or manual-override capability during a loss of primary power
- photoelectric controls for automatic control of lights during hours of darkness
- effects of local weather conditions on lighting systems
- fluctuating or erratic voltages in the primary power source
- grounding requirements
- provisions for rapid lamp replacement and luminaire cleaning
- special lighting requirements for critical areas (e.g., protected area perimeters) and a means to enable lighting to remain operable without interruption during the loss of primary power (i.e., because any amount of time without adequate lighting in a critical area may be unacceptable, these areas generally have emergency power, such as UPSs consisting of batteries and diesel generators, in case of primary power loss)
- continuous operation of security lighting systems during hours of darkness
- a security lighting system configured such that the failure of one or more lights will not affect the operation of the remaining lights
- restrike time (the time required before a light will function properly after a brief power interruption)
- a color spectrum of bulbs

4.3.3 Principles of Security Lighting

Security lighting enables security personnel to observe activities using alarm assessment and surveillance cameras around or inside a facility while minimizing their physical presence throughout the facility. Having adequate illumination levels at all approaches to a facility does not necessarily discourage unauthorized entry. However, adequate lighting improves the ability of security personnel to visually assess intrusion alarms with the use of video cameras and intervene in the event of an unauthorized access attempt. Lighting is implemented with other security measures, such as intrusion detection sensors, video assessment equipment, and alarm control and display systems as part of an integrated facility security system.

Optimum security lighting is achieved by adequate, even light in perimeter isolation zones. In addition, the use of deterrent lighting (i.e., glaring lights directed away from the fenced perimeter) can augment security perimeter lighting as a psychological deterrent to intruder

ingress. In addition to seeing long distances, security personnel must be able to see low contrasts, such as indistinct outlines of silhouettes, and must be able to detect an intruder who may be exposed to view for only a few seconds. If properly implemented, higher levels of illumination, such as that provided by deterrent lighting systems, can improve these assessment abilities.

Contrast between an intruder and the background should be an important consideration when planning for security lighting. With predominantly dark surfaces, more light is needed to produce the reflective brightness required for camera assessment than would be necessary if neutral gray backgrounds and ground cover are used. When the same amount of light falls on an object and its background, the observer must depend on the contrast of light reflected from each to determine the intruder's location. Adjusting the illumination level or the lighting location can significantly improve the observer's ability to differentiate between background and objects of interest when contrast is poor (refer to Figure 71, which shows poor contrast created by outdoor lighting (left) as compared to better contrast created by outdoor lighting (right)).

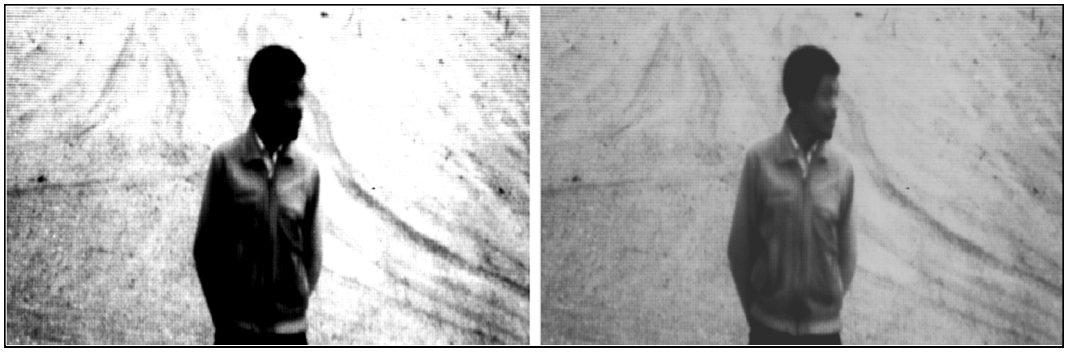


Figure 71 Contrast differences created by outdoor lighting

As shown in Figure 71 (left), the observer primarily sees an outline or a silhouette when the intruder is darker than the background. Using light-color finishes on the lower parts of buildings and structures may expose an intruder who depends on dark clothing and darkening of the face and hands. Placing stripes on walls has also been used effectively as patterns that can provide recognizable breaks in outlines or silhouettes.

Security lighting should be practical and effective. To be effective, it must discourage or deter intruder access attempts; if access is attempted, it should facilitate detection and assessment. The design of security lighting must provide sufficient illumination so that security personnel can effectively observe an intruder with the naked eye, but the lighting should not be so bright as to create a glare that may temporarily blind security personnel.

The eyes of individuals on a security response team dispatched from building interior locations will not adapt to the night before they can respond to an intrusion alarm at an exterior location where light levels are below 0.5 f-c (5 lux). Because full sensitivity change (adapting to a significantly lower light level) may take up to 30 minutes, proper illumination in exterior areas is critical to the effectiveness of responding security personnel.

4.3.4 Types of Lighting

The type of lighting system used depends on the facility's overall security requirements. Four types of lighting approaches can be used for security lighting systems: (1) continuous, (2) standby, (3) movable (portable), and (4) emergency.

4.3.4.1 Continuous Lighting

Continuous lighting is the most common type of security lighting used. As shown in Figure 72, it consists of a series of fixed lights arranged to continuously illuminate a given area during darkness with overlapping cones of light. Two primary methods used for continuous lighting are controlled projection lighting and deterrent glare projection lighting.

Figure 72 An example of a perimeter with controlled lighting

4.3.4.1.1 Controlled Lighting

Controlled lighting is optimum when the limits of the width of the lighted strip are directed to illuminate the inside of a perimeter isolation zone with minimal illumination of the areas inside the perimeter. Having too much illumination on the protected side of the perimeter may illuminate or silhouette security personnel and thus give the intruder an unnecessary visual advantage.

4.3.4.1.2 Deterrent Glare Projection Lighting

Deterrent glare projection security lighting (i.e., spotlights) is used when the glare of lights directed across the surrounding territory will not interfere with adjacent operations or be politically unacceptable to neighbors. These types of lights are a strong deterrent to a potential intruder because they make it difficult to see inside the protected area. Security personnel are protected by being in comparative darkness and are able to observe intruders who are at a distance outside the perimeter.

4.3.4.2 Standby Lighting

Standby lighting has a layout similar to continuous lighting. However, the luminaires are not continuously lit during nighttime hours; instead, they are either automatically or manually initiated when suspicious activity is detected by security personnel or the IDS.

4.3.4.3 Movable Lighting

Movable lighting consists of manually operated, movable integrated luminaire and generator assemblies that may be operated during hours of darkness or as needed. This type of system is normally used to supplement continuous or standby lighting.

4.3.4.4. Emergency Lighting

Emergency lighting is a system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative power source, such as installed or portable generators or a battery-powered UPS.

4.3.5 Lighting Definitions

Illuminance is defined as the intensity of illumination incident on a surface area and is stated in terms of “foot-candles” or “lux,” which are not equivalent measurements. One f-c is defined as the intensity of illumination on a 1-square-foot surface from a 1-lumen source of light located 1 foot away. The international system of unit’s standard unit (metric) for illuminance is 1 lux, which is defined as the illumination on a 1-square-meter surface from a 1-lumen source located 1 meter away. Specifically, 1 f-c is equal to 10.76 lux. For ease of conversion, however, industry practice uses 10 as the conversion factor between unit systems (i.e., 1 f-c = 10 lux).

Illumination is either natural or artificial. Natural illumination emanates from the sun, moon, and stars. Artificial illumination is manmade and comes from an illumination source, such as a luminaire.

Table 5 provides the approximate illumination levels for nine natural lighting conditions. As shown, the range of illumination from direct sunlight to starlight in an overcast sky spans about 9 orders of magnitude. However, because cameras cannot compensate for that range of natural illumination, luminaires must be used to illuminate assessment areas during nighttime hours. This reduces the dynamic range of camera compensation for daytime and nighttime lighting conditions to only 4 orders of magnitude.

Table 5 Relative Illumination Levels under Various Lighting Conditions

Lighting Conditions	Illumination Levels
Direct Sunlight	3,200 to 13,000 f-c
Full Daylight (not direct sun)	1,000 to 2,500 f-c
Overcast	100 to 1,000 f-c
Sunrise or Sunset (clear day)	20 to 60 f-c
Twilight	0.1 to 10 f-c
Full Moon (clear)	0.01 to 0.1 f-c
Full Moon (overcast)	0.001 to 0.01 f-c
Starlight (clear)	0.0001 to 0.001 f-c
Starlight (overcast)	0.00001 to 0.0001 f-c

A scene becomes visible when illumination is reflected from the surfaces and objects within that scene. Reflectance is the percentage of light reflected from a scene and depends on the angle of the light incident on the surface of a scene and on the texture and composition of the reflecting surface. Reflectance is determined by measuring illumination with a light meter's sensor facing down divided by the illumination measurement with the light meter facing upward. The measurement should be made such that neither the light meter nor the person making the measurements create a shadow on the sensor when it is face up or on the ground just below the light sensor when it is face down. For natural illumination, the reflectance of various scenes is relatively independent of the angles of incidence and reflection. Table 6 lists some common surfaces and their approximate reflectance.

Table 6 Typical Reflectance for Various Common Surfaces

Surface	Reflectance (%)
Empty asphalt surface	7–10
Sandy soil, wet	15–20
Grass-covered area with trees	20–25
Gray rounded river rock	25–35
Red-brick building	30–35
Sandy soil, dry	30–35
Unpainted concrete	35–40
Smooth surface aluminum	60–65
Snow-covered field	70–75

To ensure that a sufficient amount of the nighttime illumination is reflected back to the camera and that sufficient scene contrast exists for intruder detection, the ground surface of the assessment area should have a nominal reflectance of 25 to 35 percent when it is dry.

Illumination is typically measured using a light meter with the sensor face up at a specified distance above a horizontal ground plane. Normally, measurements are made at 15 to 30 centimeters (6 to 12 inches) above the ground. An area's average illumination is determined by taking several measurements of illumination at equally spaced locations in an illuminated area or zone. For example, measurements are taken in straight lines at 3.3-yard (10-foot) intervals in both the lengthwise and widthwise directions within a perimeter isolation zone beginning at one fence line and ending at the opposite fence line. Several measurements can be taken within an area or zone covered by a number of lamps and then averaged together. These are measurements of "horizontal scene illumination" or simply "scene illumination."

Average scene illumination is the average amount of light illuminating an assessment area. The average scene illumination must be high enough to achieve adequate alarm video assessment and visual assessment by security personnel. Tests have shown that an average scene illumination of 1 f-c onto a ground-cover surface with 25- to 35-percent reflectivity provides sufficient light for camera and security personnel assessment purposes in clear environments.

The “evenness” (also referred to as “flatness”) of scene illumination enhances the ability to assess an intruder’s location. In Figure 73, the scene at the left has a light-to-dark ratio of approximately 20 to 1 (20:1), which is not considered sufficient, whereas the scene at right has a light-to-dark ratio of approximately 4 to 1 (4:1).

Figure 73 Examples of light-to-dark ratios for camera assessment

Tests have shown that lighting designs with a light-to-dark ratio of at least 6 to 1 (6:1) at the end of bulb life provide sufficient illumination evenness for assessment purposes. A scene light-to-dark ratio of 6:1 should be considered to be a maximum (i.e., the lightest part of the scene that is being examined should be no more than 6 times brighter than the darkest part of the scene). A design ratio of less than 4:1 is strongly suggested for exterior lighting. Historically, assessment lighting systems have been designed to produce a light-to-dark ratio of 4:1 at installation to allow degradation to a light-to-dark ratio of 6:1 as bulbs produce a lower lumen output during their service life. At least 75 percent of the camera’s field of view should have an even illumination that meets the minimum average illumination and light-to-dark ratio requirements.

Using the lens iris control, exposure time, and electronic signal amplification, a camera averages the total scene brightness detected by the imager. As a result, there is a limit to the amount and intensity of bright areas and dark areas in the camera’s field of view for which the camera can compensate. This is known as the camera’s dynamic range. Bright spots in the camera’s field of view raise the average imager illumination level, which causes the camera electronics to compensate by lowering the average video signal output. This tends to cause the darker portions of the image to become too dark and will negatively affect an operator’s ability to assess the scene. To mitigate camera dynamic range limitations, the lighting design should specify and implement a maximum scene light-to-dark ratio. If the light-to-dark ratio is excessive, light areas will provide too much light and cause a saturation of details within those areas. Likewise, dark areas will not provide sufficient light for good resolution.

To maximize video assessment performance, the light-to-dark ratio of the scene should not exceed 6:1. This includes the entire area observed by the camera and not just the area of interest. To accomplish this, the lighting should extend beyond corners and fences to provide even illumination within 75 percent of the camera's field of view. As discussed previously, the outdoor perimeter area should use ground-cover materials that provide a 25- to 35-percent reflectance.

4.3.6 Range of Scene Illumination Readings

If a minimum average scene illumination of 1.0 f-c and a 4:1 scene light-to-dark ratio are recommended at installation, a maximum and minimum set of illumination readings at the scene can be estimated. Table 7 shows a relative range of minimum to maximum illumination readings for average illumination values of 1.0 to 3.0 f-c. For example, given a normal distribution of illumination readings, if an average scene illumination is calculated to be 1.0 f-c, the individual illumination readings are estimated to be in the range of 0.5 to 2.0 f-c.

Table 7 Ranges for Average Illumination Values That Will Give 4:1 Light-to-Dark Ratios

Average Illumination (f-c)	Relative Range (f-c)
1.00	0.5–2.0
1.25	0.6–2.5
1.50	0.8–3.0
1.75	0.9–3.5
2.00	1.0–4.0
2.25	1.1–4.5
2.50	1.3–5.0
2.75	1.4–5.5
3.00	1.5–6.0

With an understanding of the relative levels of scene illumination produced by various sources and the amount of light reflected from typical scenes, the licensee can determine the expected effectiveness of the camera portion of the video assessment system. The next step is to understand the camera imaging system being used for alarm assessment.

4.3.7 Assessment Sensitivity

Lighting for video alarm assessment must consider the camera, video processing, and the display system that produces images for security personnel to view. Lighting is required to facilitate 24-hour alarm assessment whether it is accomplished by security personnel or video cameras.

Because cameras are the primary mode of alarm assessment, camera sensitivity and lens aperture are two critical factors that affect the amount of reflected scene illumination appearing at the camera's imager. Camera sensitivity is defined as the amount of illumination required at the camera's imager to produce a usable video image. This basic rule applies whether the camera is analog or digital. The following factors contribute to producing a usable video assessment image:

- illumination and the flatness of illumination that are present at the scene
- spectral distribution (color of light) of the illumination source
- total scene reflectance

- object reflectance
- camera lens transmittance
- the aperture diameter of the camera (f-stop)
- the camera imager's spectral response (camera imager's sensitivity to the color of light)
- the camera imager's sensitivity to broad spectrum light
- the camera's automatic brightness control (gain and exposure time)

Under low light conditions, most cameras automatically compensate for the lack of illumination by increasing some combination of both the exposure time and amplifier gain depending on the overall brightness level desired by the user. Cameras with automatic iris lenses compensate for changing scene light levels by opening or closing the lens iris. The mechanics of illumination level compensation for some digital cameras can be programmed. The sequence of iris control, shutter control, and amplifier gain can be prioritized by the order in which they are used to control imager illumination. Using shutter control for low light compensation causes the shutter to be open for longer exposure times. Long exposure times will blur moving objects, whereas higher amplifier gain on very low light signals will produce grainier images. Both of these outcomes are undesirable for purposes of alarm video assessment. For example, fast-moving objects start to become noticeably blurry at exposure times greater than one-sixth of a second. The level of noise or amount of graininess in the monitor's video image that is acceptable depends on the application and the subjective opinion of the alarm station operator. Most digital cameras allow for the placement of limits on the maximum exposure time and gain so that one parameter can be favored over the other. Typically, some image blur can be tolerated over picture graininess.

An industry standard for specifying camera sensitivity has not been established. Camera manufacturers often state camera sensitivity using varying test conditions and camera parameter settings. Camera sensitivity is often stated in terms of minimum illumination level at the camera's imager to provide a usable picture. These camera specifications do not account for the illumination level degradation caused by the camera lens. Although the amount of light needed at the camera's imager to produce a usable picture is specified, the amount of light that needs to enter the lens to achieve that light level at the imager may be significantly higher. In addition, the camera's specifications may not necessarily document the illumination and scene conditions during which the camera's sensitivity is determined. Along with minimum light level, the following information is also important:

- condition of the output video—camera output and/or gain and exposure time

- lens transmissivity—the percentage of incident light appearing at the front of the lens that passes through on to the imager

- lens f-stop—the level of light reduction to the imager determined by the lens iris (or aperture) opening

- test scene reflectance—the percentage of incident light on a scene that is reflected back to its source

In some cases, the parameters used to claim sensitivity may be unrealistically assumed to indicate a better performance than that experienced in actual installations. For example, three of the favored parameters for specification enhancement are (1) higher scene reflectance than normally encountered, (2) unacceptably long exposure times, and (3) a large lens aperture (low f-stop).

These parameters are usually determined with the camera viewing a static scene. If the specification process factors in the need to effectively observe motion, the actual camera sensitivity experienced would most likely be less than (i.e., not as good as) that stated on manufacturers' data sheets.

To calculate whether the scene provides sufficient imager illumination for the camera chosen, the formula shown below may be used. To calculate the amount of illumination from the viewed scene incident on the camera imager, the scene illumination, scene reflectance, lens f-stop, and lens transmittance must be known. This formula is a quick way to check whether the camera's imager surface will experience sufficient illumination to provide an adequate video picture. However, it is highly recommended that a camera be field tested for verification under expected lighting conditions before its deployment.

$$\text{Imager Illumination} = (\text{Scene Illumination} \times \text{Scene Reflectance} \times \text{Lens Transmittance})/4 \times (\text{Lens f-stop})^2$$

where:

- The imager illumination is in f-c or lux.
- The scene illumination is in f-c or lux.
- The lens f-stop is from the lens specification.
- The scene reflectance is in percentage.
- The lens transmittance is in percentage.

For example, given an illuminated area and camera lens with the parameters shown below, the following apply:

- Scene Illumination = 1 f-c
- Scene Reflectance = 0.3 (30 percent)
- Lens Transmittance = 0.8 (80 percent)
- Lens Focal Length = 1.8

Using the equation above:

$$\text{Imager Illumination} = (1 \times 0.3 \times 0.8)/[4 \times (1.8)^2] = 0.019 \text{ f-c (or } 0.19 \text{ lux)}$$

From the example calculation, if a camera selected for video assessment had a sensitivity of 0.05 lux, it would have more than adequate sensitivity for the application if it is used to assess an area with the scene illumination, scene reflection, and the lens f-stop and transmittance shown above. The scene provides 0.19 lux, and the camera requires a minimum of 0.05 lux. Therefore, the scene provides 0.14 lux more than the minimum camera sensitivity.

Because most lighting applications are associated with bulbs that produce visible light, errors can be made in estimating the light required if the camera imager's spectrum is not considered. An example of this relates to the use of color cameras. Most color cameras render color by masking pixels on an otherwise monochrome imager with red, green, and blue filters. In a typical camera imager configuration, 25 percent are red, 25 percent are blue, and 50 percent are green. Therefore, light spectrum is filtered before it reaches the photo sensor, resulting in degradation to the imager's overall pixel sensitivity as compared to that of monochrome cameras. In addition, only 25 percent of the pixels in a color imager are sensitive to infrared light as compared to 100 percent of the pixels in a black and white camera. A color camera's

imager also has a blue filter in front of it that will further reduce its infrared sensitivity. If an NIR energy source is used, a black and white camera provides a visible video image even if the NIR illumination was not visible to the human eye.

4.3.8 Conceptual Lighting Layout

To prevent cameras from looking directly into a light source, security lights need to be located above the camera and out of the camera's field of view. It is usually recommended that security lights be no less than 3 vertical meters (10 vertical feet) above the camera's position (refer to Figure 74). It is further recommended that a light source not be directly above the camera to mitigate the potential effects of dust- and fog-induced backscatter. However, the use of a sunshield that extends beyond the front cover glass of a camera enclosure, like the brim of a cap, can also minimize those effects.

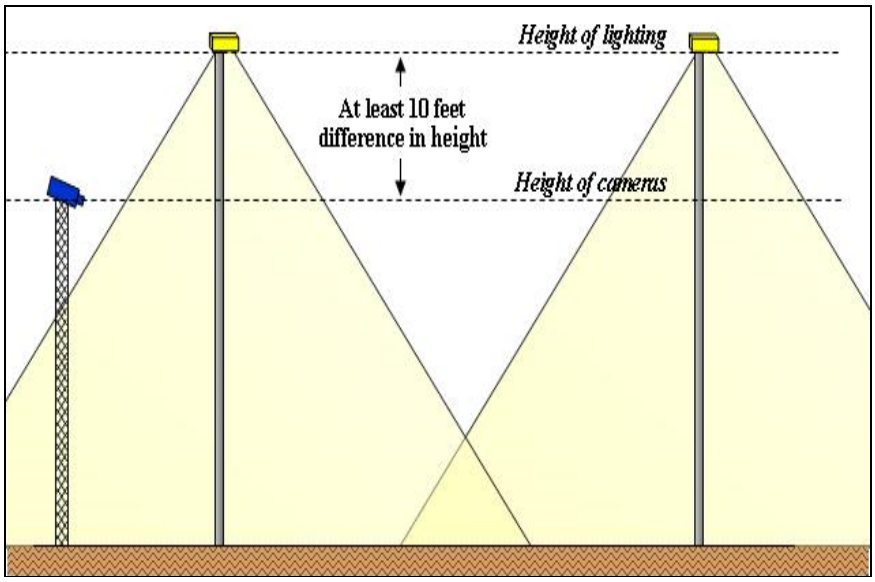


Figure 74 Recommended height differences between exterior lighting and cameras

4.3.8.1 Lighting Design

Using the lighting guidelines discussed earlier, the licensee should consult with manufacturers and suppliers of chosen lighting equipment to obtain luminaire and bulb illumination characteristics. Most major lighting suppliers and architectural engineering firms can model a proposed lighting system to determine and plot expected scene illumination levels. Maximum and minimum levels of illumination and light-to-dark ratios can also be determined. Modeling software can quickly evaluate several possible lighting configurations. The inputs to the model normally include a file containing photometric data specific to a particular type of lamp (provided by the lamp manufacturer); luminaire light pattern (provided by the fixture manufacturer); and luminaire orientation, mounting height, and light pole spacing. A facility that is going to perform extensive lighting work should consider a lighting software program for in-house use; this type of software is generally not expensive. Figure 75 is an example of output from an illumination modeling software package.

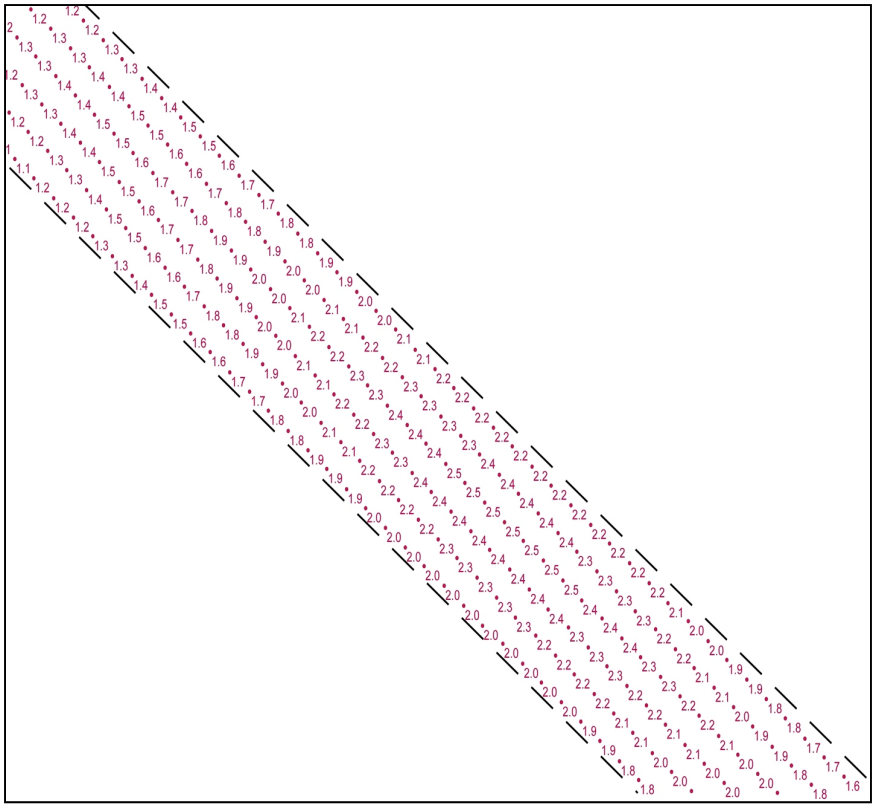


Figure 75 An example output from an illumination modeling software system

The computer-generated modeling software illumination output pattern provides data for a region of interest with expected illumination levels (i.e., numbers within the dashed lines are expressed in f-c) and other pertinent statistics. Note that the area calculated can represent data for a particular perimeter isolation zone.

The lighting design should be physically tested before installation in the final perimeter lighting configuration. A physical test is accomplished by installing a minimum of five fixtures (for single-row installations) and actually measuring the illumination provided. Measurements should be made at 15 to 30 centimeters (6 to 12 inches) above ground level and should be taken at 3.3-yard (10-foot) increments in the length and width dimensions. The brightest and darkest measurements should be identified, and the average illumination level and light-to-dark ratio should be calculated. Measurements should extend to distances at which the light level is above 0.2 f-c.

Meters equipped with a photo sensor operating in the appropriate wavelength are used to take light measurements. Some light meters are configured so that the photo sensor can be interchanged to allow illumination measurements within a specific spectral wavelength band. Measurements are typically taken 15 to 30 centimeters (6 to 12 inches) above ground level with the photo sensor facing up.

Adjustment and modification of the total lighting system after installation should be anticipated. Unidentified reflections or bright spots that occur during testing and that require correction are not uncommon.

The horizontal and vertical illumination levels required for interior lighting are determined similarly to exterior illumination values. The geometry of walls, floor, and ceiling reflections will affect ambient light levels.

Any interior lighting level suitable for human comfort and safety (e.g., between 30 and 100 f-c) will allow the use of a video camera with less sensitivity than that required for exterior video assessment applications. Energy savings can also be attained in interior spaces by illuminating a darkened room with NIR illumination sources and black and white cameras. The use of NIR illumination sources also provides a measure of covertness for the video assessment function in interior locations.

The wiring circuit for a lighting system should be arranged such that failure of any one lamp will not leave a large portion of the perimeter or a critical location in darkness. Electrical feeder lines should be placed underground to minimize the possibility of sabotage or vandalism from outside the perimeter. An additional advantage is that underground wiring reduces the effects from adverse weather conditions.

4.3.8.2 Lamp Types and Characteristics

Types of primary lamps and their characteristics are as follows:

- Incandescent. Light is emitted from a heated filament inside an evacuated globe.

- Quartz Iodine. Light is generated as it is in an incandescent lamp, but the globe is filled with a halogen gas that regenerates the filament and allows higher intensity.

- Fluorescent Lamp. Light is generated by an electric arc in a tube filled with mercury vapor. The low-pressure vapor emits ultraviolet radiation that is converted to visible light by fluorescent powders on the inner surface of the tube.

- High-Intensity Discharge Lamp. The light energy is generated by direct interaction of an arc with the gas to produce visible light. High-intensity discharge lamps include mercury vapor lamps, metal halide lamps, and high- and low-pressure sodium lamps. Argon is normally added to aid startup, and various powders or vapors may be added to improve color rendition.

- LED. The light energy is generated based on the LED solid-state technology. Lamps are usually constructed in cluster LEDs within suitable housing. Today, the LED lamp is mostly used for infrared illumination. However, LEDs may become more of a standard in the future for all types of lighting when considering the following advantages that it offers over conventional lighting:

  – LEDs that reliably offer over 100 lumens per watt are available.

  – If properly engineered, LEDs can operate for 50,000 to 60,000 hours.

  – LEDs illuminate upon activation without delay.

  – Unlike fluorescent and most high-intensity discharge technologies, LEDs contain no hazardous mercury or halogen gases.

– LEDs can be tuned to emit light in a broad range of colors.

Table 8 summarizes lamp characteristics for seven common bulb types.

Table 8 Characteristics of Seven Common Types of Bulbs

Lamp Type	Lamp Efficiency (lumens/watt)	Approximate Lifespan (hours)	Time Required for Full Output	Spectrum
Incandescent	12–20	750–10,000	Immediate	Broad (Visible to NIR about 400 to 1,000 nm)
Quartz Iodine	20–23	2,000	Immediate	Broad (Visible to NIR about 400 to 1,000 nm)
Mercury Vapor (Fluorescent)	40–65	24,000	3–7 minutes	Blue Green
Metal Halide	80–100	15,000	3–5 minutes	Broad (Visible to NIR about 400 to 1,000 nm)
High-Pressure Sodium	95–130	20,000	3–4 minutes	Gold-Yellow
Low-Pressure Sodium	131–183	18,000	8–15 minutes	Monochromatic Yellow
LED	70–100	50,000–60,000	Immediate	Broad (Visible to NIR about 400 to 1,000 nm)

4.3.9 Maintenance for Lighting Systems

Periodic inspections should be made of all electrical circuits to replace or repair worn parts, tighten connections, and check insulation. Fixtures should be kept clean and correctly aimed to provide optimal service.

Primary and alternate power sources should be identified. The following is a partial list of considerations:

- The primary source is usually utility offsite power.
- An alternate source such as a UPS consisting of batteries and diesel-fuel-driven generators is provided where required and should do the following:
  - Provide required power automatically without interrupting the assigned illumination upon failure of the primary power source.
  - Be adequate to power the entire lighting system.
  - Be equipped with adequate fuel storage and supply.
  - Be tested under load to ensure efficiency and effectiveness.

– Be located within a controlled area or hardened building inside the perimeter for additional security.

4.3.9.1 Measuring Perimeter Illumination Levels

Facilities should adopt a standard method for taking initial and periodic perimeter illumination level measurements. This standard measurement will ensure that the light levels can be correlated to previous measurements for the purpose of determining the amount of illumination degradation as bulbs age. Tracking the illumination degradation of bulbs will allow maintenance personnel to predict when luminaires need to be cleaned and when lenses or bulbs need to be replaced.

The measurement process requires two persons and the use of a 100-yard (300-foot) tape measure, a calibrated light meter, a 30-centimeter-high (1-foot-high) pedestal for attaching the light meter sensor, at least eight wooden blocks, a clipboard, and a preprinted spreadsheet for recording measurements (refer to Figure 76). Measurements are taken after sunset under darkened sky conditions after lights have been on sufficiently long to achieve full brightness. Although the following instructions depict measurements for a 100-yard-long (300-foot-long) area, the process can be applied to any length.

Figure 76 Checking light levels with a light meter within a perimeter isolation zone

4.3.9.2 Preparation for Measuring Perimeter Illumination Levels

Use the following procedures to prepare for measuring perimeter illumination levels:

- Beginning directly underneath one luminaire at the inner fence location (which will be called 0′ width and 0′ distance), use a tape measure to place wooden blocks at 3.3-yard (10-foot) intervals across the width of the perimeter toward the outer fence (refer to Figure 77).

- As in Step 1 but at a 100-yard (300-foot) distance from the initial starting point along the inner fence, use a tape measure to place wooden blocks at 3.3-yard (10-foot) intervals across the width of the perimeter toward the outer fence.

- With two persons, one at each end of the tape measure, extend the tape measure the entire 100-yard (300-foot) length to the second wooden block along the inner fence. Ensure that the tape measure is face up for its entire length.

- Firmly attach the light meter sensor (face up) to the top of the pedestal with duct tape.

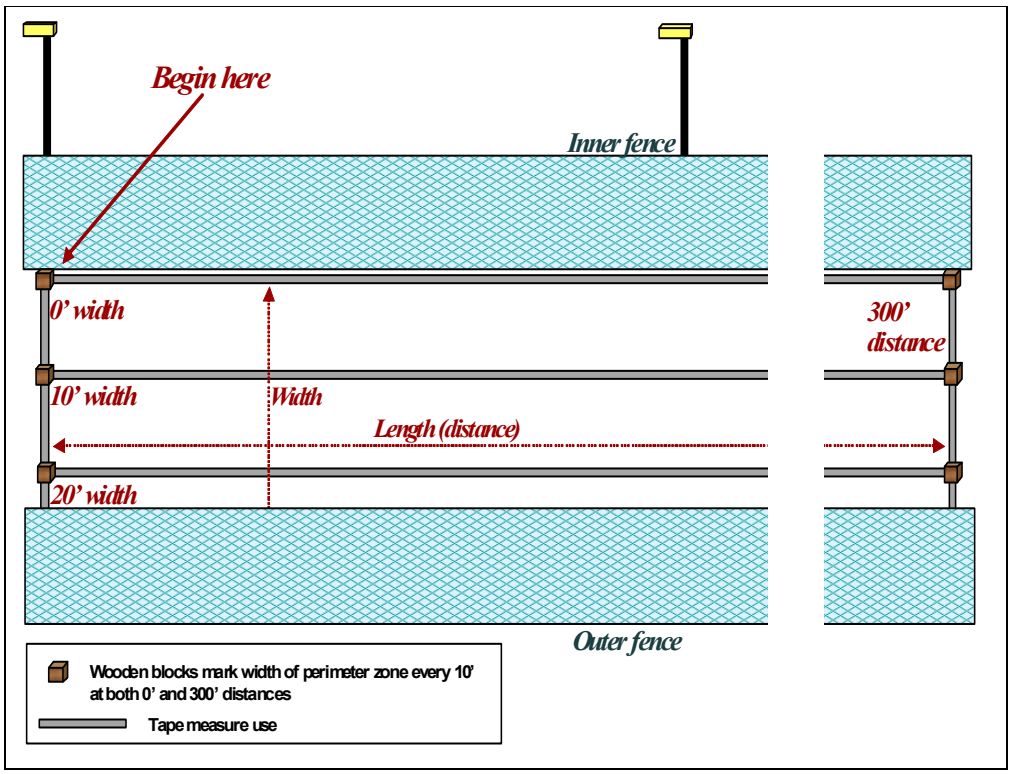


Figure 77 Preparation for measuring perimeter lighting illumination

4.3.9.3 Procedure for Measuring Perimeter Illumination Levels

The following procedures for measuring perimeter illumination levels require two people—one person takes the measurement while the other person records the reading on a data sheet:

- Beginning at the first measurement point, place the pedestal and sensor at the zero measurement point on the tape measure along the inner fence under the light fixture.
- Read the illumination value from the light meter. Ensure that personnel or other obstructions are not casting a shadow on the light meter sensor.
- Record the light meter reading on a data sheet (refer to Table 9 for a sample data sheet).
- Move to the 3.3-yard (10-foot) mark on the tape measure and read and record the light meter reading on the data sheet.
- Move to the 6.6-yard (20-foot) mark on the tape measure and repeat the measurement and recording procedure.
- Continue the measurement procedure until reaching the 100-yard (300-foot) mark on the tape measure.
- Using two people (one on each end of the tape measure), move the tape measure to the two wooden blocks at the 3.3-yard (10-foot) distance from the inner fence.
- Take measurements from the zero mark to the 100-yard (300-foot) mark as described in Steps 2 through 7.
- Move the tape measure to the blocks at the 6.6-yard (20-foot) and 10-yard (30-foot) distances (depending on the zone's width) from the inner fence and repeat the procedures in Steps 2 through 7.
- Sum all of the light meter readings taken and then divide by the number of readings. For the example, the number of readings taken is 124 (31 readings per row multiplied by 4 rows). This is the average illumination level as depicted in Figure 78. (Note that every wooden block or red circle from the diagram should have a coordinating measurement within one of the squares in Table 9).
- Ensure that the average illumination level is greater than 1.0 f-c or 10 lux.
- Find the highest reading and the lowest reading on the data sheet. Divide the highest reading by the lowest reading to derive the light-to-dark ratio.
- Ensure that the light-to-dark ratio is less than 6:1 (i.e., it should be approximately 4:1 for initial installation readings).
- As a second check of readings, divide the average illumination level, calculated in Step 10, by the lowest reading to derive the average-to-dark ratio. A well-designed lighting system will have an average light-to-dark ratio of approximately 2.5 to 1 (2.5:1) or less.

- Document the readings and calculations for comparison to subsequent readings.
- Compare the calculations taken at the initial installation with subsequent readings to determine illumination degradation.
- Plot initial and subsequent average illumination, light-to-dark ratio, and average-to-dark ratio values after each set of measurements to show long-term trends in lighting degradation.

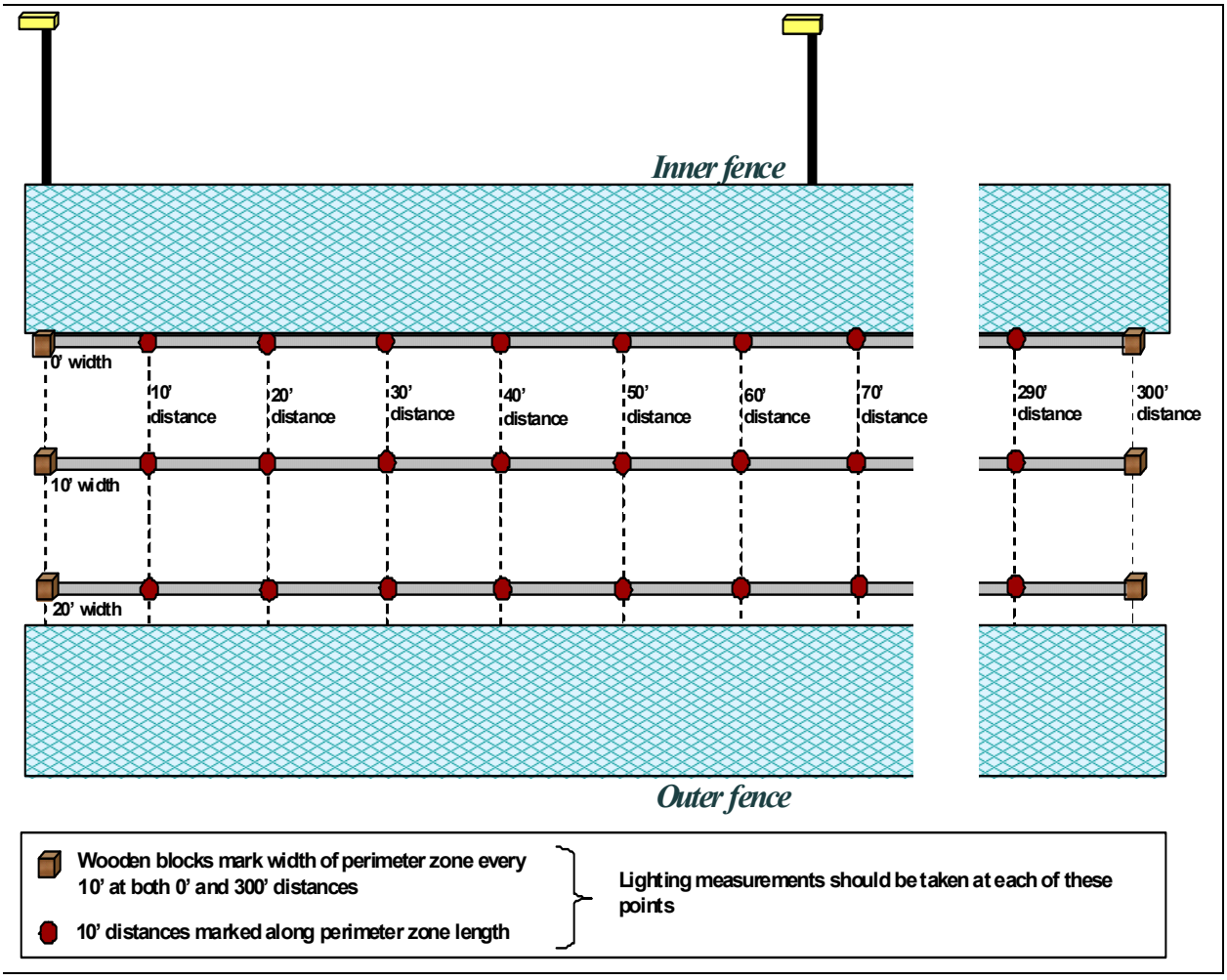


Figure 78 Points at which light readings should be measured

Table 9 Perimeter Light Measurements

Mark locations of lights

Length of Perimeter	Width of Perimeter (as appropriate)						
		0′	10′	20′	30′	40′	⊗
	0′						
	10′						
	20′						
	30′						
	40′						
	50′						
	60′						
	70′						
	80′						
	90′						
	100′						
	120′						
	130′						
	140′						
	150′						

4.4 Video Assessment System Testing

Testing requires that all the elements of the video assessment system work as integrated components rather than as individual parts. Therefore, each aspect of the video assessment system should be tested in concert. Video assessment systems that are integrated with IDSs should be tested in conjunction with each other to verify that these integrated systems are functioning and performing in the manner in which they are interfaced. They should be tested in accordance with their respective manufacturer's recommendations where appropriate.

A regular program of testing system components is imperative for maintaining their optimal operating order. Three types of tests must be performed at different times in the life of a video assessment system: (1) acceptance testing, (2) performance testing, and (3) operability testing.

4.4.1 Testing for Video Assessment Systems

4.4.1.1 Acceptance Testing

Upon receipt of cameras for final installation, the facility should evaluate the performance of the cameras to determine conformity with the manufacturer's specifications, compatibility with design criteria, and consistent performance from camera to camera. Experience has shown that final inspection at the manufacturer's plant may produce cameras with nonequivalent performance for specific field applications and lighting conditions. On occasion, equipment arrives in damaged condition, or parts have shaken loose in transit. Operating equipment continuously (performing burn-in) for a few hundred hours before final installation will decrease issues associated with immediate equipment mortality after the initial installation.

Exterior cameras should be installed in accordance with the manufacturer's requirements and should be focused at night while they are exposed to nighttime lighting conditions. Some cameras are shipped prefocused to specified distances. However, the environment in which these cameras are focused may not be the same as the operating environment at the facility. Initial camera setup should be followed by indoor and outdoor testing to confirm that the cameras perform as expected. The facility should make final adjustments to ensure camera focus and video image adequacy under nighttime lighting conditions. The video images produced by the cameras between daytime and nighttime operation should not vary much in picture quality. Washed-out images during the day or dark or low-contrast images at night are indications that the cameras are not performing to intended requirements.

Cameras should be checked for resolution and complete coverage of the assessed zone to ensure that the camera can see all detection areas in a zone. One simple method of checking camera resolution is to use 30-centimeter (1-foot) triangular, circular, and square targets. The targets that are painted white on one side and black on another are placed at the end of an assessment zone, and an alarm station operator should correctly identify the target shapes. The targets simulate the frontal cross-section of a crawling intruder. A large field resolution chart, such as a Rotakin, can also be used to provide more quantifiable information on camera resolution. In addition, the alarm station operator should be able to see the feet of an individual standing at both the inner and outer fence when the operator is standing at the beginning of the assessed zone. This test should be performed on live video from the cameras and on playback video from the video recording device for each assessment zone. In interior spaces, particular attention should be paid to the location of equipment or other objects that might occlude camera view or create shadows or blind spots.

Speed of response of a video assessment system should be tested to ensure that the alarm assessment and video recording of a detection zone occurs within 1 or 2 seconds of alarm annunciation. Other performance tests include a determination of the maximum number of concurrent alarms that can be processed, logged, and recorded at the same time and the amount of assessment delay that is occurring if more than one alarm is generated concurrently. The desired specifications and statement of acceptance testing requirements should be included as part of the terms and conditions of purchasing the system from the security systems integrator.

Conducting equipment incoming inspection, burn-in, and adjustments before actual its use should minimize maintenance and failure problems in the short term. A dated maintenance log should be kept to document problem occurrences, problem resolutions, and long-term fixes or equipment replacements undertaken to remediate recurring problems. Maintenance cycles can be established for the performance of repetitive maintenance activities and equipment replacement activities as a result of the data collected on the performance and failures occurring during system operation. This practice will substantially reduce repair time and identify substandard equipment performance.

The design phase of the video assessment system should ensure an inventory of equipment spare parts to immediately replace those that fail. The spares inventory should be replenished as spare parts are put into service.

One copy of the manufacturers' equipment documentation should be kept in a central document storage location and another copy should be kept by the security equipment maintenance organization. Modifications to the security system (as initially installed or documented) should be documented and stored at these two locations.

Acceptance testing for the video assessment system is the most encompassing because baseline performance and operability are determined and documented at this stage. Acceptance tests will uncover operational and functionality issues that the facility needs to address to ensure system operation in accordance with design specifications.

Use the guidelines listed in the sections below to perform video assessment system acceptance testing.

4.4.1.1.1 Cameras and Digital Video Recorders Used to Play Back Camera Images

(1) Ensure that each camera produces a video image on the alarm station monitors and that each camera channel produces video playback images for that channel on the alarm station monitors.

(2) Ensure that the camera channel numbering is arranged in a logical rather than haphazard order. For example, cameras for adjacent perimeter sectors should be sequentially numbered, and cameras inside buildings should be numbered according to a logical flow traversing through the building. For DVRs, ensure that the numbering of DVR camera input channels agrees with the live camera channels indicated on the alarm station monitors.

(3) With multiple individuals in the field communicating with alarm station operators, ensure that the camera image displayed on the monitor and recorded on the digital recorder is the correct one for the assessed space indicated. The alarm station operators should

observe the person in the field. Ensure that playback of video from the recorder shows the correct field location for the camera channel being tested.

(4) If camera images have graphic legends displayed on the monitor, ensure that the graphic legend is labeled correctly for the camera channel being tested.

(5) Ensure that camera resolution is sufficient for intruder classification and that cameras are in focus at night with nighttime illumination. To perform this test, one individual in the field places a 1-foot triangle, circle, and square at ground level at the end of the assessment zone or area. While communicating with an individual in the field using a two-way radio, the alarm station operator should correctly identify the order of the triangle, circle, and square. Alternately, using a field resolution chart calibrated for the distance from the camera, the alarm station operator should be able to accurately observe four distinct lines on the resolution chart at the calibrated position.

(6) Ensure that video recorder playback resolution is sufficient for intruder classification. Repeat the procedure for determining camera resolution (Step 5) to ensure video recorder playback resolution.

(7) Ensure that exterior cameras are focused such that the camera image is in focus at both the near and far fields of view. For example, check to ensure that the video image at both the beginning and end of an assessment zone is in focus.

(8) In exterior perimeter isolation zones, ensure that cameras are aimed such that the entire perimeter width can be observed on the alarm station monitors and in the recorded video. Camera aim can be tested by using two orange cones and two fiberglass rods in the following fashion. Two 61-centimeter-long (2-foot-long) fiberglass rods with a reflector at one end are fabricated with a clamping mechanism (e.g., a battery jumper cable clamp) for attachment to the top horizontal pipe of the perimeter fence (i.e., rods are available at a local building materials store). The rods are attached to the top of the inner and outer perimeter fences at the beginning of each perimeter isolation zone. The two cones are placed along the perimeter side of the inner and outer perimeter fences at the beginning of each assessment zone. The alarm station operator should be able to see the bottoms of the cones at the beginning of the sector and the reflectors at the top of the fence attachment rods.

(9) Ensure that a low-profile intruder observed on the alarm station monitors (and on the playback of recorded video) can be classified at the far end of each perimeter assessment zone. This should be tested at night at the inner and outer fence line inside the perimeter and at the center of the perimeter. The test subject should be a small individual who performs a belly crawl with his or her head toward the camera. The alarm station operator observing the monitor (and the playback of recorded video) should be able to determine whether the simulated intruder can be observed and accurately classified.

(10) During bright sunlight and nighttime illuminated conditions, observe each exterior camera on the alarm station monitors (and on the playback of recorded video) and ensure that images from each camera have approximately the same brightness and contrast and that monitor images of assessment zones do not have bright spots or dark spots. Images that are too bright, too dark, or lacking in contrast may require camera or

lens adjustment or replacement. For analog camera systems, video transmission or communication modules may also be the source of video brightness anomalies.

(11) Observe the scene from each interior camera on the alarm station monitors and ensure that images from each camera have approximately the same brightness and contrast. Images that are too bright, too dark, or lacking in contrast may require camera or lens adjustment or replacement. For analog camera systems, video transmission or communication modules may also be the source of video brightness anomalies.

(12) Observe interior and exterior cameras on the alarm station monitors and ensure that images are clear and crisp and do not have fuzzy or flickering images.

4.4.1.1.2 Camera Tests

- Ensure that exterior cameras are tilted down and do not view above the horizon at the camera's far field of view.

- Ensure that bright spots, shiny reflections, or glare from luminaires do not appear or cast a bright image in a camera's field of view.

- Ensure that large objects, such as electrical junction boxes that an intruder could hide behind, are not in an exterior camera's fields of view.

- Check all fasteners for the camera tower and mount to ensure that they are secure and that loose fasteners are not causing any movement.

- Ensure that the camera, enclosure, and mount are firmly affixed and not affected by wind causing the camera of move.

- For camera enclosures with external sunshades, ensure the enclosures have sunshades that extend at least 5 centimeters (2 inches) beyond the front of the camera enclosure.

- During blowing snow conditions, ensure that enclosure heaters melt the snow accumulation on the enclosure's front cover glass without creating an accumulation of ice.

4.4.1.1.3 Intrusion Alarm and Assessment Camera Interface Tests

Ensure that intrusion alarms in assessed areas trigger the appropriate camera's video to appear on the alarm station monitors (and on the playback of recorded video). While communicating with the alarm station operator using a two-way radio, an individual in the field should trigger an alarm in each intrusion detection zone. The alarm station operator should ensure that the assessment video displayed is from the correct camera for the zone in alarm and that the assessment video appears on the monitor within seconds. If an intrusion detection zone has multiple sensors, perform an intrusion alarm and video verification for each sensor.

4.4.1.1.4 Camera Lighting Tests

Turn off nighttime illumination and ensure that an alarm indicating loss of video contrast occurs for each camera.

4.4.1.1.5 Power Tests

- Disconnect or switch the main source of power to the video assessment system to simulate loss of offsite power and ensure that the UPS and diesel generator maintain uninterrupted power to the intrusion detection and assessment systems for the appropriate timeframe (i.e., this will vary with the facility).

- Disconnect individual cameras at field camera junction boxes and ensure that an alarm indicating loss of video occurs for each camera.

4.4.1.1.6 Tampering and Accidental Disconnection Tests

- Cover the front of the camera enclosure and ensure that an indicating loss of video contrast occurs for each camera.

- Shine a bright light into the front of each camera and ensure that an alarm indicating loss of video contrast occurs for each camera.

- Disconnect the video signal cable from each analog camera and ensure that an alarm indicating loss of video occurs for each camera.

- Disconnect the fiber-optic video transmission cable (fiber) for each camera and ensure that an alarm indicating loss of video occurs for each camera.

- Disconnect the Ethernet cable from each digital camera and ensure that an alarm indicating loss of video occurs for each camera.

- Disconnect the camera Ethernet cable from Ethernet switches carrying video signals and ensure that an alarm indicating loss of video occurs for all cameras connected to the switch.

- Disconnect the power cable to Ethernet switches carrying video signals and ensure that an alarm indicating loss of video occurs for all cameras connected to the switch.

- Simultaneously create intrusion alarms in multiple (two through five) adjacent and nonadjacent perimeter intrusion detection zones. Ensure that the alarm assessment video cues the recorded and live (prealarm and postalarm) video and displays the video for each of the alarming zones.

4.4.1.1.7 Camera Towers

Ensure that camera towers are properly grounded and have a lightning air terminal at the top of the tower. In addition, ensure that the tower and lightning rod (air terminal) have cables exothermically bonded to a ground rod at each tower. Resistance from the lightning rod and the tower to the ground rod cable attaching point must be less than 1 ohm.

4.4.1.1.8 Camera Tower Junction Boxes and Field Distribution Junction Boxes

Ensure that the camera tower junction box and field distribution junction box create tamper alarms when each enclosure is opened. In addition, ensure that the alarm station tamper alarm notification indicates the opening of the correct junction box. To accomplish this test, an

individual in the field communicates with the alarm station operator using a two-way radio. The individual in the field opens each camera tower junction box and field distribution panel (one at a time). The alarm station operator verifies that the correct tamper alarm message occurs for the box opened. After each test, the individual in the field recloses the junction box door. The alarm station operator observes whether the tamper alarm has been cleared after the junction box door is closed.

4.4.1.1.9 Shadow and Light Variation Determinations

- During nighttime illumination of perimeter isolation zones, observe monitor images of each assessed zone to ensure that fences are vertically perpendicular to the ground to verify that a shadow alongside the base of the perimeter side of the fence is not present.

- Ensure that buildings and large equipment enclosures do not cast a shadow across the perimeter isolation zone during either daytime or nighttime hours. Shadow areas reduce image contrast and video assessment capability.

4.4.1.1.10 Camera Brightness

- Ensure that nighttime bright light illumination from adjacent buildings or parking lots does not create bright spots on the ground of the perimeter.

- Ensure that camera brightness is consistent during changing daylight brightness conditions, particularly during morning and evening hours. This ensures that camera electronics and automatic iris lens controllers are compensating properly for changing illumination levels. This condition is normally observed as a video image that is either brighter or darker than other camera images. Images that are too bright, too dark, or lacking in contrast may require camera or lens adjustment or replacement. For analog camera systems, video transmission or communication modules may also be the source of video brightness anomalies.

- Ensure that camera brightness is not oscillating between two automatic iris positions. This effect is observed as an oscillating lighter to darker camera image. Dust in the automatic iris lens mechanism or an improper combination of lens control and camera amplifier electronics parameter adjustments can cause this effect. Camera or lens adjustment or replacement may be required.

4.4.1.2 Performance Testing

Performance testing for the video assessment system is a set of tests designed to ensure that the entire video assessment system is performing to specific requirements and that all functions are operating properly. Performance tests are an indepth set of tests that identify sources of system degradation and nonfunctionality that need to be repaired to bring the system back to initial performance specifications. Tests are to be conducted for all camera locations. It is recommended that these tests be performed on the entire set of camera-assessed areas on an annual schedule. Use the following guidelines to perform video assessment system performance testing:

- Ensure that each camera produces a video image on the monitor (and on the playback of recorded video).

- Ensure that intrusion alarms in assessed areas cause the appropriate camera's video to appear on the alarm station monitor and to be recorded on the video recorder. While communicating with an alarm station operator using a two-way radio, an individual in the field triggers an alarm in an intrusion detection zone. The alarm station operator ensures that the live video and playback of the recorded assessment video resulting from the alarm is from the correct camera for the zone in alarm and that the assessment video appears on the alarm station monitor within seconds. If multiple sensors are in an intrusion detection zone, ensure that an intrusion alarm is generated and that video verification is performed for each sensor.

- Ensure that the graphic legend is labeled correctly for the alarming camera channel being tested and ensure that the graphic legend is stable and not "jittering" on the monitor screen.

- Ensure that interior cameras produce an image that is in focus. Ensure that exterior cameras are in focus at both the near and far fields of view. Ensure that the video image at both the beginning and end of an assessment zone is in focus. Ensure that camera images are clear and crisp and do not have fuzzy or flickering images.

- Ensure that camera focus and video recorder playback quality are sufficient for human intruder classification. One individual in the field places a 30-centimeter (1-foot) triangle, circle, and square at ground level at the end of the assessment zone or area. While communicating with the individual in the field using a two-way radio, an alarm station operator observes live camera video on an alarm station monitor and video recorder playback images to correctly identify the order of the triangle, circle, and square.

- In exterior perimeter isolation zones, ensure that cameras are aimed such that the entire perimeter width can be observed on the alarm station monitor. For this test, two orange cones and two fiberglass rods are required. Two 61-centimeter-long (2-foot-long) fiberglass rods with a reflector at one end are fabricated with a clamping mechanism (e.g., a battery jumper cable clamp) for attachment to the top horizontal pipe of the perimeter fence (i.e., rods are available at local building materials stores). The rods are attached to the top of the inner and outer perimeter fences at the beginning of each perimeter isolation zone. The two cones are placed along the perimeter side of the inner and outer perimeter fences at the beginning of each assessment zone. The alarm station operator should be able to see the bottoms of the cones at the beginning of the sector and the reflectors at the top of the fence attachment rods.

- Ensure that a low-profile intruder observed on an alarm station monitor can be classified at the far end of each perimeter assessment zone. At night, a small individual performs a belly crawl at the inner and outer fence line inside the perimeter and at the center of the perimeter with his or her head toward the camera. The alarm station operator observing the monitor should be able to determine whether the simulated intruder can be observed and accurately classified.

- For interior cameras and for exterior cameras, observe camera images on the alarm station monitor during bright sunlight and during nighttime illuminated conditions and ensure that camera images have approximately the same brightness and contrast and that monitor images of assessment zones do not have bright spots or dark spots. Images that are too bright, too dark, or lacking in contrast may require camera or lens

adjustment or replacement. For analog camera systems, video transmission or communication modules may also be sources of video brightness anomalies.

- Ensure that camera brightness is not oscillating between two automatic iris positions. This effect is observed as an oscillating lighter-to-darker camera image. Dust in the automatic iris lens mechanism or an improper combination of lens control and camera amplifier electronics parameter adjustments can cause this effect. Camera or lens adjustment or replacement may be required.

- Ensure that a low-profile intruder observed on the playback of video taken during Test 7 above can be classified at the far end of each perimeter assessment zone. At night, a small individual performs a belly crawl at the inner and outer fence line inside the perimeter and at the center of the perimeter with his or her head toward the camera. The alarm station operator observing the playback of belly crawl activities should be able to determine that the simulated intruder can be observed and accurately classified.

- During bright sunlight and nighttime conditions, observe each exterior camera on the alarm station monitor and ensure that images from each camera have approximately the same brightness and contrast and that monitor images of assessment zones do not have bright spots or dark spots. Images that are too bright, too dark, or lacking in contrast may require camera or lens adjustment or replacement. For analog camera systems, video transmission or communication modules may also be sources of video brightness anomalies.

- Observe interior and exterior cameras on an alarm station monitor and ensure that images are clear and crisp and do not have fuzzy or flickering images.

- Ensure that exterior cameras are tilted down and do not view above the horizon at the camera's far field of view.

- Ensure that bright spots, shiny reflections, or glare from luminaires do not appear or cast a bright image in a camera's field of view.

- Ensure that large objects, such as electrical junction boxes that an intruder could hide behind, are not in an exterior camera's field of view.

- Check all fasteners for the camera tower and mount to ensure that they are secure and that loose fasteners are not causing any movement.

- Ensure that the camera, enclosure, and mount are firmly affixed and not affected by wind causing the camera to move.

- During blowing snow conditions, ensure that enclosure heaters melt any snow accumulation on the enclosure's front cover glass without creating an accumulation of ice.

- Turn off nighttime illumination and ensure that an indicating loss of video contrast occurs for each camera.

- Disconnect or switch off the main source of power to the video assessment system to simulate a loss of offsite power and ensure that the UPS and diesel generator maintain uninterrupted power to the intrusion detection and assessment systems for the appropriate timeframe (i.e., this will vary with the facility).

- Disconnect power to individual cameras at field camera junction boxes and ensure that an alarm indicating loss of video occurs for each camera.

- Cover the front of the camera enclosure and ensure that an alarm indicating loss of video contrast occurs for each camera.

- Shine a bright light into the front of each camera and ensure that an alarm indicating loss of video contrast occurs for each camera.

- Disconnect the video signal cable from each analog camera and ensure that an alarm indicating loss of video occurs for each camera.

- Disconnect the fiber-optic video transmission cable (fiber) for each camera and ensure that an alarm indicating loss of video occurs for each camera.

- Disconnect the Ethernet cable from each digital camera and ensure that an alarm indicating loss of video occurs for each camera.

- Disconnect the camera Ethernet cable from Ethernet switches carrying video signals and ensure that an alarm indicating loss of video occurs for all cameras connected to the switch.

- Disconnect the power cable to Ethernet switches carrying video signals and ensure that an alarm indicating loss of video occurs for all cameras connected to the switch.

- Simultaneously create intrusion alarms in multiple (two through five) adjacent and nonadjacent perimeter intrusion detection zones. Ensure that the alarm assessment video queues the recorded and live (prealarm and postalarm) video and displays the video for each of the alarming zones.

- Ensure that camera towers are properly grounded and have lightning air terminals at the top of each tower and that the tower and lightning rod (air terminal) have cables exothermically bonded to a ground rod at each tower. Resistance from the lightning rod and the tower to the ground rod cable attaching point must be less than 1 ohm.

- Ensure that the camera tower junction box and the field distribution junction box create tamper alarms when each enclosure is opened. Ensure that the alarm station receives the tamper alarm notification and indicates the opening of the correct junction box. An individual in the field communicates with an alarm station operator using a two-way radio. The individual in the field opens each camera tower junction box and field distribution panel (one at a time). The alarm station operator verifies that the correct tamper alarm message occurs for the box opened. After each test, the individual in the field recloses the junction box door. The alarm station operator observes that the tamper alarm can be cleared after the junction box door is closed.

- During nighttime illumination of perimeter isolation zones, observe the monitor images of each assessed zone to ensure that fences are vertically perpendicular to the ground to verify that a shadow along the base of the perimeter side of the fence is not present.

- Ensure that buildings and large equipment enclosures do not cast a shadow across the perimeter during daytime or nighttime hours. Shadow areas reduce image contrast and video assessment capability.

- Ensure that nighttime bright light illumination from adjacent buildings or parking lots does not create bright spots on the floor of the perimeter.

4.4.1.3 Operability Testing

Operability testing for the video assessment system is an ongoing set of tests to ensure that the system continues to function properly. Operability tests identify sources of system degradation and nonfunctionality that require immediate attention and remediation. Tests are to be conducted for all camera locations. It is recommended that these tests be performed in conjunction with the IDS and component tests to verify that both systems are operating and interfacing as required. Several of these tests repeat the acceptability tests. Use the following guidelines to perform video assessment system operability testing:

- Ensure that intrusion alarms in assessed areas cause the appropriate camera's video to appear on the alarm station monitor (and on the playback of recorded video). While communicating with an alarm station operator using a two-way radio, an individual in the field triggers an alarm in an intrusion detection zone. The alarm station operator ensures that the assessment video resulting from the alarm is from the correct camera for the zone in alarm and that the assessment video appears on the alarm station monitors within seconds. If multiple sensors are in an intrusion detection zone, ensure that an intrusion alarm is generated and that video verification is performed for each sensor.

- Ensure that the graphic legend is labeled correctly for the alarming camera channel being tested and ensure that the graphic legend is stable and not "jittering" on the monitor screen.

- Ensure that interior cameras produce an image that is in focus. Ensure that exterior cameras are in focus at both the near and far fields of view. Ensure that the video image at both the beginning and end of an assessment zone is in focus. Ensure that camera images are clear and crisp and do not have fuzzy or flickering images.

- Ensure that the camera focus and video recorder playback quality are sufficient for human intruder classification. An individual in the field places a 30-centimeter (1-foot) triangle, circle, and square at ground level at the end of the assessment zone or area. The alarm station operator should correctly identify the order of the triangle, circle, and square by observing live camera video on the alarm station monitor and playback video images.

  As an alternate method for this step, at night, a small individual on all fours at the inner and outer fence line inside the perimeter and at the center of the perimeter with his or her head toward the camera moves sideways in the camera field of view. An alarm

station operator observing the monitor in the alarm station should be able to determine whether the simulated intruder can be observed and accurately classified.

- In exterior perimeter isolation zones, ensure that cameras are aimed so that the entire perimeter width can be observed on the alarm station monitor. This test requires two orange cones that are placed along the perimeter side of the inner and outer perimeter fences at the beginning of each assessment zone. The alarm station operator should be able to see the bottoms of the cones at the beginning of the sector.

- For interior cameras and for exterior cameras, observe camera images on the alarm station monitor during bright sunlight and during nighttime illumination conditions and ensure that the camera images have approximately the same brightness and contrast and that monitor images of the assessment zones do not have bright spots or dark spots. Images that are too bright, too dark, or lacking in contrast may require camera or lens adjustment or replacement. For analog camera systems, video transmission or communication modules may also be sources of video brightness anomalies.

- Ensure that camera brightness is not oscillating between two automatic iris positions. This effect is observed as an oscillating lighter-to-darker camera image. Dust in the automatic iris lens mechanism or an improper combination of lens control and camera amplifier electronics parameter adjustments can cause this effect. Camera or lens adjustment or replacement may be required.

4.5 Maintenance

A video assessment system requires regular maintenance to ensure a high level of performance and reliability.

Maintenance should be performed according to a defined schedule. If performance or operability testing shows degraded system performance, the maintenance schedule should be adjusted accordingly.

The design process should consider maintenance procedures and equipment needed to maintain the video assessment system. The long-term operability and performance of the system will depend on effective maintenance. Spare part purchases should be made at the same time as the primary equipment purchases to ensure video assessment system operational continuity and parts interchangeability. The level of maintenance to be performed on site should be decided early in the design process to determine the type and quantity of spare parts that need to be purchased and the level of maintenance and repair functions that will be required.

A staff of qualified maintenance personnel is necessary to enable the video assessment system to continue performing at the level established during the system design. Ideally, an experienced maintenance staff should be knowledgeable about the system configuration, subsystem component location, cable routing, installation, checkout, and troubleshooting procedures.

A maintenance log of all equipment repairs and adjustments should be kept to provide a historical record of the actions taken to correct specific problems. Maintenance trends can be established to identify recurring problems and corrective actions needed to eliminate repetitive

occurrences of the same problem. This can substantially reduce repair time and identify substandard equipment.

Adequate maintenance cannot be performed without adequate equipment documentation. Maintenance and operations manuals should be purchased at the time of equipment procurement. Complete documentation should include theory of operation, functional block diagrams, cabling diagrams, schematic diagrams, and parts lists with manufacturers' or commercial equivalent part numbers.

5 OWNER-CONTROLLED AREA SURVEILLANCE

5.1 Overview

Often, the owner-controlled area of a facility is larger than the section of the facility that is enclosed within protected area perimeter fencing. Figure 79 depicts an owner-controlled area (the shaded area in the middle of the image) that is much larger than the security area that is enclosed within perimeter fencing. Real-time surveillance across the owner-controlled area can be challenging, especially given widely varying terrain. Long-distance surveillance technologies should be used to survey the owner-controlled area that resides outside the protected area perimeter fencing for possible early warning or detection of intruders.

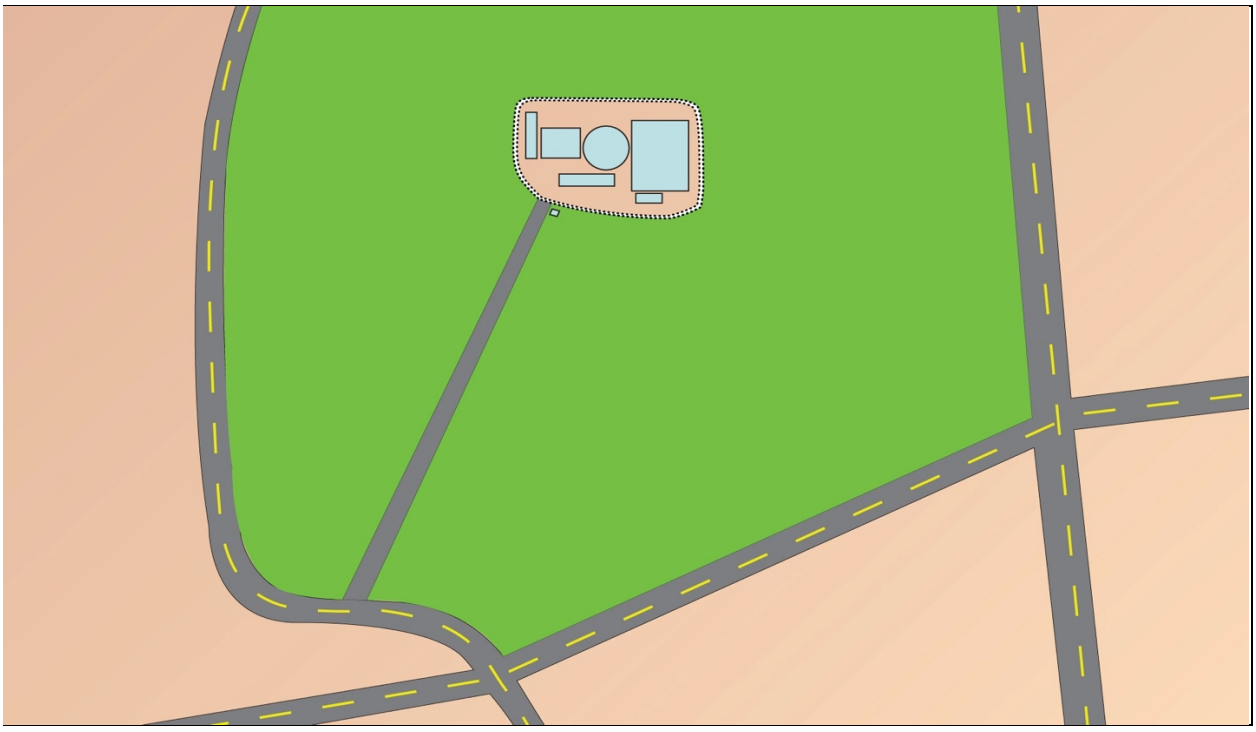


Figure 79 A large owner-controlled area

Key elements common to many long-distance surveillance devices that should be understood when considering the purchase of real-time surveillance-type devices include magnification, objective lens diameter, and field of view.

5.1.1 Magnification

This element determines the degree to which the object being viewed is enlarged. Two numbers are associated with binoculars: 7 x 50. The “7” represents the amount of magnification; the object being viewed will be 7 times larger than if it is viewed by the unaided eye. The greater the magnification or power, the smaller the field of view and the less bright the image will be. It is recommended that any item of more than 10-times magnification should be mounted on a tripod or similar device. Spotting scopes typically have three numbers:

15–45 x 80. The first two numbers (15–45) represent the magnification range of the scope, and the third number (80) relates to the diameter of the objective lens.

5.1.2 Objective Lens Diameter

Objective lenses are the front lenses of binoculars. The diameter of these lenses, measured in millimeters, is the second number associated with binoculars and the third number associated with spotting scopes. For example, for the 7 x 50 binoculars, "7" is the magnification or power, and "50" represents the diameter in millimeters of the objective lenses. The diameter of the objective lens determines its light-gathering ability, which equates to the brightness and usability of an image being viewed under certain conditions.

5.1.3 Field of View

The size of an area that can be seen while looking through a surveillance device is referred to as the field of view. Field of view is related to magnification; the higher the magnification, the smaller the field of view. A large field of view is desirable if a broad area is under surveillance. A large field of view provides the viewer with the capability to continually observe activity with minimum viewing adjustments and loss of observation. With a smaller field of view, the object being viewed is likely to move beyond the field of view causing a loss of observation and the need to continuously adjust. The same is true when the user is moving.

The following types of devices are readily available and will allow a facility to perform surveillance at different distances and under different conditions:

- binoculars
- spotting scopes
- night vision devices
- thermal imagers
- enhanced night vision devices, which use a fusion of night vision and thermal technologies

The U.S. Department of Defense has conducted extensive testing of surveillance devices. The exact model of a surveillance device for implementation at a particular facility will depend on the site conditions and the surveillance objectives to be met.

5.2 Surveillance Devices

5.2.1 Binoculars

5.2.1.1 Principles of Operation

Binoculars provide the user with the ability to use both eyes to peer through two identical mirror-symmetrical telescopes. These telescopes magnify distant objects up to a 10-times magnification. Because both eyes are used, binoculars allow for depth perception, which helps provide a three-dimensional image. Devices that employ only one eye do not provide depth perception.

Binoculars hold the two telescopes such that a hinge between them allows adjustment of the distance between the two telescopes to the individual user. A wheel allows the user to focus

both telescopes similarly by changing the distance between the eyepieces and the objective lenses. Some binoculars are available that allow the user to focus the two telescopes individually.

The quality of a pair of binoculars is predominantly determined by the quality of the lenses used, which affects the cost of a particular device. Precision-ground lenses can provide a clarity that is not available with cheaper lenses. Although the human eye can compensate for poor quality glass for short periods of time, the user will likely experience extreme eye fatigue if more than a few minutes of use is required.

Handheld binoculars are limited to a 10-times magnification because higher magnification, without the use of a tripod or similar mounting device for image stabilization, results in image vibration and destabilization. The vibration and destabilization is a result of the normal physiology of the body, such as heart and breathing rate.

Binoculars with high-quality lenses will help the human eye to see better at night than the unaided eye. High-quality lenses increase the light-gathering ability of the binoculars, which in turn increases the brightness relative to the human eye at the objective.

5.2.1.2 Types of Binoculars

A wide variety of binoculars are available that support a wide variety of applications. Binoculars that are considered “general purpose” are typically not appropriate for use by a security organization of a large facility. Long-range observation, military, and range-finder types are usually considered for security applications.

5.2.1.3 Characteristics and Applications

Most long-range observation binoculars provide good clarity for long-term use. However, one problem in using such binoculars is that below-optimal lighting conditions can significantly degrade the scene viewed.

Military-rated binoculars generally provide good optics and receive extensive testing, including shock tests, to ensure that they will function as intended under most conditions.

Range-finder binoculars can identify the distance between the user and the object being viewed. They are also the most expensive type of binocular.

5.2.1.4 Testing

Testing on a weekly basis is recommended to ascertain that the device operates as advertised by the manufacturer. If the device is dropped, the user should test the device as soon as possible.

5.2.1.5 Maintenance

The lenses of most binoculars require daily cleaning with a cleaner and soft cloth recommended by the manufacturer. Devices that have an on/off switch also require routine checks and replacement of batteries.

5.2.2 Spotting Scopes

5.2.2.1 Principles of Operation

A spotting scope is a small type of telescope that can be used during daylight conditions any time more magnification is needed than binoculars can provide.

Two factors determine the amount of magnification that can be used in a spotting scope: (1) atmospheric conditions and (2) the optical system.

Heat waves, dust, humidity, glare, wind, and air currents significantly affect the view through a spotting scope. The greater the magnification of a device, the greater the degradation of the performance of the spotting scope during such conditions. High altitudes and dry climates favor higher magnification, whereas low altitudes and wet, humid climates discourage high magnification.

The optical system of a scope is a determining factor in what and how well the user will be able to see. Image quality is directly related to cost. The inexpensive spotting scopes, regardless of size or type, lose image quality as magnification increases. Premium-grade scopes will lose very little image quality as the magnification increases.

The magnification capabilities of spotting scopes range from 10 to 400 times.

5.2.2.2 Types of Spotting Scopes

A spotting scope can either be an angled spotting scope or a straight spotting scope. Many users prefer a straight scope in which the eyepieces are parallel. In an angled scope, the eyepiece is offset at 45 degrees or 90 degrees from the scope barrel. A straight scope is recommended for individual users who plan to keep the scope setting at his or her height. With a straight scope, the user's eyes will stay level with the object being observed through the lenses. An angled scope is recommended for use at different heights. The user can use an angled scope to look down or up at things without having to adjust the height of the scope.

5.2.2.3 Characteristics and Applications

A quality spotting scope used under good atmospheric conditions can provide high-quality scenes of objects extremely far away. Because of the sizes of lenses needed for the higher magnifications of a spotting scope, these devices can become quite large and cumbersome. Most spotting scopes must be mounted on a tripod or other device to keep them still enough to use.

Higher magnifications and greater distances create a much smaller field of view for the user. Adequate lighting at great distances can also hinder the usability of a scope.

5.2.2.4 Testing

Testing on a weekly basis is recommended to ascertain that the device operates as advertised by the manufacturer. If the device is dropped, the user should test the device as soon as possible.

5.2.2.5 Maintenance

The lenses of spotting scopes require daily cleaning with a cleaner and soft cloth recommended by the manufacturer.

5.2.3 Night Vision Devices

5.2.3.1 Principles of Operation

Night vision devices (also referred to as night vision goggles) operate by amplifying available light. Such devices can take small amounts of light, such as starlight, moonlight, or area-related ambient light, and convert the light energy into electrical energy. Electrons pass through a thin disk containing over 10 million channels. As the electrons pass through these channels, they strike the walls, releasing thousands of more electrons. These multiplied electrons bounce off a phosphor screen that converts them back into photons and enables the user to see an accurate nighttime view.

Until recently, all image-intensified night vision devices had one attribute in common—they all produced a green image output. A few manufacturers are currently marketing a full-color device.

5.2.3.2 Types of Night Vision Devices

Night vision devices are categorized by the following generations that reflect the level of technology in their development:

- Generation 0 (1950s). This device required an infrared light source to illuminate the observation area.

- Generation 1 (1960s). This device was the era of the "starlight scope." Still in limited use today, such scopes comprise three intensifier tubes connected in series. These scopes are bulky and heavy in comparison to today's technology.

- Generation 2 (1970s). Use of the microchannel plate (MCP) eliminated the need for back-to-back tubes. Size, weight, and image quality were greatly enhanced.

- Generation 3 (1970s–1980s). Two major advances in materials led to an increase in detection at greater distances in much darker conditions and a significant increase in the operational lifespan of the night vision device. The gallium arsenide photocathode and the ion barrier film on the MCP enabled these advances. Image Intensification (I^2) is a common name for the Generation 3 and 4 technologies.

- Generation 4 (1998). Filmless technology with no ion barrier or protective coating on the MCP created a 20-percent increase in performance. Unfortunately, the tubes showed immediate degradation since the protective film on the photocathode had been removed. This degradation also affected the lifespan of the device, reducing it below the 10,000-hour active life requirement of some branches of the military.

Note the following:

- "Army Navy/Passive Vision Sight" is a designation prefix for night vision equipment in the U.S. Department of Defense.

- Variable gain is an improvement capability that enhances the device's capability in variable lighting conditions. It provides the user with a rheostat to limit the amount of incoming light.

5.2.3.3 Characteristics and Applications

Night vision devices can provide valuable images during nighttime hours that could never be seen without such a device. Using a night vision device, the distinct image of a moving human can be captured from a distance of 1,000 meters to more than 2,000 meters (3,280 feet to more than 6,560 feet).

One weakness in the use of night vision devices is the lack of color in the images. Acceptable clarity because of a lack of depth perception in some models can be a concern. Furthermore, an adversary could use particular camouflage that would prevent the user of a night vision device from spotting the adversary. The field of view that the device provides should also be evaluated and should be consistent and appropriate for the type of surveillance and observation required.

5.2.3.4 Testing

Testing on a weekly basis is recommended to determine whether the device operates as advertised by the manufacturer. If the device is dropped, the user should test the device as soon as possible.

5.2.3.5 Maintenance

The lenses of most night vision devices require daily cleaning with a cleaner and soft cloth recommended by the manufacturer. Batteries need to be routinely checked and replaced.

5.2.4 Thermal Imager Equipment

5.2.4.1 Principles of Operation

Unlike a night vision device, a thermal imager needs no light to operate. Thermal imager devices can detect (see) heat and the movement of heat. Thermal imagers work in the 3-micron to 30-plus-micron wavelength of the infrared spectrum. This wavelength can be termed as thermal infrared. Thermal infrared is emitted by an object, not reflected off an object. This emission is picked up by the special lenses of thermal vision equipment, focused, and then scanned by a phased array of infrared-detector elements. The detector elements create a detailed temperature pattern called a thermogram, which is translated into electric impulses and then translated into data that can be displayed on the user screen.

5.2.4.2 Types of Thermal Vision Equipment

Thermal imagers are available in vehicle- or stationary-mounted, handheld, or weapon-sight packages. Various models can provide general all-weather use under all-light or no-light conditions. Some imagers can perform well in fog, smoke, rain, or snow conditions. Thermal imagers have two ways of indicating the presence of intruders: (1) "white hot" means that warmer objects in the picture are shown in white and (2) "black hot" means that warmer objects are shown in black.

Sources of heat from objects that are not of interest to the user can be distracting and may require a further investigation and a possible response by members of the security organization.

5.2.4.3 Characteristics and Applications

Thermal imagers have the ability to operate successfully under many types of conditions in which other surveillance devices are of no value (e.g., all levels of light, smoke, fog, rain, or snow). One of the biggest advantages of these devices is that camouflage used by adversaries to hide from thermal imagers is not effective.

Because thermal imagers can weigh several pounds, they are too heavy and cumbersome to carry for prolonged periods. Thermal imagers are more suited to permanent installations than temporary setup. The field of view that the device provides should also be evaluated and should be consistent and appropriate for the specific field application (e.g., a thermal rifle optic should not be used for wide-ranging area surveillance because the field of view provided is small). Methods used to shield the thermal signature of objects within the field of view may defeat thermal imagers.

5.2.4.4 Testing

Testing on a weekly basis and under different environmental conditions is recommended to determine whether the device operates as advertised by the manufacturer. If the device is dropped, the user should test the device as soon as possible.

5.2.4.5 Maintenance

The lenses of most thermal imager devices require daily cleaning with a cleaner and soft cloth recommended by the manufacturer. Batteries should be routinely checked and replaced.

5.2.5 Enhanced Night Vision (Fusion)

5.2.5.1 Principles of Operation

Enhanced night vision devices operate through the fusion of the I^2 tube and an infrared microbolometer designed into a compact monocular design. The combination through the overlay of these two technologies greatly expands the capabilities of a night vision or thermal imager device alone.

5.2.5.2 Types of Enhanced Night Vision Equipment

Enhanced night vision devices are available as a handheld observation tool or as a rifle optic. Some recent models allow the user to determine the percentage of night vision and thermal imager use to enhance viewing capabilities under particular circumstances. Figure 80 illustrates the use of an enhanced night vision device or fusion technology. The drawing on the left shows such a device set for 100-percent I^2 use. The drawing in the middle shows it set for about 50-percent I^2 and 50-percent infrared use. The drawing on the right shows it set for 100-percent infrared use. Obviously, different situations would require different settings to gain optimal information.

Sources of heat from objects that are not of interest to the user can be distracting and may require further investigation and a possible response by members of the security organization.

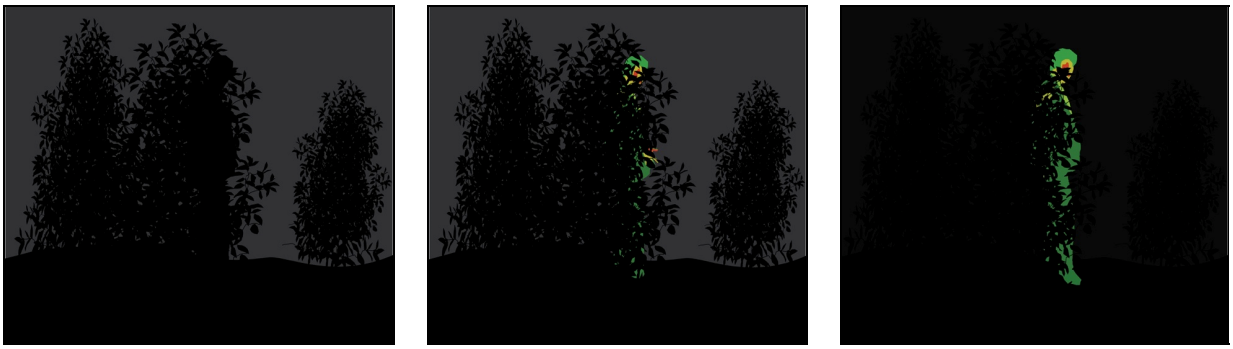


Figure 80 Use of an enhanced night vision device or fusion technology

5.2.5.3 Characteristics and Applications

Fusion technology combines thermal imager and night vision technologies and has the ability to operate successfully under many adverse conditions, excelling in poor-visibility environments that would impede other devices.

5.2.5.4 Installation Criteria

Installers should follow the manufacturer's recommendations.

5.2.5.5 Testing

Testing on a weekly basis and under different environmental conditions is recommended to ascertain that the fusion device operates as advertised by the manufacturer. If the device is dropped, the user should test the device as soon as possible.

5.2.5.6 Maintenance

The lenses of fusion devices require daily cleaning with a cleaner and soft cloth recommended by the manufacturer. Batteries should be routinely checked and replaced.

5.3 Premise Control Units

For an IDS, the detection phase typically begins as soon as a detector or sensor reacts to stimuli that it is designed to detect. The detector or sensor alarm condition is then transmitted over cabling that typically starts in a protected area and may transverse an uncontrolled area to another protected area to the premise control unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise a zone at the monitor station. A PCU is a device that receives changes of alarm status from detectors/sensors and transmits an alarm condition to the alarm monitoring station—typically the CAS and SAS. The PCU also allows authorized personnel to change the alarm zone status of the alarm zone.

To be useful, an IDS should have the capability to restrict status changes to only those who possess proper authority (e.g., alarm system administrators or alarm station operators). A system may restrict access to performing system functions in any number of ways, often with keys or codes used at the PCU or a remote PCU near an entry. High-security alarms may require multiple codes, a fingerprint, badge, hand geometry, retinal scan, encrypted response generator, or other means that are deemed sufficiently secure for the purpose.

To function as intended, the PCU must be located within the secured area to protect it from unauthorized access. The change of an alarm status may be delayed (for no more than 30 seconds) to allow completion of the entrance authorization process. Like the sensors, the PCU requires a primary power source for operation and should be connected to a backup power source to remain operable during the loss off primary power. The PCU should be equipped with a tamper alarm to detect attempts at unauthorized manipulation. All changes in status of the alarm zone must be transmitted to the alarm monitoring stations. Examples of reportable status include, but are not limited to, access/secure, tamper, loss of power, improper access code or procedure, test or maintenance mode, and masked sensors. The PCU can be configured with duress capabilities that will allow personnel to surreptitiously notify the alarm monitoring station of a compromised situation.

5.3.1 Transmission and Annunciation

The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. An additional signal is added to the communication for supervision to prevent compromise of the communication scheme (i.e., tampering or injection of false information by an intruder). The supervised signal is sent by the PCU through the transmission link to the alarm monitoring station (typically the CAS and SAS). A dedicated panel or a central processor inside the alarm monitor station monitors information from the PCU signals. When an alarm occurs, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure. To ensure transmission line security, the facility should use Class I or Class II line supervision (as defined below) when the transmission line leaves a protected area and traverses through an uncontrolled area.

5.3.1.1 Class I Line supervision

Class I transmission line security is achieved through the use of a data-encryption standard or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. To ensure Class I transmission line security, the data-encryption standard or the algorithm used should be certified by the National Institute of Standards and Technology or another independent testing laboratory.

5.3.1.2 Class II Line supervision

Class II transmission line security refers to systems in which the transmission is based on pseudorandom generated tones or digital encoding using an interrogation and response scheme throughout the entire communication or Underwriters Laboratories Class AA line supervision. The signal should not repeat itself within a minimum 6-month period. Class II transmission line security should also be protected against compromise using resistance, voltage, current, or signal substitution techniques.

Note that dc line supervision should not be used because it is highly susceptible to manipulation or substitution to circumvent valid alarm annunciation. Additional information on AC&D can be found in Section 6.

5.3.2 Intrusion Detection System Cabling

Facilities should avoid cabling designs that combine signal transmission lines and power source cabling into one of the two alarm monitoring stations or one common area before reaching the

alarm monitoring stations. Facilities should, to the extent practicable, ensure that the cabling (signal transmission and power) to each alarm station is sufficiently separated and not accessible to external manipulation. The separation and nonaccessibility of cabling provide a level of assurance that at least one alarm station will maintain the capability to perform required alarm station functions if the cabling is subject to an occurrence that results in the loss of functionality within the other alarm station. Key considerations in the design and installation of alarm system cabling are the prevention of unauthorized and external manipulation and minimization of the exposure to environmental conditions. Facilities should identify and evaluate intrusion detection and assessment system cabling that may be vulnerable to disruption by external manipulation (e.g., adversarial action) and should consider further protective measures, such as hardening or periodic surveillance.

The cabling between the sensors and the PCU should be dedicated to the intrusion detection equipment for which it provides service and should comply with national and local code standards. Cabling should be installed in metal conduit between the alarmed area(s) (i.e., controlled access area, vital area, or material access area), the PCU, and the alarm monitoring stations. Exceptions may apply when the cabling is not easily accessible, such as when it is run underground, traverses or is within another controlled area, or is encrypted with Class I or II encryption.

5.4 Entry Control Systems

If an entry or access control system, or both, is integrated into an IDS, reports received in the alarm stations from the automated entry control system should be subordinate in priority to reports from intrusion alarms. Section-6 presents additional information on AC&D.

5.5 Power Supplies

Primary or normal power sources for intrusion detection equipment may be commercial alternating current (ac) or dc power. If the primary power fails, the system should be designed to indicate that the IDS is operating on secondary, backup, or emergency power sources without causing false alarm indications. Section 7 presents additional information on backup and emergency power.

5.5.1 Backup or Emergency Power

Backup or emergency power should enable intrusion detection equipment to remain operable during the loss of primary/normal power. An emergency or backup power supply should consist of a protected independent power source that provides a minimum of 8 hours of continuous operation. Batteries used for emergency power should be maintained at full charge by automatic charging circuits. The facility should follow the manufacturer's periodic maintenance schedule and document results.

5.5.1.1 Power Source and Failure Indication

A visual (illuminated) and audible indication of power failure should be provided at the PCU of the power source in use (ac or dc) and in the alarm monitoring stations. Equipment at the alarm stations should indicate a failure in power source, a change in power source, and the location of the failure or change.

5.6 System Considerations

5.6.1 Maintenance Mode

When an alarm zone is placed in maintenance mode, this condition should be signaled automatically to the alarm monitoring stations. The signal should appear as an alarm or maintenance message at the alarm stations, and the IDS should not be securable while in the maintenance mode. The alarm or message should be continually visible at the alarm stations throughout the period of maintenance. A standard operating procedure should be established to address appropriate mitigative actions when maintenance access is indicated at the panel. A record of each maintenance period should be archived electronically in the system or on other electronic media or printed in hardcopy in accordance with site procedures. A self-test feature should be limited to 1 second per occurrence. Section 6 presents additional information on AC&D.

5.6.2 Shunting or Masking Condition

Shunting or masking of any alarm zones or sensors should be appropriately logged or recorded in the archive. The alarm monitoring stations should display shunted or masked alarm zone or sensor throughout the period that the condition exists. Section 6 presents additional information on AC&D.

5.6.3 Component Tamper Protection

Intrusion detection equipment components (to include all sensors, control boxes, and junction boxes) should be equipped with tamper protection and indication to provide deterrence, delay, and detection of attempted unauthorized manipulation.

5.6.4 System Component Status Changes

No capability should exist to allow changing the status of the IDS from a location outside the protected area. All PCUs should be located within a secure area that is equipped with intrusion detection capabilities that annunciate in the alarm monitoring stations. Only alarm station operators or authorized technicians should initiate status changes for IDS equipment and associated access control equipment. A device, password, or procedure that verifies the authorization of an individual to make such changes should be used to restrict operation of the PCU. For applications of increased security, status changes for IDS equipment and associated access control equipment may require confirmation from an additional system operating authority before the change is allowed to occur (e.g., a concurrence action from an alarm station operator confirming the status change initiated by the other alarm station operator or authorized technician).

5.6.5 False or Nuisance Alarms

A false alarm is an alarm generated without apparent cause. False alarms are generally attributed to electronic phenomena from the sensor itself or the electrical infrastructure of the sensor system. Alarm signals transmitted in the absence of detected intrusion or transmitted when the cause cannot be verified as a nuisance alarm are false alarms. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but that is not related to an intrusion attempt. To validate detection, all alarms must be assessed and may require further investigation to determine their cause. The results of all alarms should be

documented. The design goal of an IDS should be to limit false alarms and nuisance alarms to a total of not more than one false alarm per zone per day and one nuisance alarm per zone per day. A sound maintenance program is often a key factor in minimizing the number of false and nuisance alarms an IDS generates.

Alarm records should be maintained for effective preventive maintenance. These documented records support effective preventive maintenance. These records should include a daily nuisance alarm log. A daily nuisance alarm log can aid in the tracking of equipment or sectors where maintenance is required. This log should contain an assessment of the cause of the alarm and should be referenced by alarm sector; specific location within the sector; and, as applicable, component serial number, which provides unit-specific tracking. The log enables problems related to a specific alarm sector to be investigated and identified for corrective action.

5.6.6 Installation, Maintenance, and Testing

Proper system installation, maintenance, and testing contribute to acceptable system performance and minimize its vulnerability to defeat. The defeat vulnerability of a sensor is an inherent characteristic of the sensor technology, how it is installed, and how sensors are configured within the system. For an effective detection system, intrusion detection sensors must be selected and properly installed to maximize the detection probability, minimize the nuisance alarm rate, and minimize vulnerability to defeat. Intrusion detection and assessment systems and components should be installed, maintained, and tested in accordance with manufacturers' specifications, which account for system design, application, and performance. For IDSs that are integrated with other components of the physical protection system, the specific configuration of all integrated components should be evaluated to ensure that the system performs its intended function and provides the desired level of protection. Before installation, the planned configuration of PIDASs, physical barriers at the protected area perimeter (including any associated nuisance barriers), and the isolation zones should be evaluated to ensure that the planned perimeter system design will satisfy the detection and assessment goals of the physical protection program. After installation, the configuration of these components should be reevaluated based on the zone of detection provided by the IDS when it is operating to ensure that it provides the required coverage and eliminates the potential for unauthorized bypass. The configuration of the components of the protected area perimeter (intrusion detection and assessment systems, physical barriers, and the isolation zones) when combined with the IDS zone of detection should account for common defeat methodologies (e.g., walking, crawling, running, climbing, jumping, or bridging) consistent with the design goals of the physical protection program. For this reason, perimeter IDS testing should include all defeat methodologies that could be used to defeat the system. For safety considerations, simulations of certain defeat methodologies (e.g., jumping, bridging) during testing may be necessary.

Only trained and qualified personnel should perform IDS or component installation, maintenance, or testing in accordance with applicable manufacturer's recommendations. All installation, system settings/sensitivity levels, maintenance, and testing activities should be documented for use in supporting system or component troubleshooting and ensuring proper performance, maintenance, and testing intervals.

To ensure that a system or component continues to provide the level of protection intended, maintenance, testing, and calibration activities should be performed at intervals consistent with manufacturers' specifications and the operational demand placed on the system or component. Most system and component manufacturers have established similar testing criteria, especially

in the area of testing frequency. The sections below describe general manufacturer recommendations regarding intrusion detection and assessment system testing intervals.

5.6.6.1 Acceptance Testing

When first installed, a sensor must be tested before it is formally "accepted" as a part of the physical protection system. Acceptance testing consists of (1) a physical inspection to ensure proper installation of the sensor and (2) a performance test to establish and document the level of performance.

5.6.6.2 Performance Testing

Performance testing should be conducted every 6 months or whenever a system or component is returned to service after modification, repair, maintenance, or an inoperable state. The performance test should include the use of the documented levels of performance from the original acceptance testing to verify that the system or component is still performing adequately.

5.6.6.3 Operability Testing

For systems or components in continuous operation, operability tests should be performed weekly (once every 7 days) to confirm that the sensors are operational and that alarms are communicated to the alarm station display system. The facility should perform testing on a portion of the total sensors over a distributed time period to test some sensors during different times of the day within the 7-day timeframe. Subsequent testing should ensure that each sensor is tested during a different time of day than that of the previous test. When conducting perimeter IDS operability testing in conjunction with perimeter assessment equipment testing, varying the time of day a sensor is tested enables the verification of assessment capabilities during the varied illumination conditions of daylight and at night.

6 ALARM COMMUNICATION AND DISPLAY

6.1 Overview

In general, AC&D systems should have the following qualities:

- A data communication subsystem should move alarm data in a timely manner. Alarms should be communicated to the alarm station operator within 2 seconds[2] of sensor activation, although less than 1 second is preferred. The data communication subsystem needs to be fast enough to allow the overall alarm system to meet these times. Alarm timing is measured starting at sensor activation and ending at alarm display (visual and audible) to the alarm station operator.

- The data communication system should be robust with no single-point failures between field panels and the alarm stations.

- Single-point failures are defined as the loss of the entire or a significant portion of the detection and assessment system capability through the loss of any single critical component/communications link.

- A critical component/communications link is one that, if it fails, the detection and assessment capability of the security system would be completely or significantly degraded and would therefore require security force personnel to replace the functions of detection and assessment to maintain the security system's effectiveness. Intrusion detection and assessment systems should have no single component, link, or location that, if it fails, would degrade the continued detection and assessment capability of the remainder of the system.

- Redundancy refers to the ability of the system to complete the same task through multiple means. The system should be designed with redundant data communication links. Redundancy is recommended between sensors and field panels.

- The alarm system and associated data communications systems should not lose any intrusion or entry control alarms, events, tamper alarms, state-of-health messages, or any other alarm necessary to meet the level of protection of the system design.

- The system should provide automatic notification to the alarm station operator when components of the intrusion detection and assessment system fail. This state-of-health monitoring should be continuous, and any faults should be reported to the alarm station operators within 2 seconds although a 1-second notification time is preferred. In addition, the system should notify alarm station operators when components return to proper operation.

- The data communication system should be highly reliable with minimal downtime for repair.

---

[2] A standard time for many security applications is 2 seconds. Refer to Section 6.1.2.2.

- The overall system should continue to operate in the event of a component failure caused by destruction or tampering at a single physical location.

- The system should be designed to provide automatic "failover" to the greatest extent practicable to enable continued detection and assessment when single components, communication links, or locations fail. Failover refers to the ability to switch to another resource if one component fails (e.g., the central processing unit for the CAS fails over to the central processing unit for the SAS).

- Upon restoration of failed equipment or data communication links, the system should return to its original state within 30 seconds. No alarms should be lost while the system is returning to its original state.

- Upon system restoration, the system should be capable of sustaining another failure at a single physical location and still maintain the capability to perform as designed.

6.1.1 Line Supervision/External Connections

In a high security environment, all computer security networks are dedicated solely to security operations. The computer security network should not be connected to the Internet or other local or wide area networks that are not related to security. When communicating between remote sites,[3] all data communications should be encrypted to the level corresponding to the sensitive unclassified or classified nature of the data communications. All system components should be protected against tampering and unauthorized manipulation. Detection, assessment, and access control devices that communicate using RF communications are not recommended for use in high-security applications because RF signals can be interrupted or jammed and, therefore, could inhibit equipment performance.

Good alarm communication systems continuously detect failures of and tampering with critical components associated with alarm detection, transmission, and annunciation and report such events to the alarm station console. (Section 6.1.2.2 presents information on timing issues.) The data communications system supports line supervision as detailed in Table 9.

To protect the system from unauthorized manipulation (e.g., hackers or others having malevolent intent), a security local area network, if used, should not be connected to any external computer network. The security system should operate on a standalone network that does not require connections to any external network. However, for associated entry control systems, the standalone system could allow (through firewalls and other information technology equipment) temporary or one-way connections to external networks to import badge information encrypted to the line supervision Class A standard. Detection, assessment, and access control devices that communicate using RF communications are not recommended for use in high-security applications because RF signals can be interrupted or jammed and, therefore, could inhibit equipment performance. System developers need to protect and secure communication equipment and media against unauthorized access. Equipment cabinets and field hardware containing electronic equipment or cable patch panels should employ tamper alarms to achieve this function.

---

[3] Remote sites are those that, because of their location, are not part of the internal data communications systems (e.g., another location must use public lines because dedicated lines are not available).

6.1.2 Alarm Handling

6.1.2.1 Alarm Display Information

Current AC&D systems use both text and graphic displays to uniquely identify alarms to an alarm station operator. Many types of information can be displayed, but some of the more important information includes the following:

- mode of any sensor

  Mode refers to the status of a sensor. Is the device being monitored or ignored? Is the sensor online or offline? Other standard terminology includes "access" or "bypass," which means the same as offline.

- status or state of an event

  Alarm status (state) can include alarming (detecting) or secure (no detection).

- time of events

- location of events

At a minimum, the alarm station console should display the following information for alarm events:

- visual and audible annunciation of the alarm
- alarm type (e.g., intrusion, duress, tamper)
- alarm location
- time of alarm
- site-specific sensor identifier (a minimum of 64 characters is desirable)
- sensor state (i.e., alarm, secure, tamper)
- sensor mode (i.e., access, secure, offline)

Configuring the system to meet the needs of the site or facility is important. System flexibility is desired (e.g., users should be able to configure the system to direct a particular alarm, tamper, or system event to the desired console). The system should be able to direct an event to more than one console (e.g., sending all intrusion alarms to both the CAS and the SAS consoles). Administrators should be able to direct alarm events to consoles based on their location, priority, or sensor type. Figure 81 shows an example of an alarm station console display. All displays should be approximately perpendicular to the operator's line of sight and should be easily visible from the normal working position.

Text and graphical displays need to be synchronized. Operations performed on a text display should, as needed, cause the graphics display to update. Operations initiated through the graphics display should, as needed, cause the text display to update.

The AC&D system should have synchronization of all internal "clocks" of all computers and subsystems to a single time base. It is recommended that the system use the network time protocol to perform this synchronization. System administrators should ensure that the system is synchronized and configured to display time as the security force requires (usually in the local time zone or universal time).

6.1.2.2 Alarm Timing

Intrusion detection alarms need to be timely so that alarm station operators can assess the alarms and dispatch response forces, as appropriate. In general, alarms, tampers, and system faults need to be annunciated in a timeframe that is a small fraction of the total response time. The IDS timing should be maintained at all times, regardless of other activities happening on the system.

Figure 81 An optimal arrangement of AC&D monitors

"Time to report" is measured starting from the activation of the sensor, tamper, or component failure and ending when the alarm displays to a human operator in an alarm station. For most high-security system applications, alarms should be reported within 1 to 2-seconds of sensor activation.

In malevolent or attack situations, many IDS alarms will annunciate simultaneously. The system needs to handle malevolent situations without failing and without losing any of the multiple alarms. The system should be able to handle up to eight simultaneous alarms (i.e., eight alarms in 2 seconds) and should be able to count and display the number of unacknowledged alarms within 2 seconds of receipt of those alarms. The system should display the first alarm received and indicate the number of remaining alarms. In situations of multiple alarms, tampers, or system faults, the system should not fail or lose any alarm events.

The IDS should be designed to handle an increased frequency of alarms and system event notifications without prohibiting the alarm station operator from performing alarm acknowledgment activities on the console. When multiple alarms inundate the alarm console display, the number of unacknowledged system events, alarms, or tampers should not prohibit the proper display of subsequent events.

6.1.2.3 Alarm Priorities

Some IDS events, such as intrusion alarms and tamper alarms, are considered to be higher priority than other system events. In some cases, alarms received from specific intrusion sensors may be considered higher priority than others. The system administrator should assign

priority levels to system events within the IDS consistent with the site protective strategy and the objectives of the physical protection program. The system software should not make assumptions or place constraints on the priority assigned to a particular event.

The IDS must be able to prioritize the display and handling of system events that include, but are not limited to, the following:

- intrusion alarms from interior or exterior sensors
- equipment tampers
- system faults
- data communication system faults, failures, or tampers
- ac power loss
- access control alarms and events
- low-battery alarms
- duress alarms

Prioritization of events is a site-specific decision that a facility should determine after considering the elements of the physical protection program, the site's protective strategy, and the geography of the site. A good AC&D system should allow the assignment of priorities to events based on location or event type; however, exact priority assignments are site decisions.

The IDS should automatically handle the organization of incoming events. Normally, events are displayed in order of their priority and then by time of arrival. Administrators also need the capability to assign the same priority to different events (e.g., all alarms and tampers may have the same priority). In addition, the system should allow alarm station operators the flexibility to handle any event out of its priority order.

6.1.2.4 Alarm Logging and Reporting

Alarm logging lets the system maintain a historical record of alarms so that alarm station operators, system administrators, or other authorized personnel can access a list or log of all system events and activities. The AC&D system should have the capability to export system log files into commonly used file formats for reporting or analysis. The alarm log should provide a record of all alarm events and all system events.

Other useful information for the alarm log could include the following:

- time of operator acknowledgment
- time of operator cause assessment (completion of operator action)
- a "tagging" ability so that the operator can tag an alarm event with its cause

Using the log, the system should be capable of producing reports of alarm activities and providing the numbers and types of alarms based on their cause or location.

The following examples of reports are beneficial in evaluating the continued health and maintenance needs of the system:

- Nuisance and false alarm reports detail the total number of alarms, false alarms, and nuisance alarms (based on cause) per sensor zone (location) for a user-selectable time period.

- Sensor grouping reports are based on type or location. In particular, these reports are useful for interior sensors and exterior sensors.

To avoid tampering by an insider, the IDS should prevent alarm station operators from deleting saved events. In addition, the system should be designed or programmed to ensure that an alarm station operator or system administrator cannot change the status of a detection point or deactivate a locking or access control device without the knowledge and concurrence of the alarm station operator in the other alarm station.

A system with several automated features and capabilities can aid alarm station operators and administrators. For example, an AC&D system should be able to log events and save them; when the log is full, the system should have an archive capability to save the information in a long-term storage medium. If the alarm reporting log or storage space (such as a hard disk) becomes filled to capacity, the system should not fail or lose information. A full system log should not cause the IDS to fail or degrade its performance. System capabilities may include the following:

- The system should have automatic notification (such as an e-mail to the administrator) when the log space becomes limited. The system should generate an “Alarm Log Full” report at helpful intervals, such as 80 percent full, 90 percent full, and 95 percent full. Users can archive the log files before any information is lost or new information cannot be added.

- The system should have an archive capability to move the log information to removable media (e.g., compact disks, digital video disks).

6.1.3 Closed-Circuit Television Guidance

Intrusion detection and assessment systems should interface with the alarm station console to provide automatic, integrated operation enabling a CCTV assessment system to automatically display video images in the area of the detected activity upon receipt of an alarm. The system should also enable manual switching of assessment assets in response to the alarm station operators’ commands to provide increased capabilities for assessment.

When evaluating candidate systems, physical security analysts can use the following guidance to help determine the suitability of the CCTV system. Important elements that CCTV system purchasers or maintenance personnel may consider include the following:

- The CCTV should be able to display live video from any camera and to record video from any camera. In addition to the automatic, integrated operation capability, the CCTV system should enable an alarm station operator to manually control the switching of camera displays. The CCTV system should automatically record video before the alarm event and, upon receipt of an IDS alarm, should continue to record for a short time after

the alarm is received to enable video recall for further assessment. In addition, the CCTV system should be able to archive past events on a removable medium.

- The CCTV system should have a minimum equipment set of four CCTV monitors, two primary assessment monitors (live and recorded), and two surveillance monitors for the operators to view video scenes generated by the site cameras.

- Although a minimum equipment set is suggested, the CCTV system should be designed to accommodate the site-specific needs consistent with system configuration and overall size.

6.1.3.1 Assessment Monitors

Monitors dedicated to assessment are under the control of the AC&D system. These monitors play the live and recorded video from an alarm sector when the IDS detects activity within the zone of detection. If no alarm event is being handled, the monitors are either blank or show the highest priority unhandled alarm available to the AC&D system.

The monitors are normally blank unless an alarm is being assessed or the alarm station operator has requested a particular view. When a view is selected by the operator either for the purpose of alarm assessment or status determination, one of the primary CCTV monitors automatically displays live video coverage from the CCTV camera covering the area requested. If the view contains an alarm, the other primary monitor displays the alarm scene coverage that was recorded automatically on the recorder when the alarm occurred. In most cases, recorded alarm video is looped to repeatedly show the few seconds of video before and after the alarm event. If the scene does not contain an alarm, no recorded view is present.

The following scenario describes how a system could automatically process alarm video with involvement from an operator:

- When two or more alarms are awaiting assessment, the monitors should show the highest priority live and recorded video scenes unless the alarm station operator has chosen to view a lower priority alarm. Upon completion of an assessment by the alarm station operator, the system should automatically display the remaining video (live and recorded) of the highest priority alarm.

- At all other times, these monitors may be blank. The system should not replace the primary monitor scenes until the operator either ends the assessment or selects a new alarm.

- Alarm station operators may view specific alarm sector video by selecting appropriate sectors or sensors on the AC&D console. The AC&D system then displays the live video for that sector. Thus, the assessment monitors are under control of the AC&D system while the AC&D system is under the control of the alarm station operator.

- In some instances, two additional assessment monitors might be required for alarm zones that use two video cameras for full-video coverage of the zone. In most cases, however, a proper sector design requires only a single camera for assessment.

6.1.3.2 Surveillance Monitors

The free monitors that are not primary alarm assessment monitors should be available to the alarm station operator for surveillance purposes. Alarm station operators should have the capability to assign a camera from any camera view to show live scenes on these surveillance monitors at any time. If one of these monitors shows a scene in which an alarm occurs, the live scene coverage for the alarming sector will be duplicated, and the live scenes will be displayed on the free monitor and on the assessment monitor. These monitors are under the control of the operator, not the AC&D system.

6.1.3.3 Prealarm and Postalarm Video

In addition to live presentations, the system should interface with a video-recording subsystem to provide a record of alarm events and to allow alarm station operators to replay the camera images from the alarm. Recording capabilities should be automated and should be actuated by alarm signals. The alarm station console can be the main place to control the video-recording system. The system needs to record image frames at a sufficient speed to capture the cause of the alarm. Display monitors need the capability to view both the current live camera information and the recorded information.

Within the recorded video frame(s), the time, date, and location need to be embedded and displayed in the image for current and future reference.

For assessment video recording, video should be recorded several seconds before and several seconds after (prealarm and postalarm video) an alarm event. A good general range of prealarm and postalarm video clips is 3 to 10 seconds, with about 5 seconds being optimal. The AC&D system and associated video-recording systems should allow prealarm and postalarm clip recording times to be adjusted for site conditions.

The alarm station operator needs the ability to display any camera image to a surveillance video monitor at any time. Even if new alarms are occurring, any video being displayed on the assessment monitors should not be removed from the monitor unless commanded by the alarm station operator. However, CCTV systems need the capability to alert the operator or to call the operator's attention to an alarm displayed on a video recorder/monitor. The system should not constrain the operator (e.g., the operator may need to select video information associated with another incident out of priority order).

A CCTV system should detect and report tampering and loss of video signals.

6.2 Alarm Communication and Display Systems

6.2.1 Alarm Communication and Display

6.2.1.1 Principles of Operation

The primary objective of a physical security alarm system is to communicate alarm events received from sensors to a human operator. The goals of the system are to report alarms in a timely manner, never lose alarms, and survive any single-point failure with minimal or no degradation in system performance. For a system to be effective, it must be able to operate under all conditions and continue to operate even when individual components or primary data

communication paths fail, which is why redundant data communications capabilities are important.

AC&D supports the assessment period, which is the first phase that requires human or operator interaction. When an alarm condition occurs, the operator assesses the situation and then takes the appropriate action (e.g., dispatches a response force, if appropriate). The response phase begins as soon as the operator assesses an alarm condition. The response phase should also determine the precise nature of the alarm and take all measures necessary to safeguard the protected area.

6.2.1.2 Types of Alarm Communication and Display Systems

A variety of manufacturers produce AC&D systems. These systems rely on commercial, off-the-shelf computers and network components but are customized through proprietary software created by the manufacturer. When investigating potential vendors of AC&D systems, security analysts should have already defined the needs of the specific facility. In addition, security requirements and specifications for the AC&D system should be defined in advance to assist in evaluating vendors' offerings.

6.2.1.3 Sources of Nuisance Alarms

The AC&D system is not a significant source of nuisance alarms. Low-probability communications faults have been known to introduce nuisance events, but recent changes to the communications equipment used in alarm systems have greatly reduced even this low probability. Remote power sources (e.g., those at field panels) can cause nuisance alarms. The primary source of nuisance alarms comes from sensors, not from the AC&D system.

6.2.1.4 Characteristics and Application

The AC&D is the system that transports alarm and assessment information to a central point and displays the information to an alarm station operator.

AC& D systems should be easy for an alarm station operator to use. Although IDS sensors can provide a lot of data, these data should be displayed in a fashion that presents the essential information to the alarm station operator. In addition, the alarm station operator should not be overwhelmed with data, interaction with the system should be efficient, and the alarm station operators should be able to perform their functions quickly and easily.

The following are characteristics of an AC&D system:

- The AC&D system should be designed to withstand the environments in which they are placed.
- AC&D components should be designed to last a long time (i.e., they should be highly reliable or have a long mean time between failure frequency).
- An AC&D system should provide redundant or backup capability, or both for critical components.
- Alarm information should be available to alarm station operator in a timely manner. The AC&D speed should be a negligible factor in calculating response or assessment times.

- The AC&D system should be secure from attacks by adversaries.

6.2.1.5 Installation Criteria

An AC&D system is somewhat different from a sensor in that limited, specific criteria apply to all possible systems. One criterion for the installation of an AC&D system and its communications and power is that these systems must be installed in accordance with the National Electrical Code, which is the case with many industrial electrical components.

In general, AC&D vendors have either specific installation criteria or instructions that purchasers of these systems must follow. Many vendors allow only fully trained and qualified distributors to install their systems. For other systems, a team of properly trained engineering and technical personnel will be necessary to correctly install a complex AC&D system. An AC&D vendor is the best source of information on the criteria necessary for installing an AC&D system.

6.2.1.6 Testing

6.2.1.6.1 Failover Testing

The AC&D system will occasionally fail because of power outages or component failures. Failover testing involves the ability to simulate these power or mechanical failures and then check the system to ensure that it responds accurately to system failures. Failover testing should do the following:

- Identify all critical components through the use of fault tree analysis (refer to Figure 82) or similar techniques. The fault tree allows analysts to explore all the components of a system and define all the events (single or in combinations) that could cause a system failure. Using standard logic symbols, analysts build system maps to show all the undesired system states and the components that could contribute to a system failure. The fault tree analysis technique has been used in safety and risk engineering for the determination of safety hazards.

- Identify the causes of failure for all components discovered during fault tree analysis (e.g., servers, workstations, switchers, routers, other data communications devices, and power sources).

- Cause failures in various components of a system.

- Verify that the system continues to communicate data and display alarm information before, during, and after such failures.

- Verify that the system is restored to its original state once the failure is removed and that alarms continue to be captured, communicated, and displayed during the restoration.

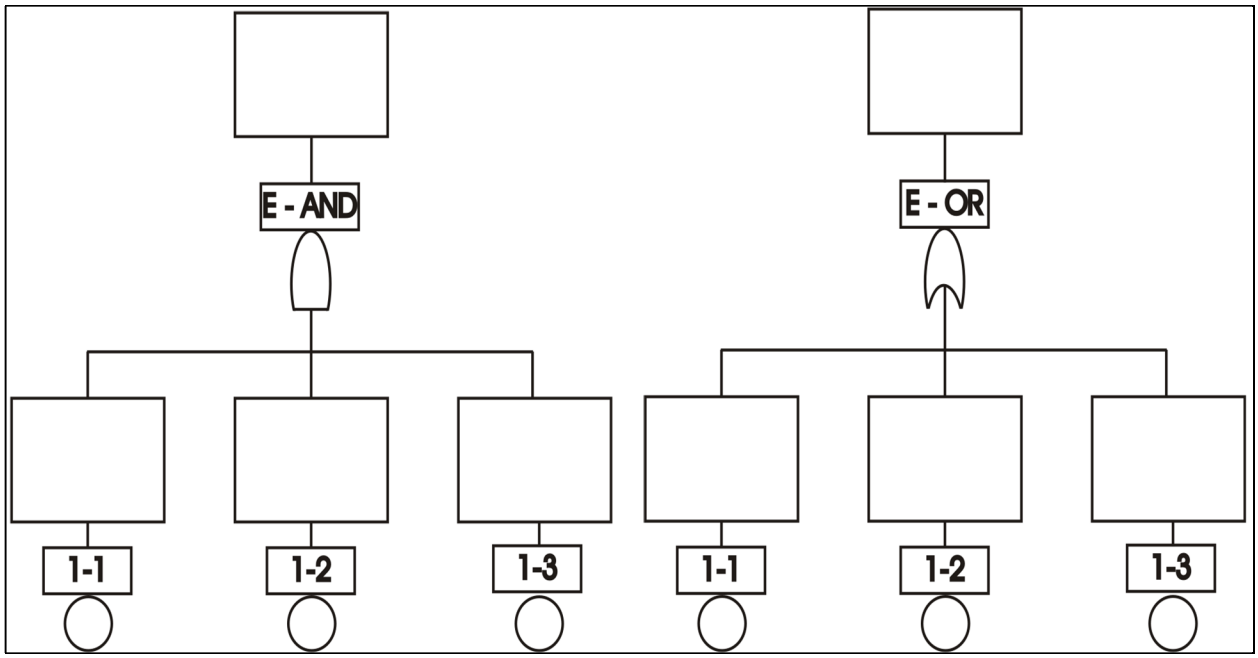


Figure 82 Fault trees used to analyze system events

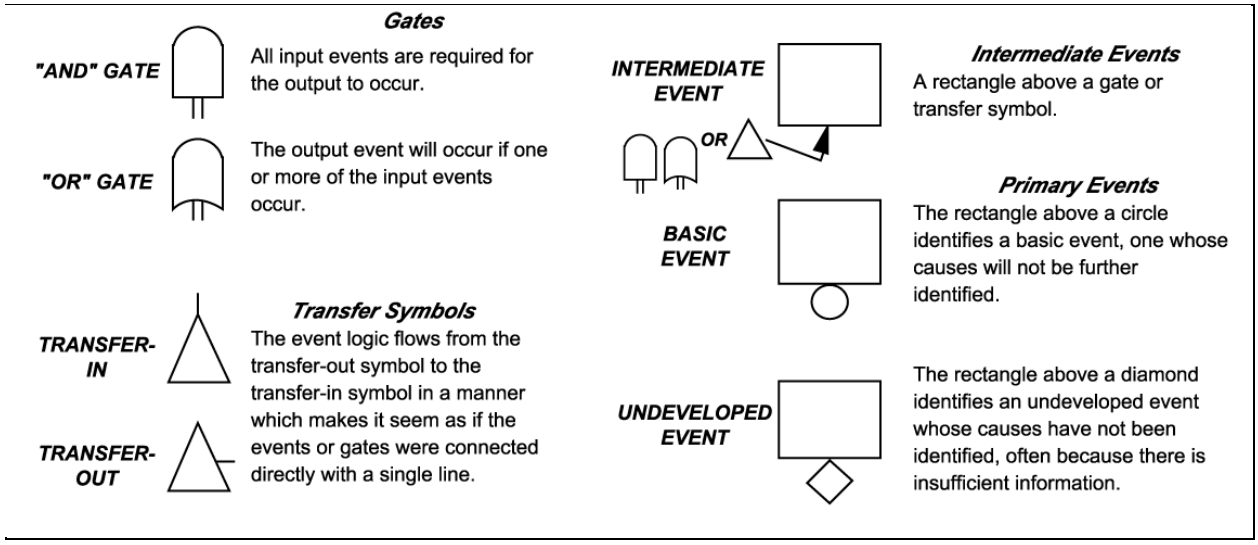


Figure 83 Symbols used in the graphical representation of a fault tree

6.2.1.6.2 Acceptance Testing

Acceptance testing is typically performed at installation to verify that the AC&D system meets all specifications. Acceptance testing typically consists of tests that challenge and demonstrate the performance criteria associated with the manufacturer's specifications. Acceptance tests should be conducted anytime the AC&D system software changes or major hardware additions are installed.

6.2.1.6.3 Performance Testing

Performance testing of the AC&D system is typically done as part of the acceptance test process. Those requirements that have a measurable performance metric are tested appropriately (e.g., timing tests measured with external time measurement devices). In general, the AC&D system performance changes only when hardware or software changes are made. A good AC&D system has little degradation or component drift, which distinguishes the system from its associated sensors. A semiannual performance test is recommended. A performance test should also be conducted after major hardware or software installations.

6.2.1.6.4 Operability Testing

Operability tests should be conducted during the normal operation of the system. In most cases, AC&D operability can be tested by performing sensor and video operability tests and observing that generated events are displayed properly on the AC&D console.[4] Table 10 shows an example of AC&D operability testing.

Table 10 Operations Testing Matrix

Required Feature	Test To Ensure Operability
Time, date, and location are embedded in the image of the recorded video.	Alarm station operator inspects console display of the recorded video for the time, date, and location.
Video should be recorded several seconds before and several seconds after (prealarm and postalarm video) an alarm event.	While an alarm station operator works at the console, a security officer should perform a test of the IDS at the desired location. The alarm station operator inspects the console display of the recorded video for the site-specified number of seconds for prealarm and postalarm video.
Any camera image should be displayed to a surveillance video monitor at any time.	Alarm station operator ensures that all cameras respond to commands to display on the system in the order chosen by the operator.
CCTV systems should detect and report tampering and loss of video signals.	While an alarm station operator works at the console, a security officer should perform an intentional tamper with the CCTV apparatus to cause an alarm to annunciate at the console. To test for loss of video signals, the security officer in the field should turn off the camera to ensure that the alarm station operator receives a system notification of the signal loss.

6.2.1.7 Maintenance

A strong, proactive maintenance program should be in place to maintain the AC&D subsystem. Manufacturers of AC&D systems have specific recommendations on maintenance requirements. The appropriate maintenance personnel should be on site or on call to meet the “mean time to repair” requirements specified by the vendors or should be available to meet the site-specific requirements that may vary depending on the environmental conditions at the facility.

---

[4] Many sites conduct ongoing operability tests (weekly or monthly) throughout the year on a schedule that ensures that all alarm points are covered at least once per year. Other effective schedules are possible.

7 POWER SOURCES FOR CRITICAL SECURITY SYSTEMS

7.1 Sources of Emergency and Backup Power

7.1.1 Emergency and Backup Power System

7.1.1.1 Principles of Operation

The primary power source for critical security systems and components for a limited area should come directly from the normal onsite power distribution system or directly from the public utility. Because of the potential for a loss of power, whether such loss is caused by a natural phenomenon (e.g., weather) or by a malicious act committed by an adversary, a facility should have reliable backup or emergency power sources, or both, on site that will provide power when needed. Institute of Electrical and Electronics Engineers (IEEE) Standard 692-2013, "IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations," contains additional guidance.

All critical security systems and components, including the following, should have emergency and backup power capabilities in case of a loss of primary power if they are required to function as intended to maintain a high physical protection standard:

- intrusion detection equipment
- assessment equipment (CCTV systems)
- illumination equipment (lights required for assessment cameras)
- automated access control systems
- alarm monitoring systems
- nonportable communications equipment

These power sources should have an automatic switching capability to the auxiliary source of power (battery or generator, or both) that will function immediately without causing false alarms and without causing a loss of system function or data (refer to Figure 84).

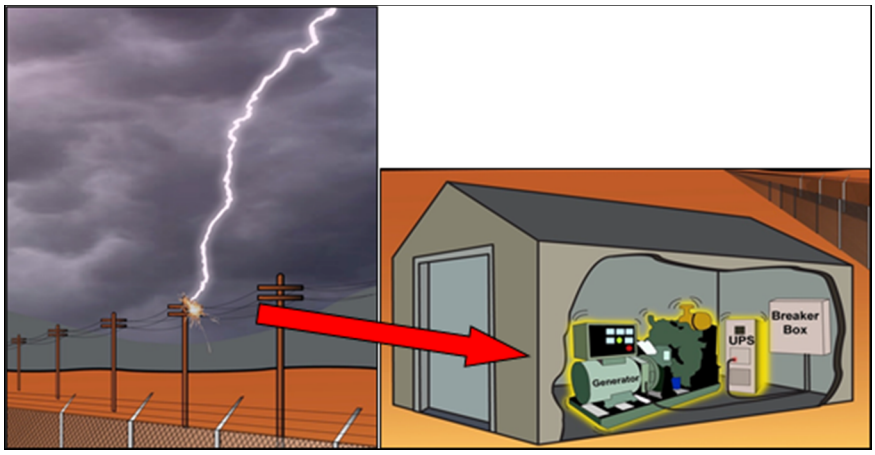


Figure 84 Emergency and backup power supplies used in the event of a loss of power

Alarm stations should be designed such that they will automatically receive an alarm indicating any of the following conditions:

- The primary power source has failed.
- The facility has transferred to an emergency or backup power source.
- The emergency or backup power source has failed.

The design and selection of emergency and backup power sources should consider site-specific conditions for the capability to restore primary power. The capability of emergency and backup power sources to sustain system operations should be based on the timeframe necessary to restore primary power as derived through a site-specific analysis.

7.1.1.2 Types of Emergency and Backup Power Supplies

Although a wide variety of emergency and backup power mechanisms are available, most facilities use the following three primary categories:

- UPSs
- batteries
- generators

7.1.1.2.1 Uninterruptible Power Supplies

Uninterruptible power supplies are typically used to supply an uninterrupted source of power to important instrumentation and control systems, enabling continuous operation during the loss of normal power without loss of system or component functionality. They are also used to provide continuous, quality power for systems sensitive to disturbances occurring in an electrical power distribution system caused by switching, faults, or power transfer. Designs for UPSs may include various combinations of batteries, rectifier/charger, battery transfer, bypass switch, and inverter. Most UPS systems are placed between the primary power source and the component it protects, effectively funneling all power at all times while keeping its own batteries charged.

7.1.1.2.2 Battery Systems

A battery system includes all switchgear and distribution equipment necessary to provide quality voltage and current as required by the connected load. The batteries are normally in full float operation whereby they are connected in parallel with a charger and the load and the charger supplies the normal dc load plus any self-discharge or charging current, or both, required by the battery.

7.1.1.2.3 Generators

A generator is a device that uses electromagnetic induction to convert mechanical energy to electrical energy. For most industrial applications, a diesel engine supplies the mechanical energy. A generator, when properly sized and designed, will provide reliable electrical power to the intended load equipment for the required amount of time.

7.1.1.3 Sources of Nuisance Alarms

Sources of nuisance alarms do not apply to this discussion.

7.1.1.4 Characteristics and Application

When identifying the system functions for a backup power source, the discussion of system functions in the system design description should address the effects of both normal and backup power source failures, any need for electric power for safe shutdown of the applicable system(s), and prevention or mitigation of credible accidents.[5]

The backup power source should have the capability to perform its required function over the expected range of environmental and load conditions independent of the normal sources of power. The environmental considerations should include the effects of anticipated operating conditions and failed plant equipment that may have an adverse impact on the ability of the backup power source to perform its function.

The backup power source, associated distribution systems, and necessary support systems should be protected against those events likely to produce a loss of normal power. Examples of such events are hurricanes (high winds), tornadoes, floods, snow or ice storms, lightning, fire, and seismic events. The level of protection should be related to the expected frequency and consequences of total loss of ac power caused by the particular event.

Facilities should coordinate output breaker protection and load breaker protection in accordance with National Fire Protection Association 110, "Standard for Emergency and Standby Power Systems." A fault on an individual load or circuit should not trip the output breaker of the backup power source. Output breakers should have an interrupt rating greater than or equal to the maximum available fault current at its location. Output breakers should be located such that a fire at the backup power source will not damage the bus feed circuit downstream of the output breaker. This should prevent a fire at the backup power source from causing the loss of ability to feed loads from the normal source.

The following list gives examples of requirements that may be addressed in the discussion of requirements and bases in the system design description:

- load lists with load power requirements and load functions
- load profile and sequence for various abnormal or accident conditions
- method of load transfer or connection to normal offsite power
- reliability or availability
- protective features
- equipment control and protective setpoints

7.1.1.5 Installation Criteria

Directions and recommendations provided by the manufacturer should be followed as appropriate. Emergency and backup power systems and key components, including batteries, generators, fuel tanks, and switch gear, should be physically located where they will be protected either under continual surveillance or contained in a locked enclosure with an IDS installed to protect against tampering and unauthorized access.

---

[5] Section 4, "General Requirements," and Section 5, "Detailed Requirements," of U.S. Department of Energy (DOE)-STD-3003-2000, "Backup Power Sources for DOE Facilities," issued January 2000, contains more details on the information in this section.

Nonrechargeable batteries should be replaced whenever their voltage drops below 20 percent of the rated voltage or based on the manufacturer's recommendation. An alarm signal should alert the alarm stations of this condition.

A generator must be capable of providing power compatible with the equipment it sources. The generator should have adequate capacity and rating for all loads to be operated simultaneously. The emergency and backup power system should start automatically (or be brought online) upon loss of primary power. The transfer of power from battery to generator power should occur at a setpoint before the battery power declines in voltage below the levels needed to continue the operation of assigned equipment. This transfer of power is typically set to occur before the battery voltage falls below 80 to 90 percent of normal in the event the generator initially fails to start.

7.1.1.6 Testing

A regular program of testing emergency and backup power sources is necessary to keep them in optimal operating order. Three types of testing must be performed at different times in the life of a power system: (1) acceptance testing, (2) performance testing, and (3) operability testing.

7.1.1.6.1 Acceptance Testing

Acceptance testing is the process that a facility must go through after an installer has completed the installation of the system but before the system is used operationally. Acceptance testing consists of the following two parts:

- Physical Inspection. The newly installed components should be thoroughly inspected to ensure that the system has been installed in accordance with the manufacturer's specifications and the detailed engineering drawings for the site-specific design and installation. A facilities engineer must determine whether the installer implemented commonly accepted practices for electrical; mechanical; and plumbing work, including safety requirements.

- Performance Test. A complete and positive performance test should be conducted (see Section 7.1.1.6.2).

7.1.1.6.2 Performance Testing

Performance testing is the periodic testing of the full range of expected capabilities of a particular emergency or backup power system. Most importantly, the testing should demonstrate that the emergency/backup power system does the following:

- receives instant notification when primary power has failed
- becomes fully operational within the timeframe for which it was designed
- provides the power voltage for which it was designed
- continues to operate for the length of time for which it was designed
- reliably returns to normal power when appropriate

This complete test should be accomplished at least once every 12 to 18 months or whenever a change to the system has been made, including the rerouting of power sources, movement of equipment, or an upgrade of features or components.

To provide full assurance that the system will function as required, the entire IDS should be tested while being powered by the backup power. Through observation of power source transition testing or through the review of testing and maintenance records, the following systems should be verified as remaining operable without interruption during the transition from normal power to the UPS: (1) the protected area perimeter IDS, (2) the perimeter assessment systems, including the video-image-recording cameras, (3) the security computer processing units, (4) the alarm station consoles and video display monitors, and (5) illumination assets or other technology that augments illumination required for assessment.

7.1.1.6.3 Generator Testing

An integrated test of the emergency/backup power system should be performed at least once a year to demonstrate proper operation during a loss of primary power. This series of tests demonstrates the ability of the generator unit and associated switch gear to perform their intended function under simulated accident conditions. In addition to the steps performed during the monthly test outlined in Section 7.1.1.6.4, the following steps should be performed:

- Verify that the busses that will be powered by the generator deenergize and load shed, as required.

- Verify that the generator starts automatically and attains voltage and frequency within prescribed limits and time.

- Verify the proper loading sequence and verify that voltage and frequency are within the manufacturer's specifications for connected loads for both transient and steady-state conditions.

- Run the generator for at least 8 hours after reaching temperature equilibrium.

- Demonstrate that the generator operates at its continuous rating and, if installation permits, efficiency rating (also called the load power factor). If the connected load is above the continuous rating but within the short-time rating, the unit should be operated at the short-time overload value for no longer than the time specified for the short-time rating.

- After the test is complete, shut the unit down and demonstrate, within 5 minutes, the ability of the unit to perform a hot restart and load to its continuous rating.

7.1.1.6.4 Uninterruptible Power Supply Testing

A UPS in its standby or normal operating mode may not demonstrate many of the various features that may be required to function during emergency conditions that include, but are not limited to, a loss of power or equipment failure.

The following tests are recommended UPS tests and, depending on the design of the UPS system, should be performed according to manufacturer's recommendations or at least on an 18-month interval:

- Light-Load Test. Operate controls and instruments for stability and values of voltage and frequency.

- Synchronization Test. Measure the rate of frequency change during synchronization and UPS voltage during transfer (when an alternate source is part of the design).

- Alternating Current Input Failure Test. Verify that the transfer to a dc source occurs as designed.

- Alternating Current Input Return Test. Verify that system performs a stable return to the normal source.

- Transfer Test. Forward and reverse UPS systems using static bypass switches.

- Rated Full-Load Test. Check that the system meets the connected or rated load-carrying capability for the required duration for extremes of ac- and dc-input voltage.

- Output-Voltage Balance Test. Measure the phase angle and voltage to meet specifications for balanced and unbalanced conditions.

- Harmonic-Components Test. Measure harmonic content in the output voltage for linear and nonlinear load conditions.

7.1.1.6.5 Testing Batteries

The only real measure of a battery's capacity and capability to provide power to its required load is derived from the performance of two different tests: (1) the performance discharge test and (2) the service test. During these tests, the battery will be unavailable for duty because of significant discharge. These tests should be performed only under conditions when the unavailability of the battery is acceptable, or provisions should be made (compensatory measures) for an alternate source to be temporarily connected to the loads for the duration of the test and recharging of the battery.

The performance discharge test indicates the remaining capacity of the battery expressed as a percentage of the rated capacity and thus the remaining useful life of the battery.

The service test demonstrates the ability of the battery to carry its required load for the required time period. To perform the service test, the load profile for the battery must be known.

7.1.1.6.6 Operability Testing

Operational testing is the monthly testing of the emergency/backup power system to confirm that it is functional. Because regular maintenance is critical in many systems, performance of this operational testing requirement at the same time as regular maintenance is highly recommended. Because it is sometimes difficult to distinguish between what constitutes periodic testing and what constitutes periodic maintenance, the two have been combined in Section 7.1.1.7.

Table 11[6] provides an example of good practices for surveillance and testing of lead-acid cells, including expected values and testing frequency. Adjustments (increases or decreases) to the intervals in the table should be based on experience and the manufacturer's recommendations.

Table 11 Typical Lead-Acid Battery/Cell Surveillance and Tests

Subject[a]	Values[b]	Period
Battery Terminal Voltage (Typical 60-Cell Battery)	(129–130.2) volts PbSb (130.2–135) volts PbCa	Monthly
Electrolyte Level	Between fill lines (distilled water only)	Monthly
Cell Float Voltage (Pilot Cell)	(2.15–2.17) volts PbSb (2.17–2.25) volts PbCa	Monthly
Cell Float Voltage (All Cells)	(2.15–2.17) volts PbSb (2.17–2.25) volts PbCa	Quarterly
Specific Gravity (Pilot Cell)	1.215 ± 0.010	Monthly
Specific Gravity (All Cells)	1.215 ± 0.010	Quarterly
Cleanliness and Corrosion Check	N/A[c]	Monthly
Resistance Measurement Cell to Cell and Terminal Connections	< 20% above the value when new or after cleaning or retorquing bolts	Yearly
Battery Capacity Test (Performance Discharge Test)	> 80% of capacity[d]	5 years
Battery Load Test (Service Test)	Design load and duration with adequate voltage	Yearly[e]

a All manufacturer's safety precautions should be observed when working on batteries.
b Values outside these ranges indicate that action is necessary to restore the parameter to within the specified values.
c Battery cleaning should be done with baking soda and water with a clear water rinse; no other cleaning materials should be used.
d A battery capacity (performance discharge) test is used as an indicator of battery age. Initially, a battery should be fully charged with a temperature near 25 degrees C and clean terminals.
e This test is not required for a battery that is used for the generator only and not for other loads. The periodic monthly start of the generator is a load test. Load tests should be done in an as-found condition.

7.1.1.7. Maintenance

Because of the nature of emergency/backup power supplies and their expected irregular schedule of use, regular maintenance is critical to guaranteeing their full functionality and reliability when the primary power source is unavailable. Maintenance for emergency and backup power supplies should be done in accordance with the manufacturer's recommendations.

7.1.2 Generators

To avoid unnecessary and premature degradation of the generator, follow the manufacturer's recommendations in regard to prelubrication, acceleration, loading, and unloading. All

---

[6] The information in Table 11 was obtained from DOE-STD-3003-2000.

generator starts for testing purposes should follow the manufacturer's recommendations for prelubrication and other warmup procedures to minimize mechanical stress and wear.

Regular exercising of the generator keeps parts lubricated, prevents oxidation of electrical contacts, uses up fuel before it deteriorates, and helps provide reliable engine starting. The generator set should be run at least once a month for a minimum of 1 hour loaded to no less than one-third of the nameplate rating.

The following, at a minimum, should be performed at least once per month, unless otherwise specified by the manufacturer:

- Record the as-found condition and the identity of the test personnel.
- Verify that the generator starts on a simulated loss of offsite power and accelerates to the operating revolutions per minute in (the required value) seconds. Generator voltage and frequency should be (required value + 10 percent) volts and (60 + 2 percent) hertz within (required value) seconds.
- Verify that the starting system disengages properly.
- Verify that fuel tank levels (i.e., fuel storage tank, day tank, and engine tank) are within specifications.
- Remove accumulated water from fuel tanks and the oil/water separator.
- Verify that the fuel transfer pump system starts and that fuel is being transferred from the storage tank to the day and engine-mounted tank (if present).
- Verify that the generator can accept loads up to 90 percent of the continuous rating for the duration of the test (i.e., the test time should consider the manufacturer's recommendations). This may be done using normal loads or a load bank or synchronizing to the offsite grid if this capability is available. If a load bank is routinely used, a dedicated connection should be provided. The value of 90 percent is used to provide margin to avoid inadvertent overloading.
- Verify the cooling water tank level.

When recording test results, a failure should be recorded if the generator fails to start, accelerate, reach nominal voltage and frequency, or accept the rated load within and for the time required or if it otherwise fails to satisfy the specified acceptance criteria.

7.1.3 Uninterruptible Power Supplies

The UPS system should be inspected and tested on a frequent basis in compliance with the manufacturer's recommendations. The type of service to which the equipment is subjected (e.g., duty cycle, chemicals, dust, heat) and trending dictate the frequency of the inspections. Less frequent activities (i.e., internal cleaning, filter replacement, checking electrical connections for tightness, and calibration of instruments) should be done according to the manufacturer's recommendations.

7.1.4 Batteries

Many types of batteries, if they are allowed to sit without a charger, will internally discharge, often with irreversible cell degradation. For these types of batteries, maintaining a proper charging float voltage during standby is important. Because of inherent differences between cells, float voltage and specific gravity values will vary from cell to cell over time. If cell float voltages or specific gravity values, or both, are allowed to remain in an unequal condition for extended periods of time, cell sulfation will result. To overcome this problem, a periodic equalizing charge must be applied to equalize cell voltages and specific gravities. The manufacturer's recommendations should be followed in regard to equalizing charge. When performing an equalizing charge, care should be taken to ensure that the charger voltage does not exceed the voltage rating of the load connected during the equalize charge. Batteries are usually rated at a temperature of 25 degrees C. Higher temperatures will improve battery capacity at high discharge rates but significantly reduce battery life. Lower temperatures have a significant effect in reducing battery capacity. Typical battery types for standby service are lead-acid (i.e., calcium, antimony), pure lead (generally a "round cell"), or nickel-cadmium. Manufacturers will provide necessary information on the care, precautions, charging, and treatment of specific batteries, including maintenance during periods of storage.

8 REFERENCES

1. Garcia, M.L. *The Design and Evaluation of Physical Protection Systems.* Amsterdam: Elsevier/Butterworth-Heinemann, 2001.

NRC FORM 335
(12-2010)
NRCMD 3.7

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-1959
Revision 1

2. TITLE AND SUBTITLE
Intrusion Detection Systems and Subsystems
Technical Information for NRC Licensees

3. DATE REPORT PUBLISHED
MONTH: September
YEAR: 2017

4. FIN OR GRANT NUMBER

5. AUTHOR(S)
John W. Bowen
Stephen M. Sohinki
Elisabeth L. Potter

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.)
Dade Moeller and Associates
1835 Terminal Dr #200
Richland, WA 99354

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 Physical and Cyber Security Policy
Office of Nuclear Security and Incident Repsonse
U.S. Nuclear Regulatory Commission
Washington, DC 20555-001

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)
This report provides information about the design, installation, testing, maintenance, and monitoring of intrusion detection systems (IDSs) and subsystems used for the protection of facilities licensed by the U.S. Nuclear Regulatory Commission. It contains information on the application, use, function, installation, maintenance, and testing parameters for internal and external IDSs and subsystems, including information on communication media, assessment procedures, and monitoring. This information is intended to assist licensees in designing, installing, employing, and maintaining IDSs at their facilities.

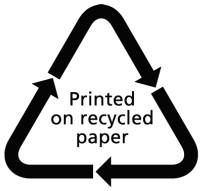
12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
Intrusion Detection System
Assessment
Nuisance
Interior / Exterior
Passive / Active
Proximity
Volumetric
Alarm

13. AVAILABILITY STATEMENT
unlimited

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

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS

NUREG-1959
Revision 1

Intrusion Detection Systems and Subsystems
Technical Information for NRC Licensees

September 2017