4. INTERIOR INTRUSION DETECTION SENSORS

4.1 Balanced Magnetic Switch

4.1.1 Principles of Operation

The magnetic switch is the most ubiquitous security device in the world, used for both door and window protection. (Refer to Figure 36). It consists of a magnet, which is installed on a door or window, and a switch unit, which is 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, which causes an alarm to be initiated.

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 (bypass or spoof) a simple magnetic switch. In response, the balanced magnetic switch (BMS) was developed more than 30 years ago. The BMS requires a great deal more skill to defeat than a simple magnetic switch.

A BMS employs 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 is closed.

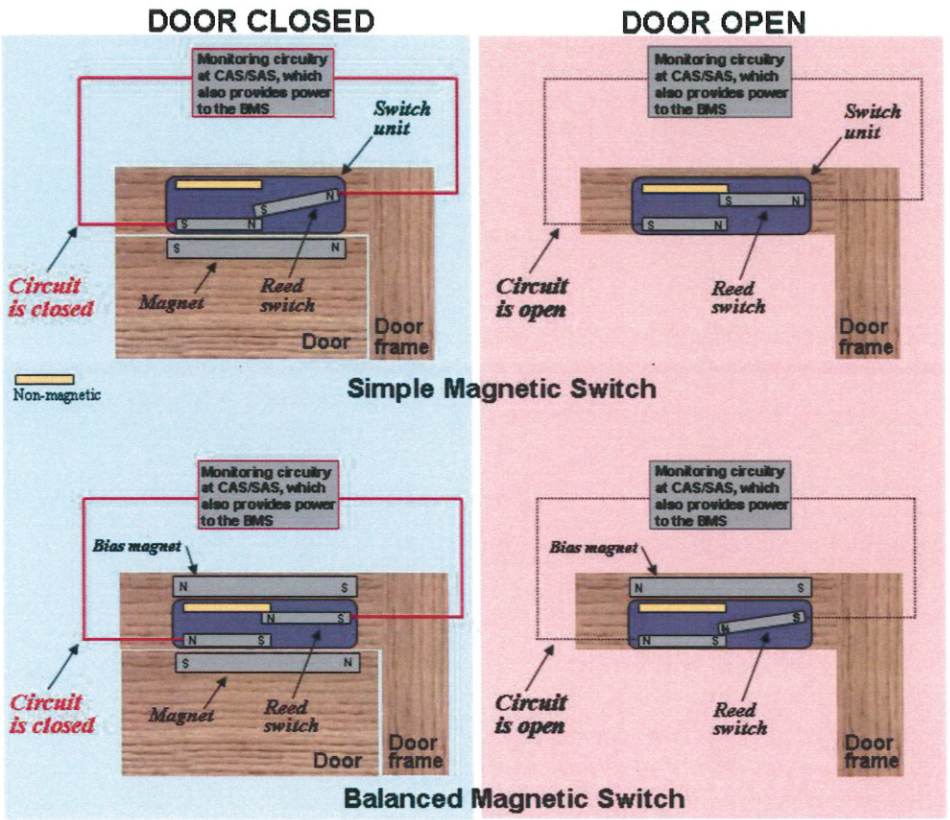

Figure 37: A schematic of a simple versus balanced magnetic switch.

With the door or window closed, the magnets are adjusted to create a magnetic loop, causing 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 trigger an alarm indicating a security breach. In some models, this magnetic field is accomplished 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, such as opening the door or window, results in the transfer of the reed switch to the "closed" position and an alarm output. 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 that the BMS be completely replaced with another matched pair.

A BMS is a passive, visible, point-detection sensor.

4.1.2 Types of Balanced Magnetic Switch Sensors

BMS sensors have a variety of designs. Some use multiple magnets; 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, such as 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 a facility chooses should be based on providing reliable functionality within the environment and the goals of the physical protection program.

4.1.3 Sources of Nuisance Alarms

BMS sensors are very reliable when installed correctly on a properly installed door with hardware that is in good condition. Nuisance alarms are almost never caused by the BMS alone.

Most nuisance alarms generated by a BMS can be attributed to the poor condition of the door or its hardware. Most common nuisance alarms are caused by a worn or out-of-adjustment latch that occurs because of excessive door movement or play. Nuisance alarms can also be caused by excessively worn door hinges or an improperly installed BMS that causes misalignment of the switch unit and magnet unit.

When a BMS is used on large rollup doors, nuisance alarms are usually caused by slight misalignment of the doors. 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.

4.1.4 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 door frame is steel, a nonferrous (aluminum or

plexiglass) spacer should be installed between the door frame 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 ½-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 provide protection for the alarm wiring. Materials with high magnetic permeability, such as Mumetal®, are preferable for the shielding. However, steel can also be used.

Sensor electronics enclosures should have tamper switches. Line supervision is the means for monitoring the communication link between a sensor and the alarm control center. Use of supervised lines between the sensor and host alarm system, as well as continuously monitored sensor tamper switches, will help protect against adversary attacks on communication links and sensor electronics enclosures.

4.1.5 Characteristics and Applications

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

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

An externally introduced magnetic field has the possibility of defeating a BMS. BMS sensors 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. Consideration should be given to 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, it will indicate a secure state even when the system is breached.

4.1.6 Testing

A regular program of testing sensors is imperative for maintaining them in optimal operating order.

4.1.6.1 Acceptance Testing

When a BMS sensor is first installed, it should be tested in order to formally "accept" the sensor as part of the physical protection system. Acceptance testing consists of two parts:

(1) A **physical inspection** to ensure that the sensor is installed properly consists of the following:

- Verify that the installation matches the installation drawings, which should follow the guidance provided by the manufacturer.
- Verify that signal and power wires are routed in the conduit.
- Verify proper power levels (voltage and amperage).
- Verify correct wire connections.

(2) A **performance test** to establish and document the level of performance (see next section).

4.1.6.2 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/or repair will be required; after this repair, a formal performance test should be run. Also, operation of the sensor tamper and communication to the alarm stations are verified during testing.

Three basic tests constitute a performance test for a BMS:

(1) Evaluate the response of the switch when an externally introduced magnetic field is produced via a foreign magnet during testing. (Refer to Figure 38.)

(2) Establish that the BMS detects a door opening within a specified distance. A commonly used requirement is that a BMS shall generate an alarm when the leading edge of the door has been moved 1 inch or more from the fully closed position.

(3) Establish that the BMS does not detect a door opening within a smaller specified distance. A commonly used requirement is that a BMS shall not initiate an alarm for door movement of ½ inch or less. The importance of the condition of the door and its associated hardware cannot be overemphasized. If the door is not properly installed and maintained, the BMS effectiveness will be degraded.

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.

4.1.6.3 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. Then another test is 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, given that there is some play in the latch.

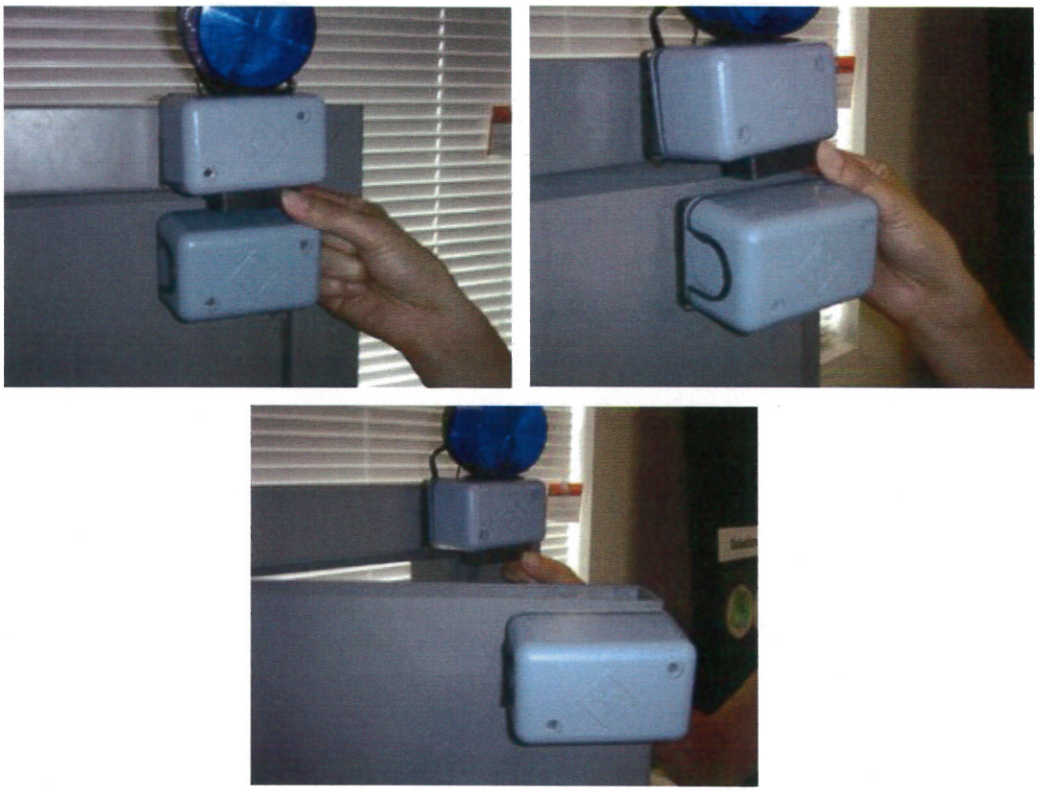

Figure 38: Demonstration of introducing an external magnetic field to a BMS. Note that this procedure is much more difficult to accomplish than the photos would suggest.

The door hardware should be in good condition. The door should open and close smoothly without rubbing or scraping on the door frame. It should latch easily and the amount of play in the latch should be minimal.

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

4.1.7 Maintenance

At a minimum, maintenance of a BMS should be performed every 6 months. The following should be verified 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 alarm when a foreign magnetic field is introduced 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 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.

4.2 Interior Microwave Sensors

4.2.1 Principles of Operation

Interior microwave sensors are active volumetric sensors and are typically monostatic, employing 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, and 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. As 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.

Microwave sensors typically operate in the X band radiofrequency region (7 to 11 gigahertz) with low power output that is approximately 5 to 10 milliwatts. Figure 40 illustrates typical sensor coverage patterns. 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 (approx. 29.5 feet) up to 30 meters (approx. 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. The antenna is usually a microwave horn but may be a printed circuit planar or phased-array antenna.

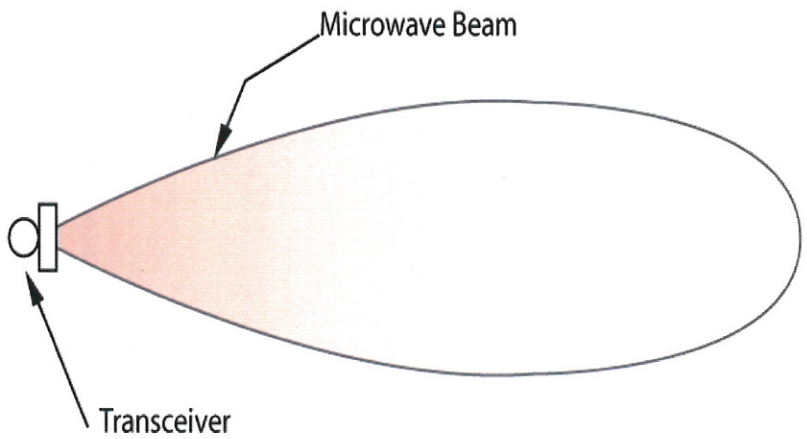

Figure 39: A common interior microwave antenna propagation pattern.

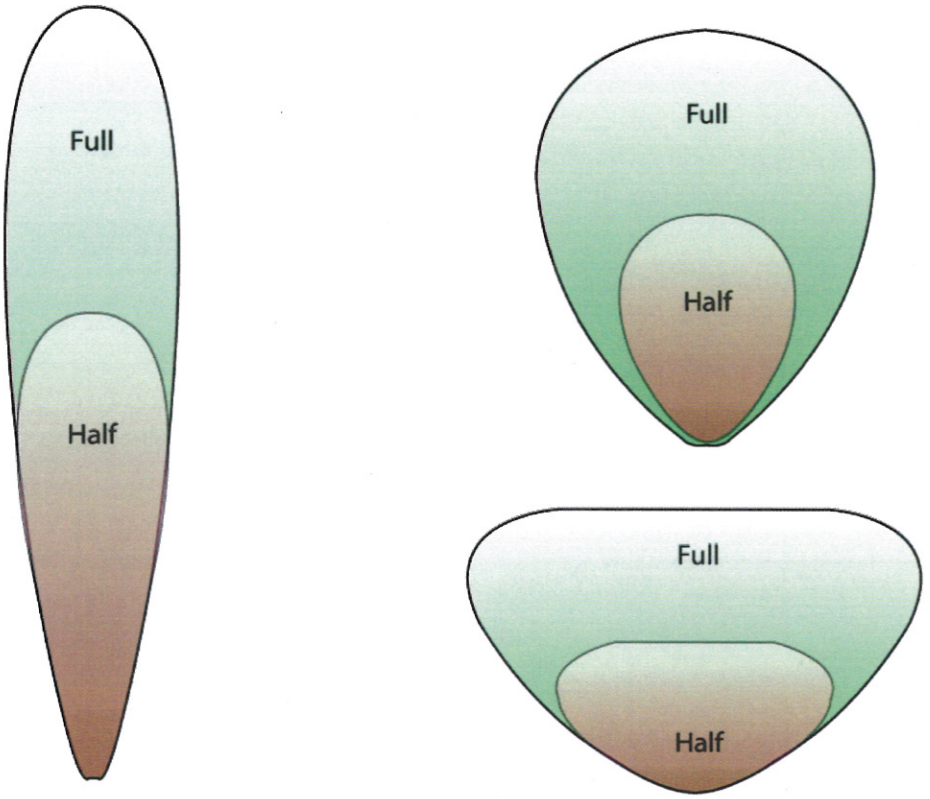

Figure 40: Examples of different microwave antenna propagation patterns; the half and full envelopes indicate half-power and full-power settings.

Optimal detection for microwave sensors is achieved when the target is moving toward or away from the sensor—not across the detection zone. Therefore, placement of microwave sensors should be such that the adversary will be necessarily forced to move towards or away from the sensor to accomplish the adversary's objective.

4.2.2 Types of Interior Microwave Sensors

The two basic types of 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 for the area being covered, but is more commonly applied in exterior applications.

4.2.3 Sources of Nuisance Alarms

Because of the high frequencies of 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 a microwave sensor is installed in a room made from light construction materials and the detection area of that microwave is larger than the room, nuisance alarms will occur because of movement

outside the room. The structural materials and the thickness that a particular microwave can penetrate will vary, based on the device's manufacturer, model, and frequency. (See Figure 41.)

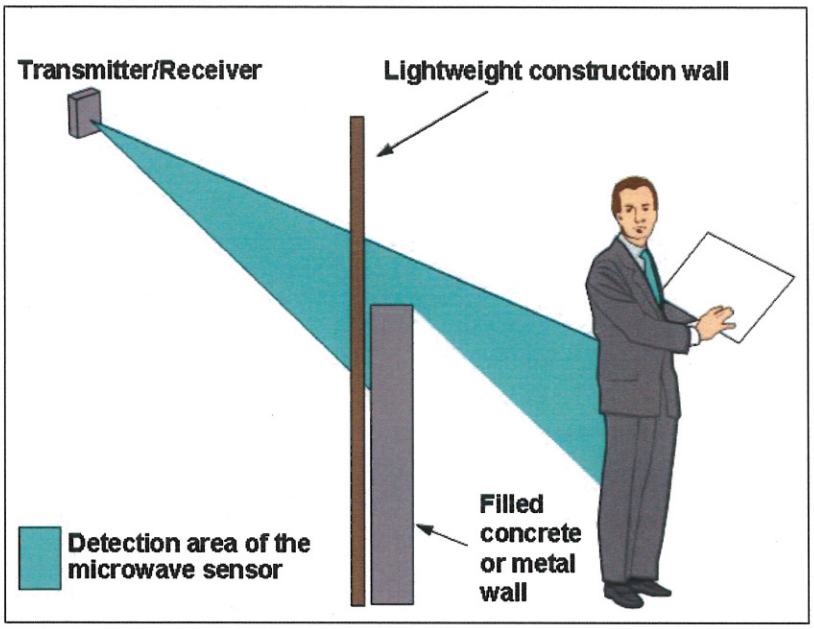

Figure 41: A microwave sensor can trigger nuisance alarms because of its ability to transmit through some light-weight construction materials.

Nuisance alarms can be generated by fans, rodents, pets, or equipment. 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, reflections from the moving fan blades can be detected by microwave energy traveling through the duct. Another source of nuisance alarms for microwaves is plastic drainpipes located behind dry wall. Water draining through the pipes can cause alarms.

Some microwave sensors can be triggered by fluorescent lights. The gas within fluorescent lights is a reflector of microwave energy when ionized. The light actually 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 possibility. In fact, if more than one microwave sensor is installed in the same area, they can potentially interfere with each other and cause nuisance alarms. Fortunately, microwave sensors are available that allow the user to select from several different frequencies. More than one microwave in the same area will require different frequencies.

Finally, signals reflected off metal objects, such as filing cabinets, trash cans, and electrical boxes, can "extend" sensor coverage to areas not intended to be covered, thus creating the potential for nuisance alarms.

4.2.4 Characteristics and Applications

Microwave sensors are most sensitive and effective when installed so that an adversary would necessarily walk toward or away from the sensor.

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 where a well-defined area of coverage is needed, 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 a PIR 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 provides security personnel with additional information to help them accurately assess an alarm and discriminate actual or potential penetrations from nuisance events.

Microwave sensors are least sensitive if installed such that an adversary would be able to limit his or her movements to paths across the detection pattern.

The special properties of microwave beams allow them to penetrate most types of surfaces (metal is not one of them). Because of this, it is possible for a microwave to detect motion in an area where detection is not desirable and not detect motion 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 hiding place for a potential adversary. On the other hand, because the beam can penetrate walls, the sensor may detect motion behind a wall in another room.

As microwave sensors are extremely sensitive to motion, they are also prone to nuisance alarms. Objects being moved by air currents generated by the heating, ventilation, and air conditioning (HVAC) or fans may trigger alarms. Even fluorescent lighting, which emits detectable light particles, may trigger a false alarm.

Since 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 aid in avoiding this problem.

Very slow movement by an intruder is harder for a microwave sensor to detect, though to actually defeat a microwave sensor is not easy. 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 still have some sensitivity against intruders moving at speeds as slow as 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 will be required to be inside the detection area for a lengthy period to allow the time necessary to move this slowly and avoid detection, which thereby increases 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 hence, no detection will occur. This is, however, a very difficult movement for an intruder to accomplish correctly and subsequently avoid detection.

The three graphs in Figure 42 show the differences between the detection pattern shape and size with respect to test subject direction of movement into an area that is sensored by a microwave. The left graph shows the maximum detection pattern with the test subject walking directly toward the sensor. The right shows a small decrease in detection pattern size with walk testing parallel to the sensor center line. The top graph shows a much smaller detection pattern with walks that are parallel to the sensor face. This direction results with less of a Doppler frequency shift; the Doppler shift requires a sufficient amplitude change and duration time to cause 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.

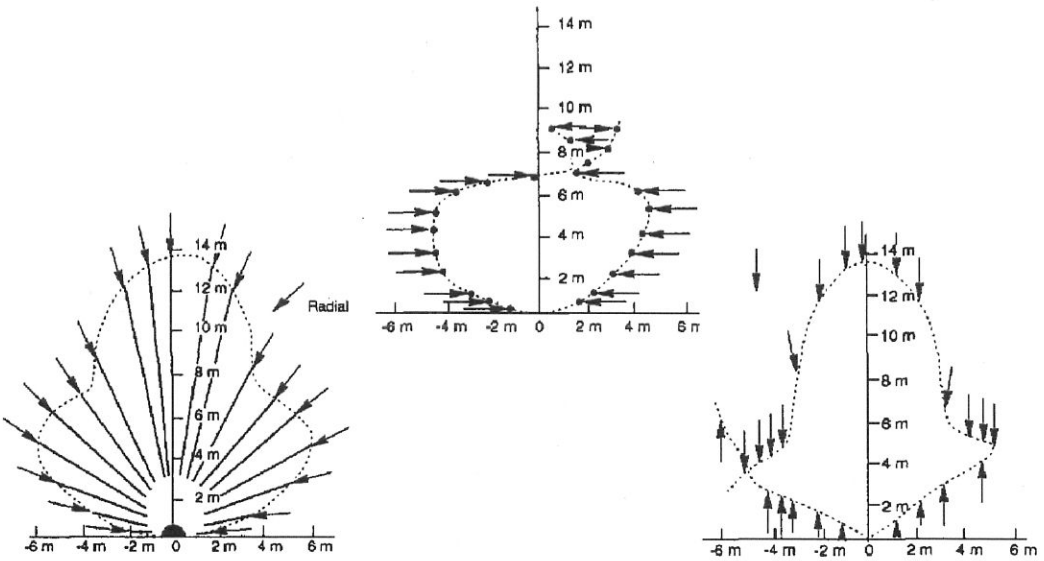

Figure 42: Differences in detection patterns occur for walk tests that are performed from a variety of orientations and from different directions.

4.2.5 Installation Criteria

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 (ceiling, corner, wall, etc.) will depend on the particular sensor being used, as well as the area or target it is intended to protect.

Care should be taken when surveying the area to be protected to note any object that may degrade the detection capability of the sensor (metal filing cabinets, fans, air conditioner vents, etc.). 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 metal mesh of 0.6 centimeters (0.25 inches) mesh or a radiofrequency absorber, eliminates such signal interference.

4.2.6 Sensor Testing

A regular program of testing sensors is imperative for maintaining them in optimal operating order. Three types of testing need to be performed at different times in the life of a sensor: acceptance testing, performance testing, and operability testing.

4.2.6.1 Acceptance Testing

When a sensor is first installed, it should be tested in order to formally "accept" the sensor as part of the facility's physical protection system. Acceptance testing consists of two parts:

(1) A **physical inspection** to ensure that the sensor is installed properly consists of the following:

- Verify that the installation matches the installation drawings, which should follow the guidance provided by the manufacturer.
- Verify that signal and power wires are routed in the conduit.
- Verify proper power levels (voltage and amperage).
- Verify correct wire connections.

(2) A **performance test** to establish and document the level of performance. Refer to the following section for details.

4.2.6.2 Performance Testing

Performance tests (refer to Figure 42) are designed to verify the level of performance of each 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 the maintenance section.

All relevant processor readings should be recorded, and new readings should be compared to the last recorded readings. As in all test situations, the area under test should be maintained under visual observation by a member of the site security force, or a member of the site security force should actually conduct the test. For each sensor, the test 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 both line supervision and tamper-indication alarms are received in the alarm station as appropriate.

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

4.2.6.2.1 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 (refer to Figure 43), which is the most effective detection approach against a microwave.

(1) Start outside of the published detection area in front of the sensor, and walk at 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 testing on that path until the required number of tests is completed. Multiple tests along each test line path are required to establish a P_D (probability of detection). As an example, to establish that a sensor has a minimum P_D of 90 percent at a confidence level of 95 percent, the sensor would have to pass 29 out of 30 tests.

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

4.2.6.2.2 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 (refer to Figure 43), which are the least effective detection approach against a microwave.

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

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

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

(4) Repeat testing on that path until the required number of tests is completed. Multiple tests along each test line path are required to establish a P_D (probability of detection). As an example, to establish that a sensor has a minimum P_D of 90 percent at a confidence level of 95 percent, the sensor would have to pass 29 out of 30 tests.

(5) Perform the above tests on remaining paths.

(6) Repeat Steps 1 through 5, starting from the other side of the detection area.

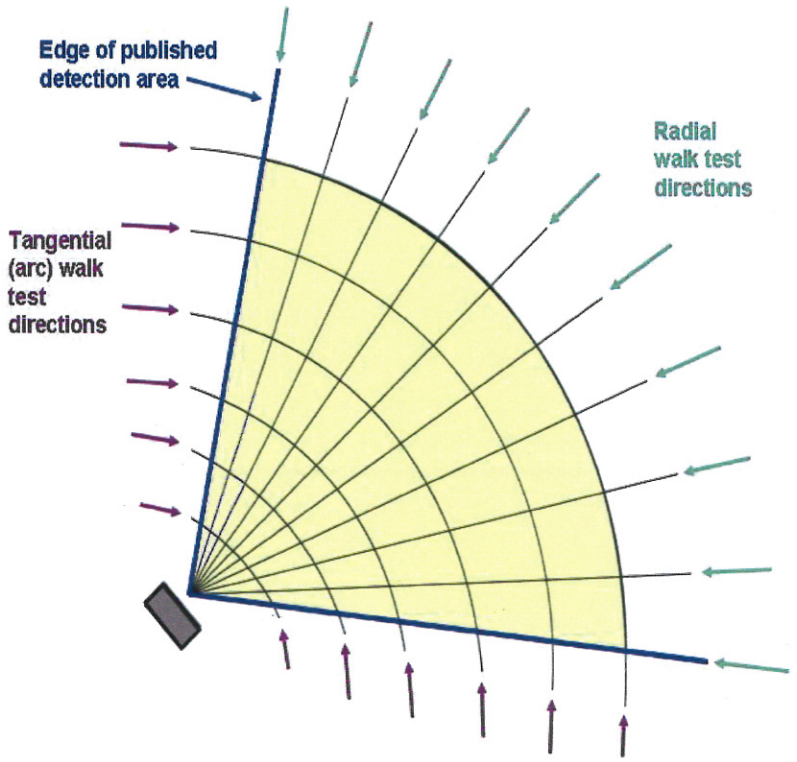

Figure 43: Recommended walk test paths and directions for the performance testing of a microwave sensor.

4.2.6.2.3 Slow Walk Tests

Slow walk tests are conducted at speeds less than 0.5 feet per second. Most volumetric sensors such as the microwave will have a speed where 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 person will likely be different than detection of a walking person.

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, which will reduce the possibility that environmental effects and other unknown factors are affecting the test results (i.e., detection or nondetection). Using a random sequence, there is less chance that the test results would be biased.

4.2.6.3 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.

4.2.7 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 self-test 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.

4.3 Passive Infrared

4.3.1 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.)

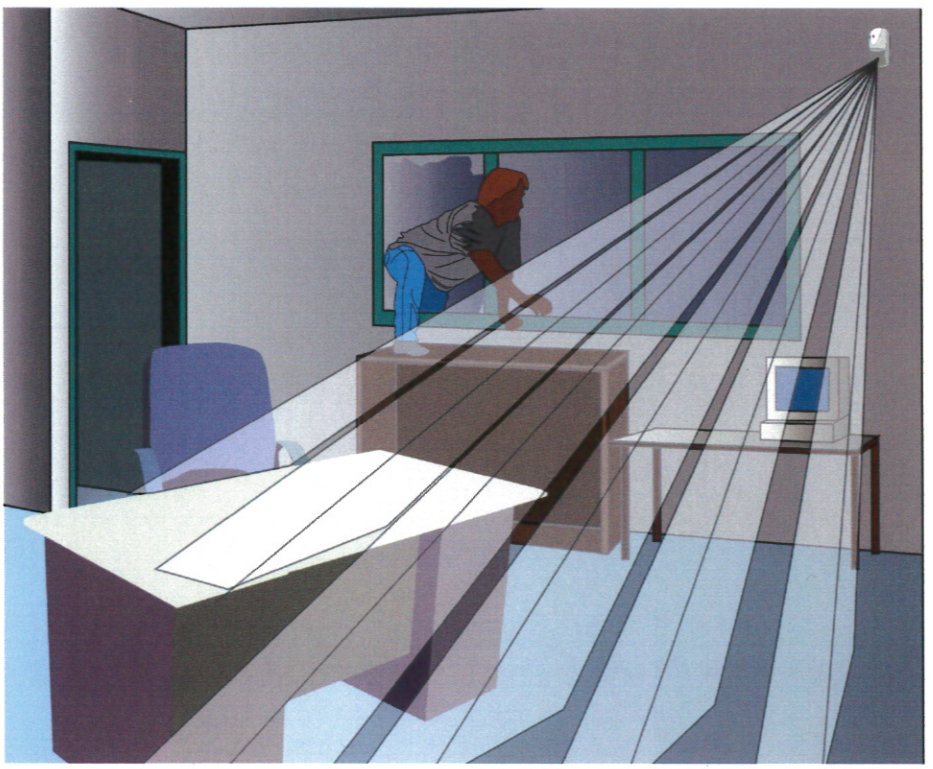

Figure 44: Detection pattern for a typical installation of a PIR sensor.

PIR sensors detect the electromagnetic radiated energy generated by sources that produce temperatures below that of visible light. PIR sensors do not emit any energy field into the area

they are protecting and do not measure the amount of infrared energy. Rather, PIRs measure changes in thermal radiation. PIR sensors detect 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 lens, the detection pattern is subdivided into solid angular segments. (Refer to Figure 45.) As a person passes across the detection segments, each segment passed through will generate an increase or decrease in temperature, which will trigger an alarm. This infrared energy is detected by a thermopile or pyroelectric device and converted 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 Celsius.

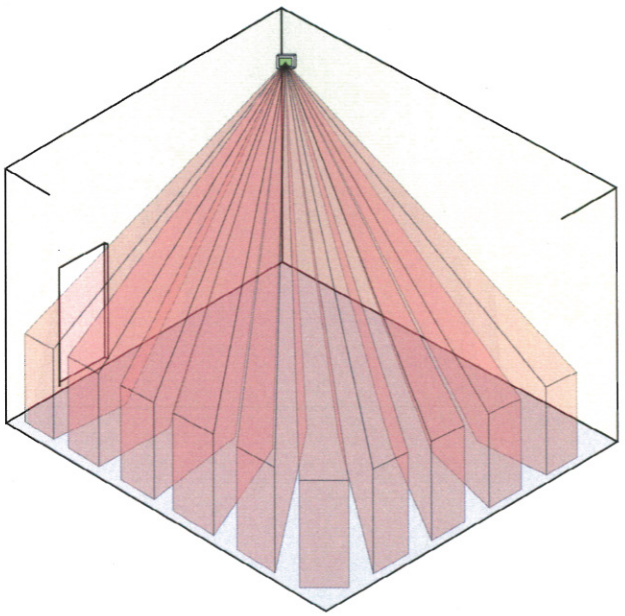

Figure 45: A PIR sensor's detection pattern is subdivided into solid angular segments; a specific number of segments must detect an anomaly before the sensor will signal an alarm condition.

While 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 an area being protected. 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.

4.3.2 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, as shown in Figure 46 and Figure 47.

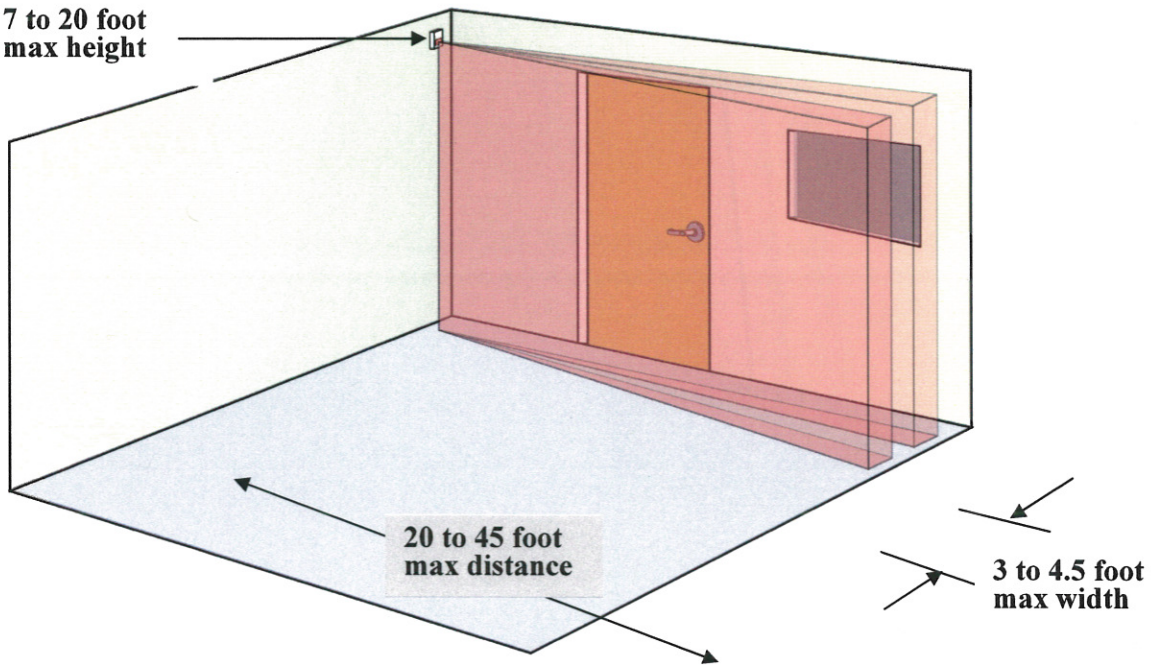

Figure 46: An example of a curtain PIR application.

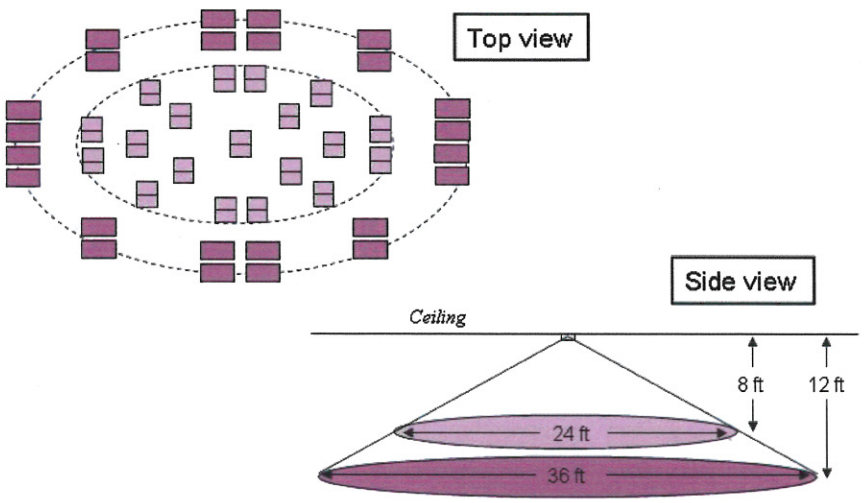

Figure 47: These two diagrams illustrate the detection pattern of a ceiling-mounted PIR sensor (top view and side view). This configuration is also known as the hemispherical pattern.

4.3.3 Sources of Nuisance Alarms in Passive Infrared Sensors

Any object causing 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
- HVAC vents
- Hot pipes

In practice, nuisance alarms are less likely to be generated by localized heating and cooling 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 be 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 trigger 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 cause 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.

4.3.4 Characteristics and Applications

PIRs are 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 user to focus the beam 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. 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/or location of a passive sensor is more difficult for an intruder to determine than an active sensor, putting the intruder at a disadvantage.

In environments where explosive vapors or explosive materials may be present, passive sensors are safer than active ones because no potentially explosion-initiating energy is emitted.

Multiple passive sensors can be placed in a volume without interfering with each other (interacting) because no signals are emitted.

Detection effectiveness is less than optimal for motion directly toward or away from the sensor.

Since the PIR is a line-of-sight detector, the field of view can be easily blocked by cubicle partitions or furniture.

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 be a problem. A PIR sensor will not detect very slow motion. However, defeating a PIR sensor with slow motion is difficult to do because a person 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.

4.3.5 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 be 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 fitting 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 in any position that would allow an intruder access to the sensor from beneath the sensor.

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 be provided with 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 sensor coverage area.

4.3.6 Testing

A regular program of testing sensors is imperative for maintaining them in optimal operating order. Three types of testing need to be performed at different times in the life of a sensor: acceptance testing, performance testing, and operability testing.

4.3.6.1 Acceptance Testing

When a PIR sensor is first installed, it should be tested in order to formally "accept" the sensor as part of the physical protection system. Acceptance testing consists of two parts:

(1) A **physical inspection** to ensure that the sensor was installed properly consists of the following:

- Verify that the installation matches the installation drawings, which should follow the guidance provided by the manufacturer.
- Verify that signal and power wires are routed in the conduit.
- Verify proper power levels (voltage and amperage).
- Verify correct wire connections.

(2) A **performance test** to establish and document the level of performance consists of following the performance testing procedure (described below for the recommended tests.

4.3.6.2 Performance Testing

Performance tests are intended to 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 the maintenance section and perform the prudent routine maintenance. Test procedures recommended by the manufacturer should be followed. As in all test situations, the area being tested should either be kept under visual observation by a member of the site security force, or a member of the site security force should conduct the test.

For each area of detection, the test should do the following:

- Ensure that the system 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 both line supervision and tamper-indication alarms are received in the alarm station 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 compared with the results of the initial acceptance test to check for any degradation in the coverage of the sensor.

4.3.6.2.1 Tangential (Arc) Path Testing

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

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

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

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

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

(5) Perform the steps above on remaining paths.

(6) Repeat Steps 1 through 5, starting from the other side of the detection area.

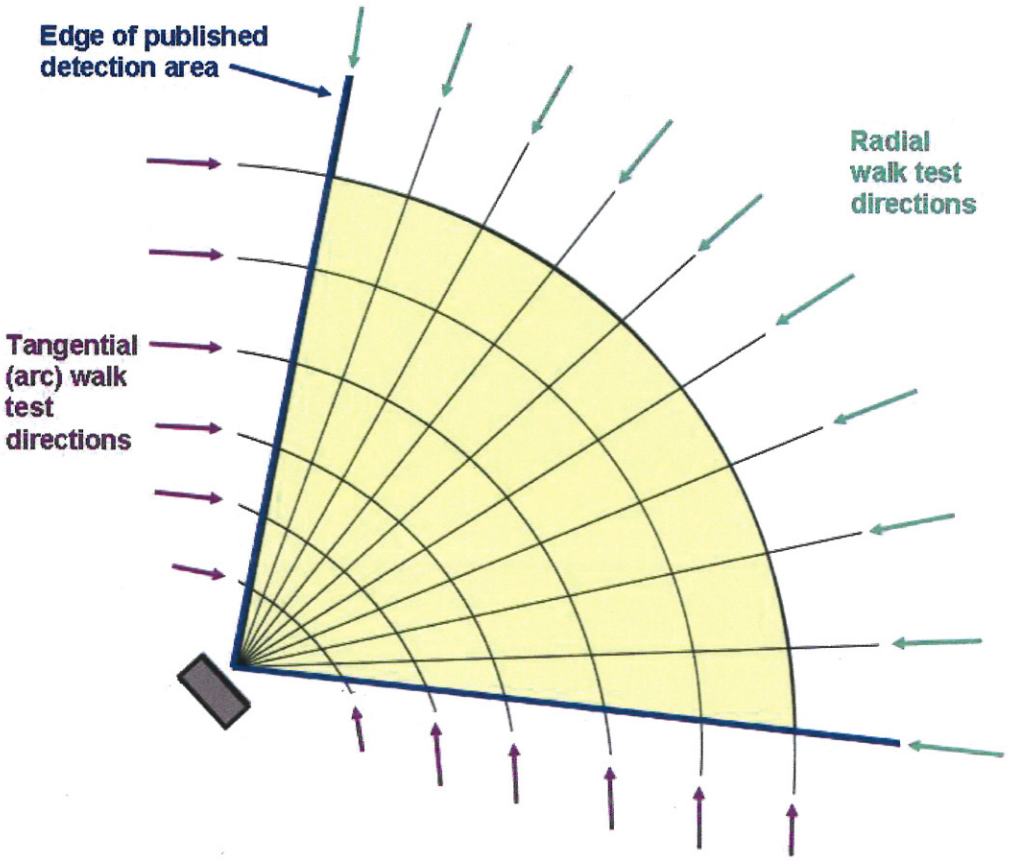

Figure 48: Recommended walk test paths and directions for the performance testing of a PIR sensor.

4.3.6.2.2 Radial Path Testing

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

(1) Start outside of the published detection area in front of the sensor and walk at 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 walk test along the same path.

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

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

Changes in room configuration can affect sensor coverage and should be checked. If room configuration has changed significantly, a complete retest of the sensor coverage should be initiated 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). This determination will, in most cases, be sensor and location dependent. 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, which will preclude the possibility that environmental effects and other unknown factors are affecting the test results (detection or nondetection). Use of a random sequence reduces the chance that the test results will be biased.

When a designer is determining the best place to locate an asset within a room, the enclosed sample graph showing the PIR sensor detection pattern could be used as guidance (refer to Figure 49). The asset should be placed inside the area that has a high PD, no matter the direction from which the intruder approaches the sensor.

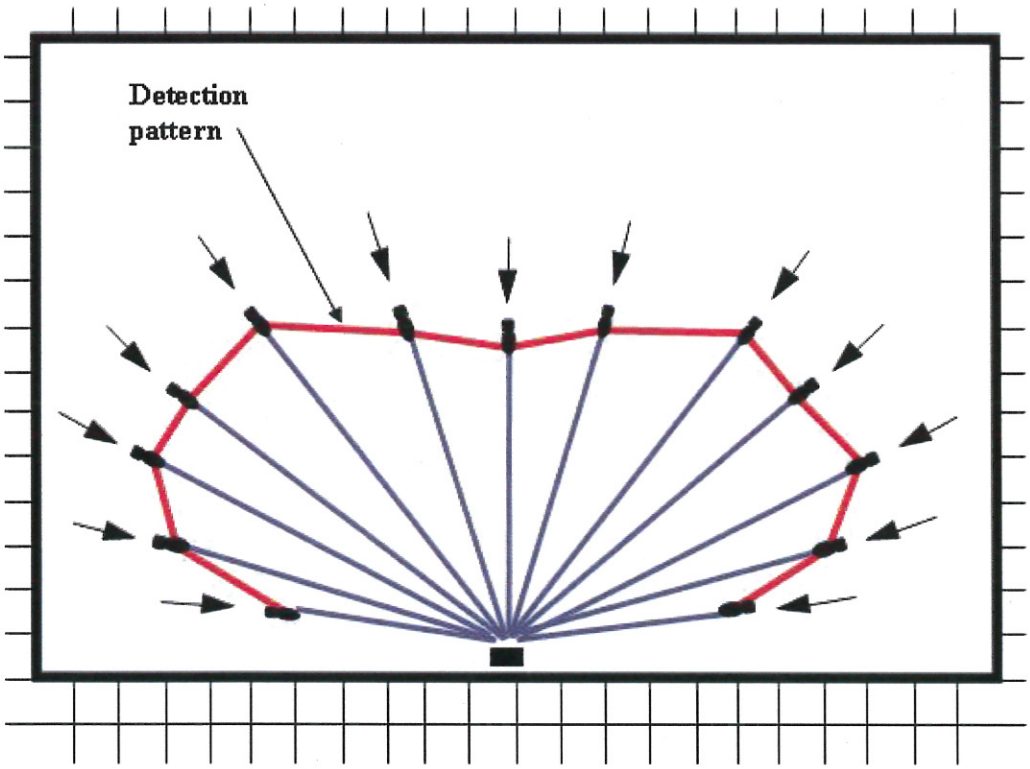

Figure 49: A typical PIR detection pattern derived from walk tests towards the sensor.

4.3.6.3 Operability Testing

Operability testing should be conducted by crossing the zone of detection in the area that the sensor is installed to monitor. The detection capabilities of each PIR should be walk tested in a different, preferably random, order every 7 days, 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 every 7 days. 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.

4.3.7 Maintenance

The general maintenance guidelines outlined in the manufacturer's technical manuals should be followed on a schedule determined by security maintenance staff and security forces, as well as by the environment in which the 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 keeping 10 to 20 percent of spare parts on hand, based on total facility units. This requirement may be adjusted as maintenance data are accumulated on the failure rate of specific sensors and sensor components. If replacement parts can be obtained quickly from regional distributors, smaller onsite inventories would be adequate.

4.4 Proximity Sensors

4.4.1 Principles of Operation

Proximity sensors, also known as point protection/detection devices, have the capability of detecting 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/or volumetric sensors. Since 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. Because of this, proximity sensors should not be used as primary detection on a high-risk item. Proximity sensors are most effective for protection against an insider.

4.4.2 Types of Proximity Sensors

Types of proximity sensors include the following:

- Capacitance
- Pressure
- Strain
- Switches

The various types of proximity sensors are described below.

4.4.2.1 Capacitance

Capacitance proximity sensors operate on the same principle as an electrical capacitor. These types of detectors are used to protect metal containers that can be isolated from ground such as safes or file cabinets. 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 changes the capacitance. The processor (part of the capacitance sensor) detects the change in capacitance and generates an alarm.

4.4.2.2 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 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. They are constructed so that when an adequate amount of pressure, depending on the application, is exerted anywhere along the ribbon, the metal strips make electrical contact. 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. Then anyone who approaches the item steps on the mat and initiates 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.

4.4.2.3 Strain

Strain sensors measure small amounts of deformation or flexing of a surface. A basic configuration of a strain sensor would be one or more sensing devices connected to a processor. The sensing devices can employ 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 bent, stretched, or compressed. The processor continually measures the electrical properties of the sensing device and will output 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 output 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 there is a change, such as when the object is removed or tampered with.

4.4.2.4 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 monitors 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 cause an alarm if the movement is such that it causes the switch contacts to change positions. The surface and switch mounting need to be designed so that it is very difficult to remove the protected item while maintaining the switch in the secured position.

4.4.3 Sources of Nuisance Alarms

The sensitivity of capacitance sensors is affected by changes in relative humidity and the relocation of other metal objects closer to or farther away from the protected item. 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, resulting in an alarm. Conversely, a decrease in humidity or drying of the air reduces the conductivity. Similarly, when larger metal objects (high electrical conductivity) such as cabinets, desks, equipment racks, etc. are moved close to an object 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 lowered, 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 because it is worn out or exposed 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 workers or other personnel would inadvertently step on it is an additional source of nuisance alarms. Pressure mats that are in good condition and installed properly should have very few nuisance alarms.

Strain sensor devices can be affected by changes in temperature, which result in 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 change enough with humidity changes to cause nuisance alarms.

Switch sensors in good condition and installed properly should have 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.

4.4.4 Characteristics and Applications

Proximity sensors should not be used as primary detection for high-risk items. They are typically used as a second or third line (layer) of protection and are most effective for protection against an insider. 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. (See Figure 50.) Portable, high-risk/value items should be locked in cabinets or secured by other means to add delay in removal. Proximity sensors can be installed to detect attempted removal of tiedowns or opening of cabinets.

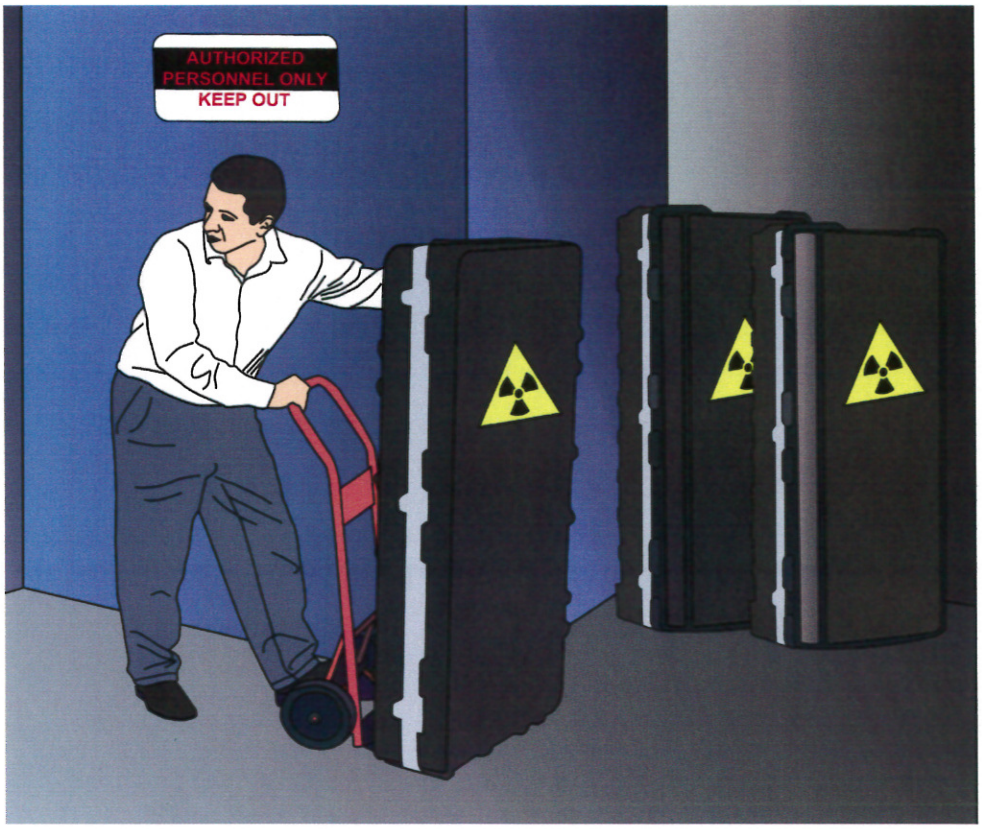

Figure 50: Example of portable, high-value items.

A typical application of a capacitance proximity detector would be the protection of a safe or file cabinets (see 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 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 requiring protection. In this type of application, the metal screen becomes part of the protected circuit, as is the safe or any other metal object.

Pressure mats are commonly used in industrial and commercial applications such as controls for opening doors or as safety devices for machinery. Although 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.

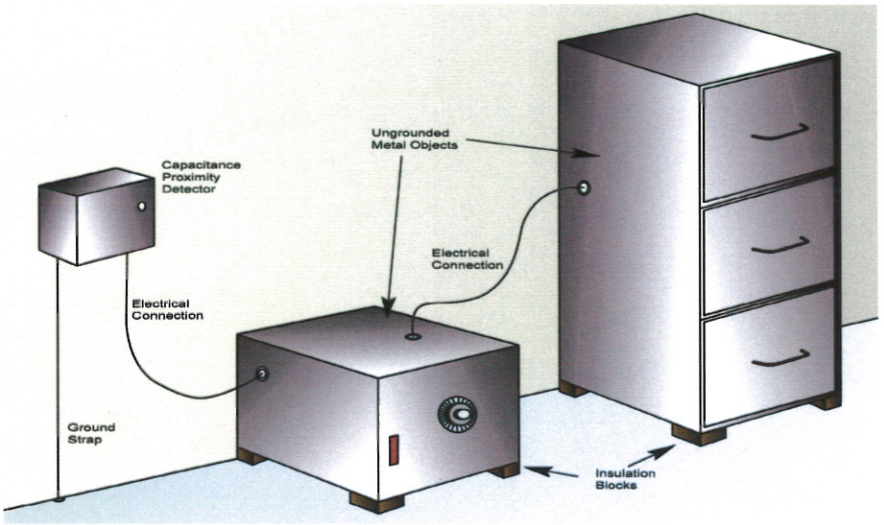

Figure 51: Example of a capacitance sensor installation.

Strain sensors can be used to continually monitor the weight of an object, sensing when it is being lifted, moved, or tampered with (Figure 52). The environment, such as changes in temperature or humidity, must be considered. Strain sensors can also be used to detect a person's weight as he or she approaches a protected area or item (Figure 53).

A self-adjusting capacitance proximity sensor may be defeated by extremely slow approach to the protected object. An adversary can detect the presence of a capacitance proximity sensor by employing radiofrequency field-sensing equipment, such as that 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, generating a nuisance alarm. These objects include persons walking near or leaning on the surface, cabinets or other objects being moved close to the surface, or loose-fitting components of the protected object itself.

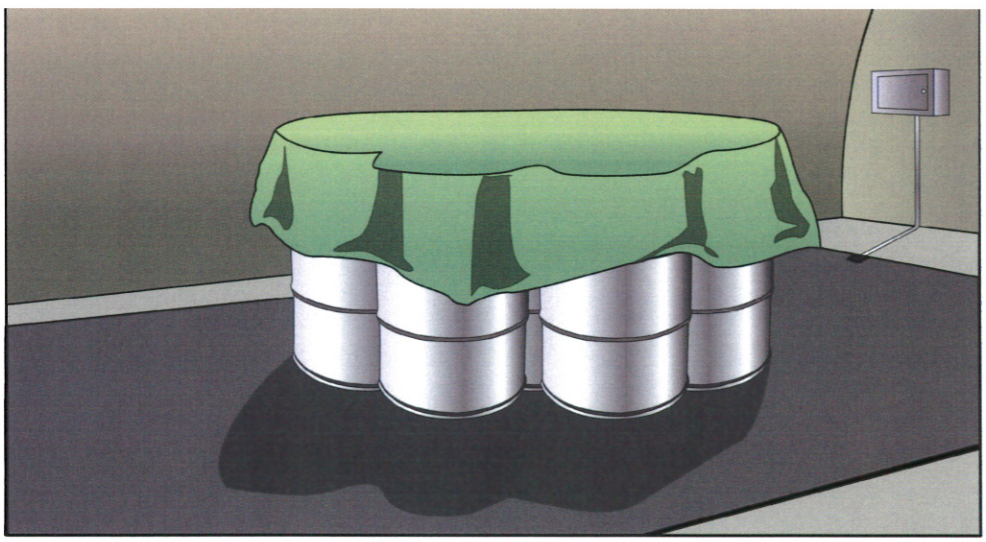

Figure 52: Pressure mat example.

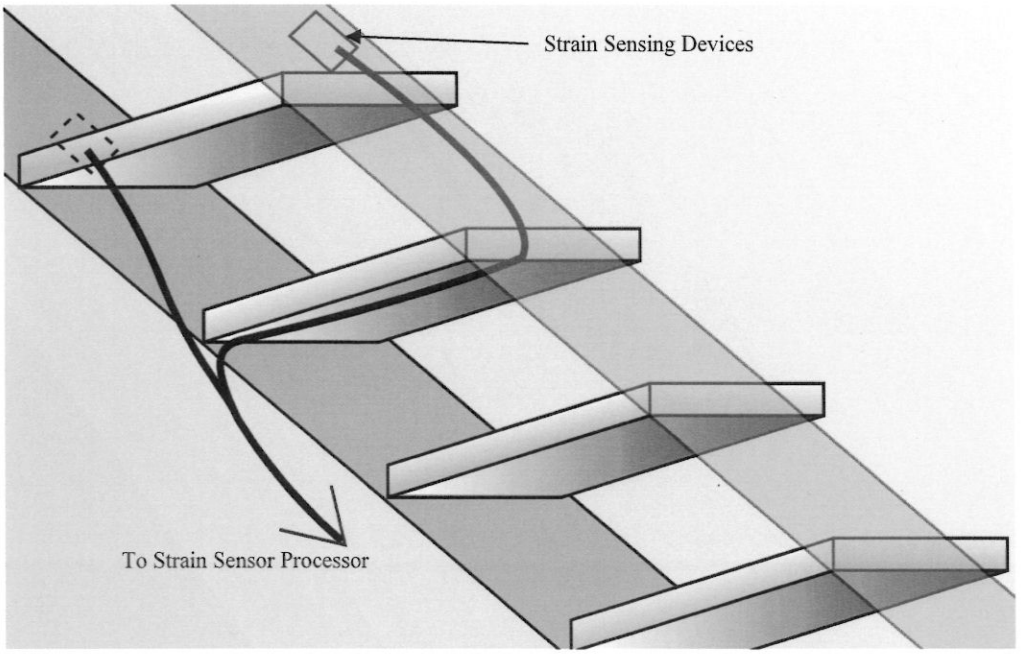

Figure 53: Strain sensor concept to detect person on stairs.

A capacitance sensor may not work well (i.e., high nuisance alarms) if the protected object is in an area where there is high traffic close to the object when the sensor is in the secured condition.

The sensitivity of a capacitance proximity sensor is affected by sudden changes in the relative humidity. Changes in the moisture content of the air will vary the dielectric characteristics by either increasing or decreasing its conductivity. If the sensor 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 a board placed on bricks or by jumping or stepping across it. A pressure sensor also is subject to considerable wear from normal traffic, and periodic tests should be performed to ensure that the sensor is operating effectively. The example mat sensor shown in Figure 54 could be used to let room occupants know that someone is at the door, but it can be easily bridged if installed this way for security applications.

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

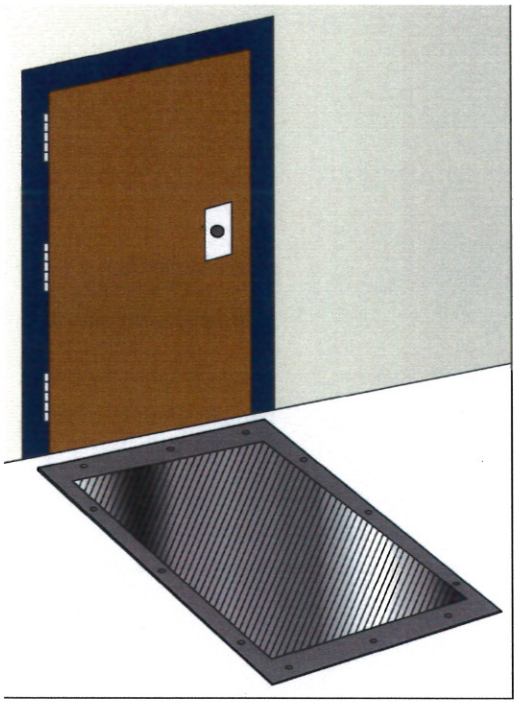

Figure 54: Mat sensor near door can be bridged if it is not installed correctly.

4.4.5 General Installation Criteria

For installation and setup of proximity sensors, manufacturer 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 a cover or door (that allows access to the sensor electronics) being removed or opened. 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 desired detection capability. Testing should include attempting to defeat the sensor using defeat methods for the sensor technology. Short-term trial operation (several days to several weeks) will help determine if there are any initial and common nuisance alarm sources. An end-to-end self test is also desirable. General installation criteria for each type of proximity sensor follow.

4.4.5.1 Capacitance Sensor

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

4.4.5.2 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.

4.4.5.3 Strain Sensor

Generally the sensing device is 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 sensor in the center of the surface. The sensor is bonded to the surface as rigidly as possible, so when the surface flexes, the sensor will be forced to elongate or contract and will not separate or slide along the surface. Site- or object-specific design and fabrication of the mounting or attaching surface may be required.

4.4.5.4 Switch Sensor

This sensor may also 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 to make it very difficult to remove or move the object while maintaining the switch in the secured position, and connection of the switch contacts to an alarm communication system.

4.4.6 Sensor Testing

4.4.6.1 Acceptance Testing

When a sensor is first installed, it should be tested in order to formally "accept" the sensor as part of the physical protection system. Acceptance testing consists of two parts:

(1) A **physical inspection** to ensure that the sensor is installed properly consists of the following:

- Verify that the installation matches the site installation documentation/ drawings, which should follow the guidance provided by the manufacturer.
- Verify that signal and power wires are routed in the conduit.
- Verify proper power levels (voltage and amperage).
- Verify correct wire connections.

(2) **Performance testing** to establish and document the level of performance is described below.

4.4.6.2 Performance Testing

Performance testing should include a visual inspection of the 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 a single person to manage.

For proximity sensors, performance testing should include tests to verify good detection when a protected item and any associated delay hardware is 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), a form to record the sensor model, serial number, settings, and other data as needed. 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.

4.4.6.3 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., activating sensor alarms by opening doors, moving through sensored areas, or being close to or touching an object such as a safe). Certain proximity sensors require a protected item to be moved or a protective cage or cabinet to be opened to activate the alarm (e.g., switch and strain sensors). Testing of these types of alarms may require increased coordination with facility personnel to ensure that safety and security are maintained during the testing.

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

4.4.7 Maintenance

Periodic operability and performance tests, in addition to any self-test invoked by the sensor or the system, need to be performed to ensure that the sensor is operating effectively. A visual inspection of the installation should be performed periodically, particularly after any major maintenance to the protected surfaces. 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, who performed the maintenance or repair, and an assessment of what may have caused the problem. Maintenance activities for each sensor are described below.

4.4.7.1 Capacitance Sensor

Extremely good housekeeping is required in the area near the protected object 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.

4.4.7.2 Pressure Sensor

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

4.4.7.3 Strain Sensors and Switch Sensors

During periodic testing, these sensors should be inspected for loose attaching hardware, loose connections and excessively worn parts.

4.5 Dual-Technology Sensors

4.5.1 Principles of Operation

Dual-technology sensors (also referred to as "dual techs") were designed to lower the false or nuisance alarm rates in an interior sensor. This is accomplished by combining two different types of sensors in one casing so that each sensor is complementary: 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 detection 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. Because of this possibility, dual-technology sensors 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, while 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. (See Figure 55.)

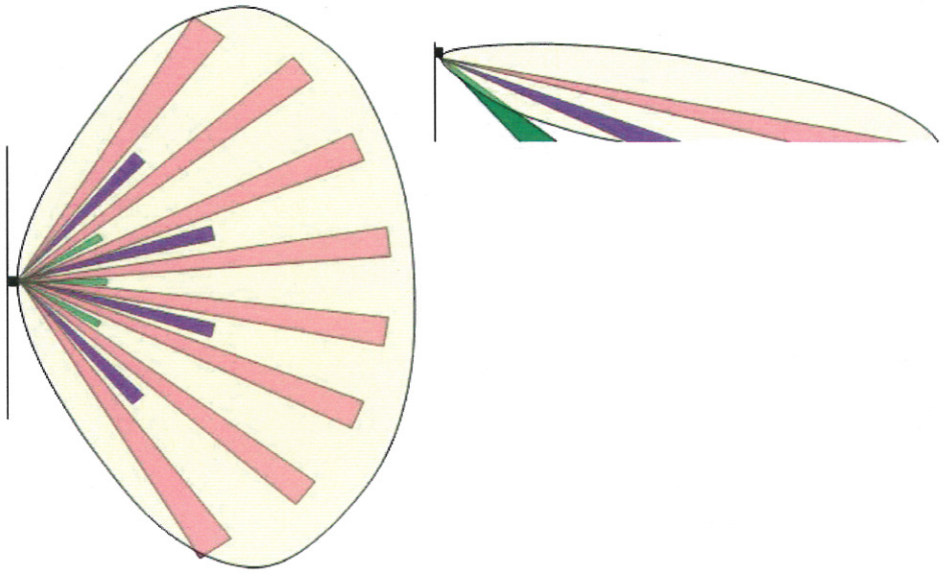

Figure 55: The figure on the left depicts an overhead view, and the figure on the right depicts a side view, of the patterns of detection for a dual-technology sensor comprising a PIR sensor and a microwave sensor; the pale yellow "bubble" illustrates the microwave detection pattern, and the remaining "fingers" illustrate the PIR detection pattern. Note that most dual-technology sensors use "AND" logic for the two different sensors, such that both sensors would have to sense a detection before the sensor would signal an actual alarm.

4.5.2 Types of Dual-Technology Sensors

Two combinations of dual-tech sensors are usually used for interior protection: Passive Infrared Acoustic and Passive Infrared Microwave. Numerous manufacturers build these sensors with varying technical specifications so care should be taken in selecting the sensor that meets the needs of the particular application.

4.5.2.1 Passive Infrared Acoustic

The PIR-acoustic dual-technology unit employs 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 anyone moving in a radial direction in the energy pattern. The shape of the PIR detection segments is similar to the ultrasonic energy pattern configuration. Someone moving in the zone of detection will create an alarm if detected by both the PIR sensor and ultrasonic sensor.

4.5.2.2 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 someone moving in the area with some radial velocity relative to the detector. This teardrop-shaped pattern typically covers an area 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 (Figure 55).

4.5.3 Sources of Nuisance Alarms

Because dual-technology sensors are normally configured to operate with "AND" 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 within most dual-technology units can trigger false alarms from sources of heat, sunshine, and incandescent lights, as well as other sources. (See "Sources of Nuisance Alarms in Passive Infrared Sensors" in Section 4.3 of this report.)

For the PIR-acoustic dual-tech sensor, the ultrasonic sensor effectiveness is reduced by air turbulence from heating or air-conditioning ducts, drafts, or other sources of moving air. Acoustic energy generated by ringing bells and hissing noises, such as the 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 an intruder, which can confuse the signal processor and result in nuisance alarms.

For a PIR-microwave dual-tech sensor, one important characteristic to remember is that microwave energy can pass through light construction material, which can be a source of nuisance alarms.

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

4.5.4 Characteristics and Applications

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

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

A PIR-acoustic dual-tech sensor can typically cover open areas 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. Since 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 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 where it is 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 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 as well as long, narrow areas up to 61 meters (200 feet) long.

When sensors are combined in a logical "AND" 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 having a 0.95 P_D, then the resulting 0.90 P_D for the dual–tech sensor is the product of the individual probabilities. A P_D of 0.90 may not meet the required probability of detection for some facilities.

Assuming a single direction of intrusion, a higher P_D can be obtained from separately mounted sensors than 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 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-tech 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" configuration, if either sensor is defeated, then 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, then another sensor (dual- or single-technology) should be used and installed in such a manner that each sensor unit protects the other, as well as providing overlapping detection coverage within the area being protected.

It is important to avoid environments where either detector type would be prone to false alarms. If either detector is exposed to an environment where it experiences a high number of false alarms, then the probability of one of these false alarms being present at the logic AND gate 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 the microwave detector would not be affected by this environment. The drafts would still cause temperature changes that could affect the infrared detector, but since 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-tech sensor that combines microwave and infrared detectors with "AND" logic is that the microwave's detection zone is usually much larger than the infrared's detection zone; hence, no detection will occur until the adversary reaches the point where both sensors can detect.

4.5.5 Installation Criteria

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

- Performance testing and evaluation should be similar to that of a PIR sensor.
- The sensor should be installed with primary consideration given to the PIR section. The most likely paths to the protected item or area should cross through the PIR detection pattern and not be directly toward or away from the sensor unit.
- A dual-technology sensor should be located so that the likely path of an adversary will be across the sensor detection area and less likely to be toward the sensor.

A dual-technology sensor should be installed using a sturdy mount. 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 such as heaters.

If dual-technology sensors are to be used, multiple sensor units should be installed, with each unit offering overlap protection of the other.

4.5.6 Testing

A regular program of testing sensors is imperative for maintaining them in optimal operating condition. Three types of testing need to be performed at different times in the life of a sensor: acceptance testing, performance testing, and operability testing.

4.5.6.1 Acceptance Testing

When a dual-technology sensor is first installed, it should be tested in order to formally "accept" the sensor as part of the physical protection system. Acceptance testing consists of two parts:

(1) A **physical inspection** to ensure that the sensor is installed properly, consisting of the following:

- Verify that the installation matches the installation drawings (and the drawings should follow the installation guidance provided by the manufacturer).
- Verify sensor intersection spacing.
- Verify that signal and power wires are routed in conduit.
- Verify proper power (voltage, amperage) levels.
- 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.

(2) **Performance testing** should establish and document the baseline level of performance (see below for a description of the recommended tests).

4.5.6.2 Performance Testing

Performance testing and evaluation should be similar to that of a PIR sensor. (See Section 4.3.6.2.) The most likely path to the protected item or area should ideally cross through the PIR detection pattern and not be directly towards or away from the sensor unit. In addition to the extensive walk tests described in the PIR section of this report, additional tests can be performed. Slow walk tests are conducted at speeds less than 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 person will likely be different than that of a walking person.

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 an electronics module is replaced, when there is a change of the physical alignment or any adjustment that can affect sensitivity, after remodeling of the building structure, or any major change in the arrangement of furniture or equipment. The performance test 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.

Within each area being monitored by sensors, the test should (1) ensure that the system meets the manufacturer's specifications for probability of detection, (2) verify that no dead spots exist in the zone of protection, and (3) 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 so that deterioration in equipment capability can be monitored. Walk tests should be performed for all areas covered by the sensor and 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 room configuration could affect sensor coverage. If room configuration has changed significantly, a complete performance test of the sensor coverage should be initiated to ensure asset or room protection. 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 questions listed below:

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

4.5.6.3 Operability Testing

The operability testing should consist of a simple walk test and tamper test on each 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 the positions numbered 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 an alarm from the sensor was received from the correct location. If any of these simple tests fails to initiate an alarm, the sensor should be checked for alignment problems.

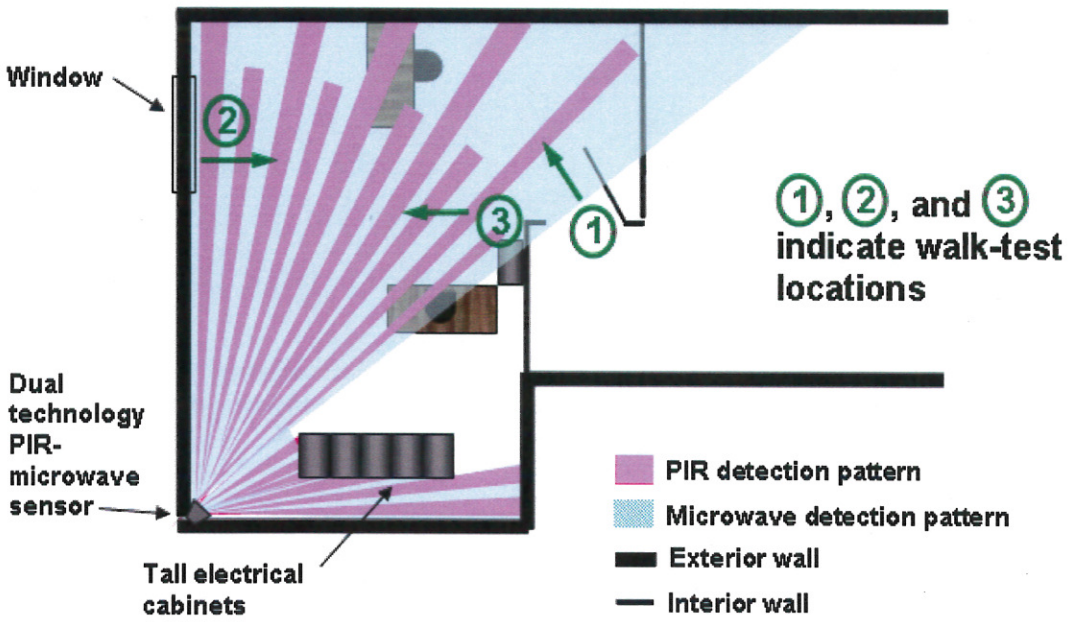

Figure 56: This diagram illustrates the possible walk test locations in a room with sensor coverage by a dual-technology PIR-microwave sensor. Note two things: (1) The microwave portion of the sensor can penetrate light construction, but since the sensor's "AND" logic requires that both sensors detect before an alarm is registered, a person in the adjoining room won't cause a nuisance alarm, and (2) the tall electrical cabinets block a portion of the sensor's detection pattern. This could be a problem if the electrical cabinets are a possible target and it is possible for an adversary to hide in the location where the detection pattern is blocked.

4.5.7 Maintenance

A visual inspection of the installation should be performed 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-test 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.

4.6 Video Motion Detection

4.6.1 Principles of Operation

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

imagers, and 360-degree-view cameras. VMD requires the addition of hardware modules and/or alarm processing hardware and software. 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 detection 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 then the DSP transmits it to the alarm stations when an alarm event has occurred.

VMD technology has experienced significant advances in the state of the art since the early 2000 timeframe. Lower performance modules are available that provide simple movement detection, while higher performing equipment employs 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.

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

Early VMD equipment consisted of a module inserted in 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 video processing implemented in these early VMD modules was simplistic and, as a result, produced numerous nuisance alarms, thus making 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 camera enclosure's front cover glass. As the 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 made active for different detection events. For example, one area could be set to alarm on any movement, while another area could be set to alarm when there was movement from right to left and not when the movement was 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 (human, vehicle), 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 to far field of view. At each location, the operator calibrates the software to an individual's height. For each location, that height calibration information is saved 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 closer to the camera

than when further away. To compensate, VMD software can scale the detection algorithm's function for identifying human movement throughout the camera's field of view.

In some VMD equipment software, it is possible to calibrate the alarm algorithm to allow detection of movement at the ground level so that movement that occurs above ground can be exempt from classification as an alarm target. That assumes that detection of a person either walking upright or crawling on the floor is the target of interest. However, if there is a concern about a person swinging into an area on a rope, 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.

VMD detection and alarm notification are based on a set of "rules" and "areas of interest" defined by a system operator. This capability allows specific detection functions to be active only within certain portions of the camera's field of view. The detection function does not have to be implemented throughout the entire camera viewing area. For example, if the area of interest is inside a large room and there is an aisle for passage through the room alongside the area of interest, the intrusion detection function can be configured to be operational for the area of interest, while human movement outside the area of interest does not trigger an alarm.

VMD vendors have established many detection rules for their hardware and software configurations. The specific kinds of rules, their functionality, and their reliability vary widely from vendor to vendor and from application to application. The technology supplied by a vendor of interest should be thoroughly tested in the specific applications envisioned before committing to the installation of a particular technology.

4.6.2 Types of Video Motion Technologies Available

VMD functionality is available in three configurations:

(1) Software running on a personal computer with video capture cards

(2) Stand-alone single- or multi-channel hardware/software modules

(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 to include a tracking function. A movable (pan-tilt-zoom) 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. Analog cameras are connected to a VMD processor using coaxial cable Bayonet Neill-Concelman (BNC) connectors, while digital cameras are connected using Ethernet connections 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, it is instructive to note that transmission of high-bandwidth video signals is, in many cases, not viable using Ethernet systems designed for message transmission such as 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.

4.6.3 Sources of Nuisance Alarms in Video Motion Detector Systems

Commercial VMD technologies have varying degrees of performance; however, performance testing of the technology has identified conditions that produce performance challenges. Generally speaking, indoor environments tend to produce significantly fewer challenges than do 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, such as trees or large birds, and 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, it is necessary to thoroughly test the VMD equipment to ensure that the equipment performs to expectation before system purchase and installation.

When used indoors where environmental variables are significantly fewer, VMD technology produces significantly 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 tend not to shake and vibrate in indoor applications, and animals are not present to trigger alarms.

4.6.4 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 are not sensing the presence of an intruder within a sensored space. Changing attributes of a video image are being analyzed by software, and the results of that analysis determine if an alarm condition is present. Current video analysis software only approximates a portion of the detection and assessment capability of the human mind. While VMD detection software has significantly improved since 2000, VMD software 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 provides that continuous observation and alerts the alarm station operator to allow 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 rather than phenomenological. Diagnostic information is also provided to the operator with a VMD alarm that is not provided with physical sensor alarms. The VMD software puts 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 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. Movements across the camera's field of view change more pixels in the image with the same amount of movement than does movement towards or away from the camera. Therefore, when VMD is used as a detection sensor, the camera should view the scene so that the detection pattern is across the camera's field of view. VMD should not be used with cameras that view scenes that experience large changes in scene illumination. For example, if a camera is oriented so that it views the inside of an exterior door, opening the door on a bright sunny day will cause a large change in scene illumination when the door is opened and may either cause a nuisance alarm or nondetection of personnel entry 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. These colors are at the extremes of the color spectrum and less decisionmaking is needed about pixel movement as compared to 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 where there are windows (particularly if the windows are facing east or west), the low sun angle entering the windows can cause persons to cast shadows inside the building. If the area of interest includes an area where moving shadows are cast, this may cause unnecessary activation of the detection and classification algorithms creating 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 results in significant image processing and analysis. If there is by chance some patterned motion within the random motion of all the pixels in motion, the detection algorithm will create an alarm because, in its analysis, there appeared to be "motion with purpose" in the video stream.

As described earlier, some VMD software algorithms can adapt to slow scene changes. This adaptive response is needed, particularly for exterior applications where outdoor illumination in lighted areas may vary by four to five orders of magnitude. Adaptive algorithms can compensate for very slow movements. A very determined intruder could gain entry into an area with very slow movement. Also, 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, an intruder could insulate themselves with highly insulating garments and then cloak themselves under another thick insulating material so that the thermal imager does not view movement of a human because everything in the thermal imager's field of view appears to be at the same temperature. In these cases, complementary sensors with orthogonal detection criteria would be needed.