

Security PACE Book 5 - Intrusion Detection

Use the Menu at left to navigate through the course.

[Course Introduction](#)

Intrusion Detection Systems and Concepts

[Intrusion Detection Overview](#)

[Perimeter Intrusion Protection](#)

[Area/Space Intrusion Protection](#)

[Object/Spot Protection](#)

[Holdup/Panic Protection](#)

[Signaling Devices](#)

Intrusion Detection Overview

Select the first topic below to begin this lesson:

- [Typical Area Requiring Intrusion Detection Coverage](#)
- [Control Panel and Keypad Basics](#)
- [Types of Intrusion Detectors](#)

[TOP](#)

Typical Area Requiring Intrusion Detection Coverage

Intrusion Detection, in its simplest form, is the process of recognizing something or someone is in an area where — at this moment in time — they should not be. Probably the most foolproof method of Intrusion Detection is placing a human observer at every location to constantly monitor the entire area of coverage. While this may be foolproof, it may well be foolhardy, for the costs of such a "system" would be impossible to justify. Current Intrusion Detection systems thus combine technologies that afford high levels of detection, using cost-effective methods and equipment.

Traditional Intrusion Detection systems focused on incursions from the outside — that is, around the perimeter of a space — but it is essential for effective Intrusion Detection systems to monitor not only external events but

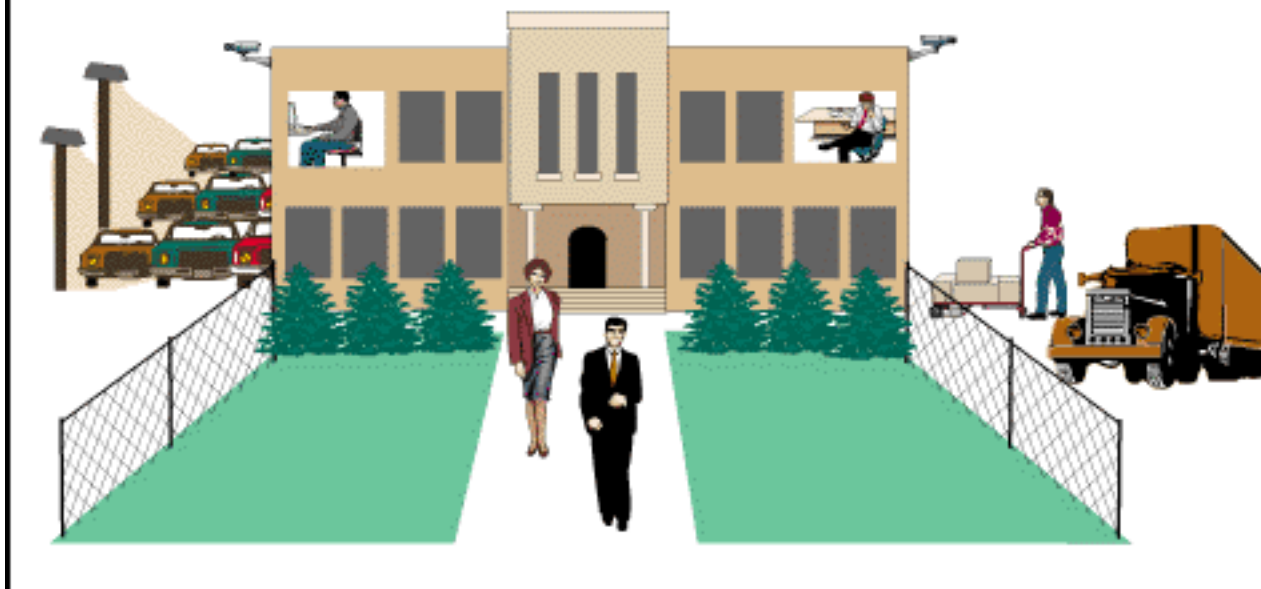
internal events (events occurring within the boundaries of the area of coverage) as well. An example: an R&D laboratory will be in use during the day, but when all lab personnel have logged out for the day, no movement should occur within the boundaries of the laboratory. In this instance, compromised security may come from within the confines of the building in which the lab is housed, and simple peripheral Intrusion Detection would never isolate the intruder.

An effective Intrusion Detection system provides capabilities to detect both external and internal incursions. Such systems include three major components:

- ◆ Detection devices
- ◆ Central processing device (control panel)
- ◆ Alarm or notification devices.

After a brief look at control panel basics, we will focus on various security detection devices in the remainder of this PACE Book.

Typical area requiring Intrusion Detection coverage



Control Panel and Keypad Basics

As you will learn in the following pages of this PACE Book, there are many types of Intrusion Detection devices. At their most basic, they all act as switches. Any change in their normal state — closing (completing a circuit) if normally open, or opening (breaking a circuit) if normally closed — causes the control panel to issue an alarm. It is the task of the control panel to monitor the various states of the devices connected to it, and respond when an event occurs.

The most basic control panel is little more than a switching device. Today, with significant advances in technology, most control panels contain sophisticated processing capabilities to do much more. For example, all

control panels should contain some type of "self-security" — specifically at least a fundamental level of password protection. Another important feature is the ability of the control panel to provide a history of events (or a log) occurring within the system.

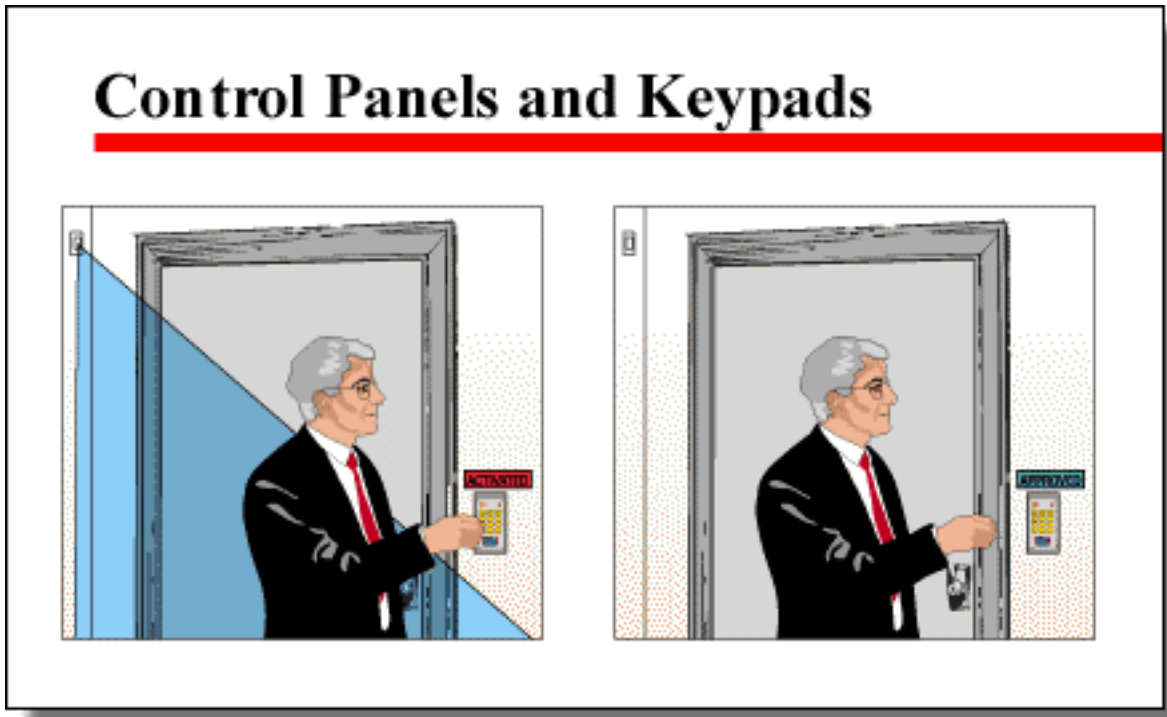
Typically, an Intrusion Detection system is designed around a series of zones. A zone may contain several detection devices located in the same general area. Most basic control panels allow for up to eight (8) zones. In this basic panels, an operator will only know that an event has occurred in a given zone.

More advanced systems feature addressability. With this capability, each device is assigned as "address" — a code. When the device reports to the control panel, it sends this code. Addressability allows the operator to determine exactly which device within a zone has been triggered. This, in turn, provides an exact and immediate location of the possible problem.

Operators interact with the control panel using a keypad (with LCD or LED displays) or in the most advanced systems, a workstation consisting of a computer screen and keyboard. Even with a keypad, an authorized operator has a great deal of control over the system:

- ◆ turn the system on or off
- ◆ identify the alarm state of the system
- ◆ locate the zone or specific device causing an alarm condition
- ◆ suspend an alarm condition
- ◆ perform a system reset

- ◆ display an event.



Types of Intrusion Detectors

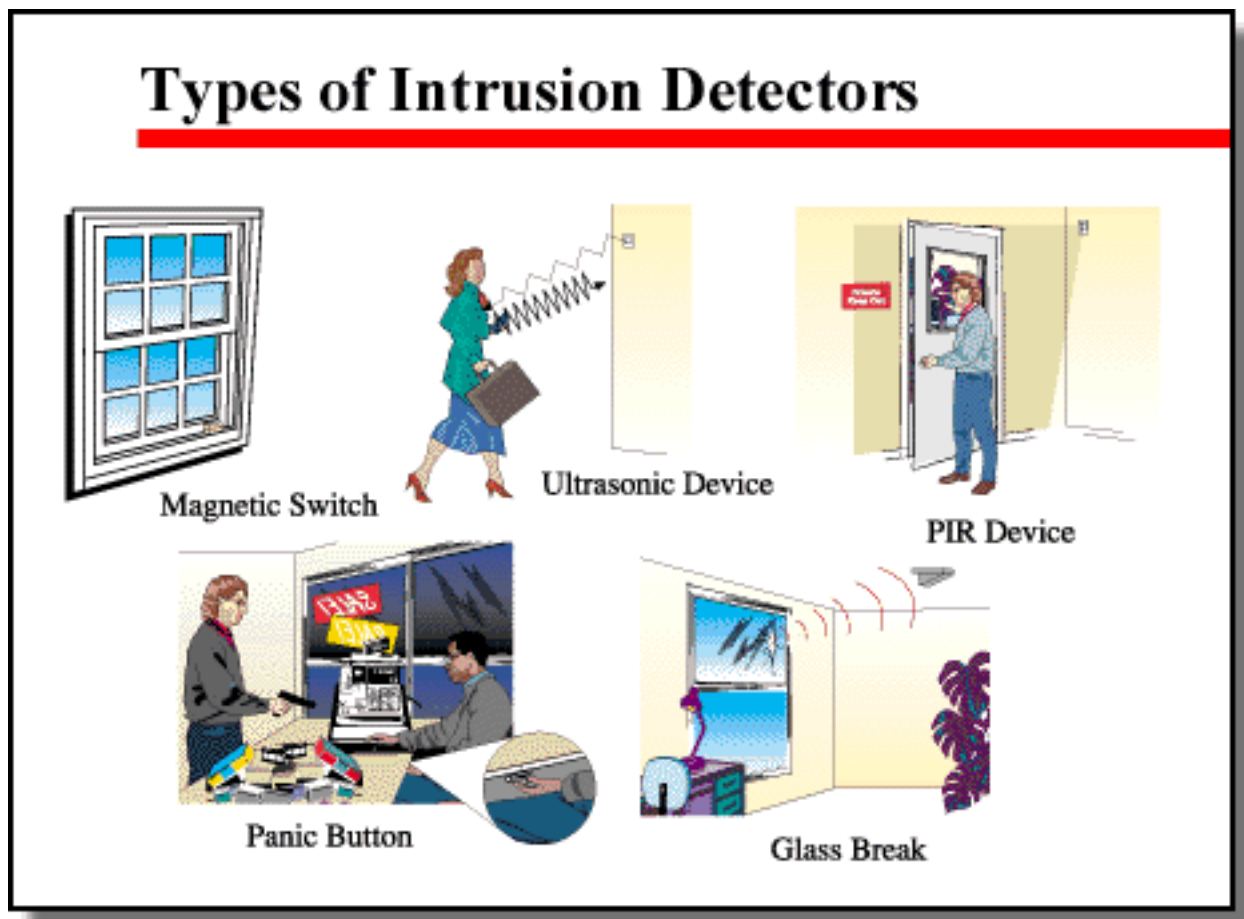
We have indicated that there are two basic types of Intrusion Detection concerns: intrusions from outside and intrusions from within.

Perimeter detection devices respond to outside incursions. Within the interior, there is a range of specialized detection technologies available. A complete listing of detection devices — for both exterior and interior — includes:

- ◆ perimeter detection devices
- ◆ area/space detection devices

- ◆ object/spot detection devices
- ◆ holdup/panic alarm detection devices
- ◆ signaling devices

Each of these detection "sub-systems" will be discussed in detail in the following sections. In each of these types of detection system, note that often two detectors using different technologies may be combined to create "dual technology" solutions. Using dual technology can provide strengthened detection capabilities given the nature of a specific environment.



Perimeter Intrusion Protection

Select the first topic below to begin this lesson:

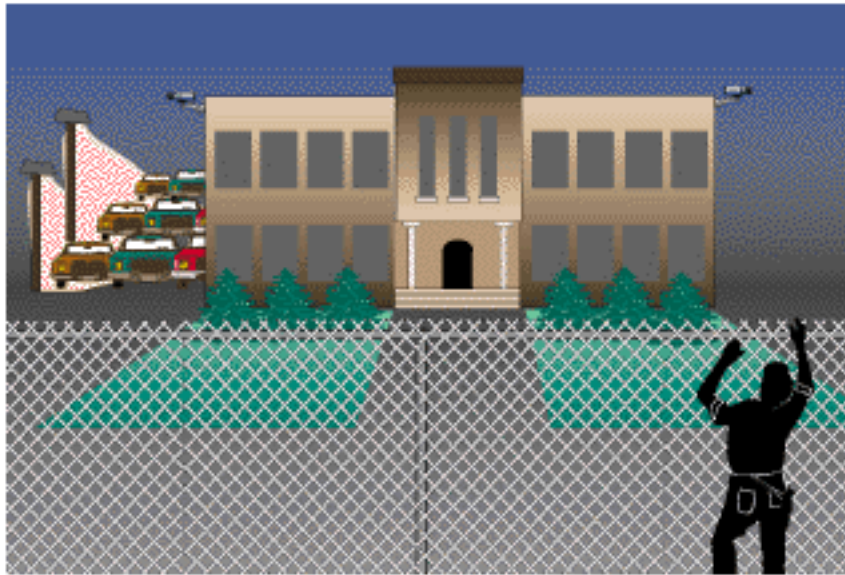
- [Perimeter Intrusion Protection](#)
- [Fence Intrusion Detection](#)
- [Exterior Microwave Detection Devices](#)
- [Microwave Detector Coverage](#)
- [Glass Breakage - Foil Detection](#)
- [Glass Breakage - Audio Detection](#)
- [Intrusion Detection: Magnetic Switches/Contacts](#)

Perimeter Intrusion Protection

Consider almost any type of facility. It might be a school, medical facility, or office building. In any of these cases, there may actually be several boundaries or perimeters. The edge of a site as marked by a fence, the area between a fence and a building, and the actual walls of the building(s). There are several devices to handle Intrusion Detection at each perimeter.

The first defense against intrusion occurs at the point farthest from the core area of coverage. In many instances, such Intrusion Detection will be located at fences surrounding the property.

Perimeter Intrusion Detection



Fence Intrusion Detection

The most basic form of fence Intrusion Detection is a simple single-strand 24 or 26 gauge copper wire, having a low tensile strength. This is often referred to as a "breakwire." When woven into a fence, such a wire will break with excessive movement of the fence. In some instances, in addition to restricting human access, fence Intrusion Detection may also be designed to sense the presence of animals in the protected area. Note that this form of detection is easily defeated.

Newer fence systems may utilize fiber optic cable. Instead of signaling an alarm when a wire is broken, in fiber optic systems, an alarm sounds when movement

along the fence results in bending of the fiber optic cable.

Perhaps the most common fence Intrusion Detection system is built around a photoelectric cell. Here a light source sends a narrowly focused beam of light, either in single, dual, or quad configurations, to a photoelectric receiver. When the beam is interrupted, the system is notified.

Exterior Microwave Detection Devices

For Intrusion Detection across a larger area, microwave sensing devices may be used. To begin, be aware that microwave protection should be approached with caution. It can be difficult to setup and is susceptible to electrical and RF (radio frequency) interference. It is therefore prone to false alarms. At a time when police departments are almost universally instituting policies which impose fines for unacceptable levels of false alarms, the use of microwave systems should be carefully considered. In addition, it is expensive. Often other detection solutions — e.g., infrared or ultrasonic — provide greater reliability at a lower cost. With these cautions noted, we now look briefly at microwave operation.

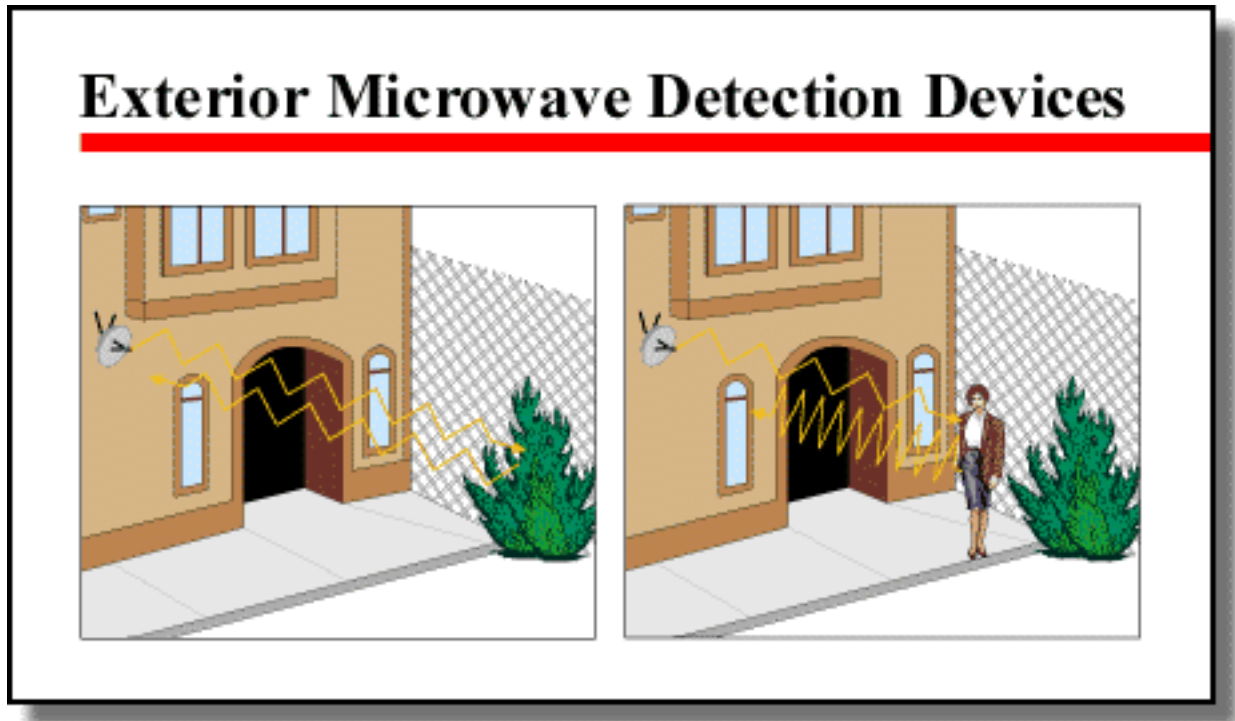
Microwave sensing devices, as with all devices designed around wave-processing, rely on a predictable phenomenon called the Doppler Effect. This effect applies to all energy transmitted in waves — radio (as is microwave), sound, light, etc.

To understand the Doppler Effect, imagine standing beside a highway with a vehicle — a large trailer truck, for example — approaching. The sound seems to increase in pitch slightly as it approaches, but as the truck passes by, the sound suddenly lowers in pitch and rapidly fades. Keep in mind we are talking about tone not volume.

What is actually happening is that when the truck approaches, the sound waves which are coming from the truck are actually being compressed. The forward movement of the truck "squeezes" the sound waves together. In effect, the squeezed sound waves are closer together, and thus have a higher frequency. Interestingly, if the truck was stationary, and we were able to approach at high speed (without of course creating our own sound — wind, noise, etc. — so we could still hear the truck, the sound would also change in pitch.) This phenomenon of moving energy waves is known as the Doppler Effect.

Now apply this to a microwave motion detection device. Radio waves are sent out into an area. Because there are objects in the area, e.g., walls, fences, light poles, shrubbery, etc., some of the radio energy is reflected back to the sensor. Because there is no movement in the area, as the sensor compares the frequency of the reflected waves, it "sees" no differences. If, however, something does begin to move in the area of coverage, the sensor immediately recognizes a change in frequency of the waves being reflected off the object in motion. The sensor will then signal an alarm. Microwave sensors are adjustable. They may be "tuned" to meet the specific conditions of the area of coverage. These adjustments allow the system to ignore smaller reflections of waves,

that is, a change in size (amplitude), rather than frequency, thus eliminating false alarms due to small animals, etc.

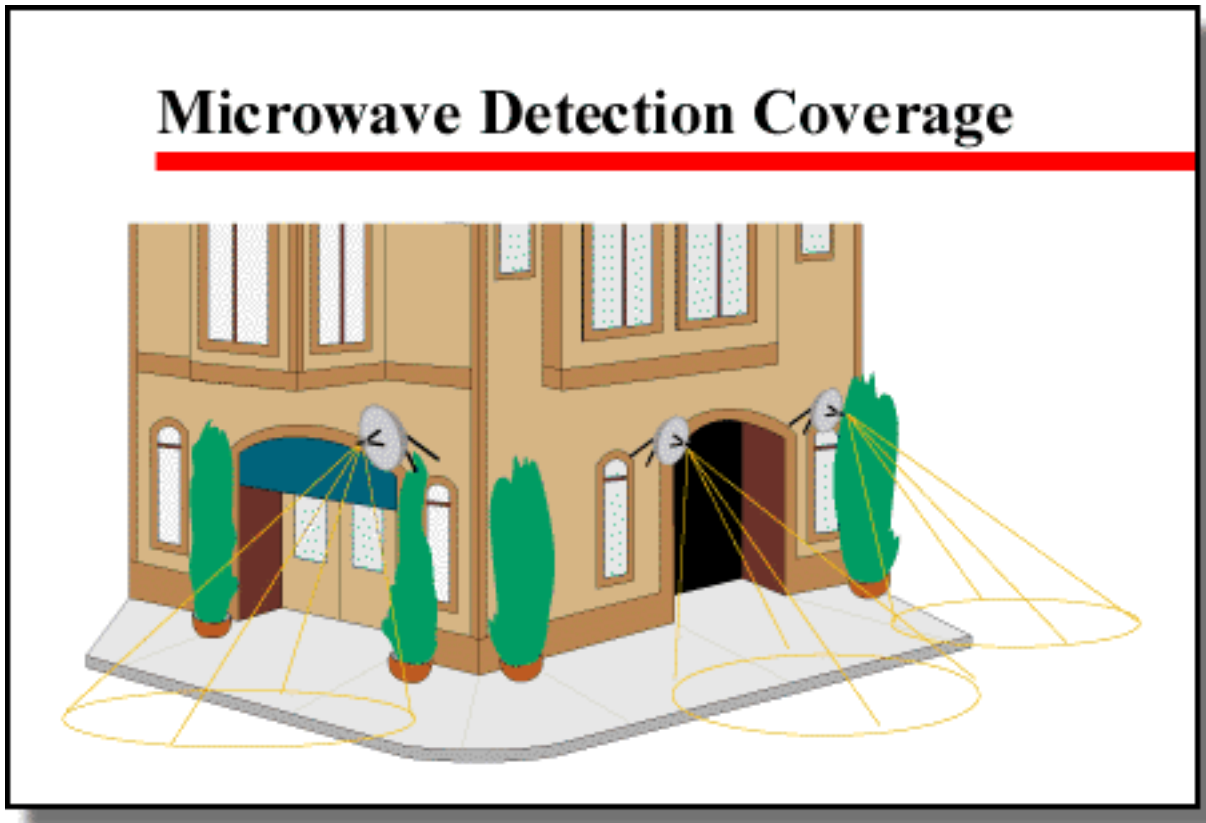


Microwave Detector Coverage

Microwave detectors can be configured to provide several different coverage patterns, using either wide or narrow beams. Narrow beams may be used along a narrow perimeter; however, keep in mind that the change in wave frequency (Doppler Effect) is more pronounced when the waves are striking the sensor head-on. For this reason, ideally the sensors should be positioned to anticipate "in-coming" movement as opposed to side-to-side movement.

Microwave detectors must be carefully aligned and adjusted to minimize the possibilities of false alarms.

Further, as mentioned earlier, some applications (e.g., exterior locations with frequent rain, snow, fog, etc.) simply are not suited for microwave technology.



Glass Breakage - Foil Detection

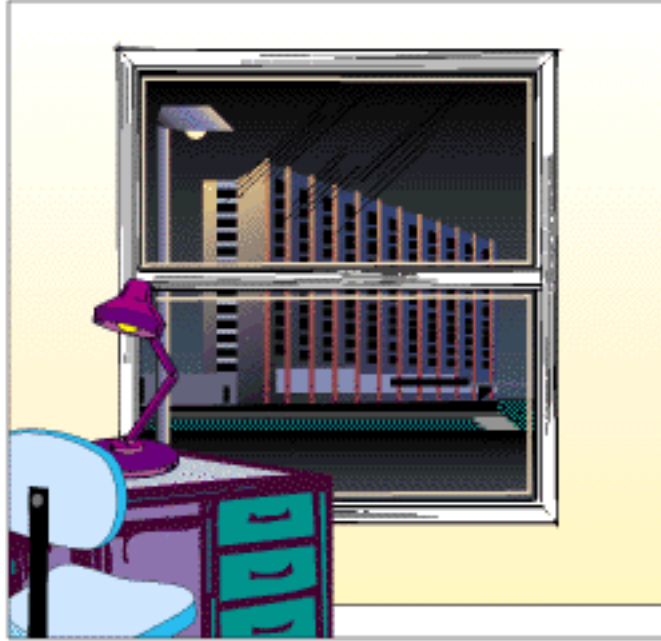
The last perimeter before the interior of a secure building is the building's walls, including, of course, windows and doors. Obviously one way to gain access to a secure area is simply to break the glass in a window or door. An older technology designed to detect such breakage is Window Foil. Foil comes in either 1/2" or 1" strips and is adhered to the edges of a glass window or door on the secure side. A current (rated at 60 ma to 60 volts) is applied to the foil and any break in the foil results in a break in the electrical circuit, thus initiating an alarm. The theory is that any breakage of glass results in breakage of the foil.

In practice, it is possible to cut glass without breaking the foil, thus defeating the detection system. In addition, foil is fragile and susceptible to scratches or cuts, which may result from accident (e.g., window cleaning), intentional illegal activity, or even normal expansion and contraction of the glass surface due to environmental changes.

Note that foil is clearly visible to intruders. Some experts suggest that this may deter some intruders; others suggest such visibility only serves to warn intruders. If, for example, the foil is broken, this will be apparent to an observant intruder, and the intruder will know the glass detection system is not functional. It should be clear from our discussion of foil technologies that it requires a high level of regular inspection and maintenance.

In response to some of the limitations of foil, variations in foil technology exist. For example, some foil applications use copper wire embedded in the foil. Another variation, although considerably more expensive, is a specially manufactured glass which has a thin wire embedded in the glass itself.

Foil Detection



Glass Breakage - Audio Detection

We have discussed the limitations of foil as a means of detecting glass breakage. There is a more sophisticated technology available to detect such breakage. These are electronic devices which combine specialized microphones and circuitry to "listen" for the sounds of breaking glass. As the technology has become more sophisticated, audio detection devices have become more sensitive and more "tuned" to specific events or effects. The most basic employs general sound detection, which evolved to shock detection, then vibration detection and finally flex detection.

Audio ("acoustic") detectors are mounted on a wall or

ceiling and are "aimed" at the glass. They "hear" the sound of breakage through the air. Shock, vibration, and flex sensors are physically mounted on the surface of the glass or framing and "feel" changes in the surface (shocks, vibrations, deflections, etc.)

The human ear can generally discriminate between sounds almost instantaneously. Even without seeing it, when we hear a bat hitting a baseball we know what's happened. Similarly, we know immediately the sound of a ball breaking a window.

Transferring this capability to electronic circuitry requires the sound characteristics of breaking glass to be "memorized" by the sensor. In addition, the task becomes more complex because of the wide range of variations possible: the type of glass involved and the environmental characteristics of the location.

For example, types of glass include:

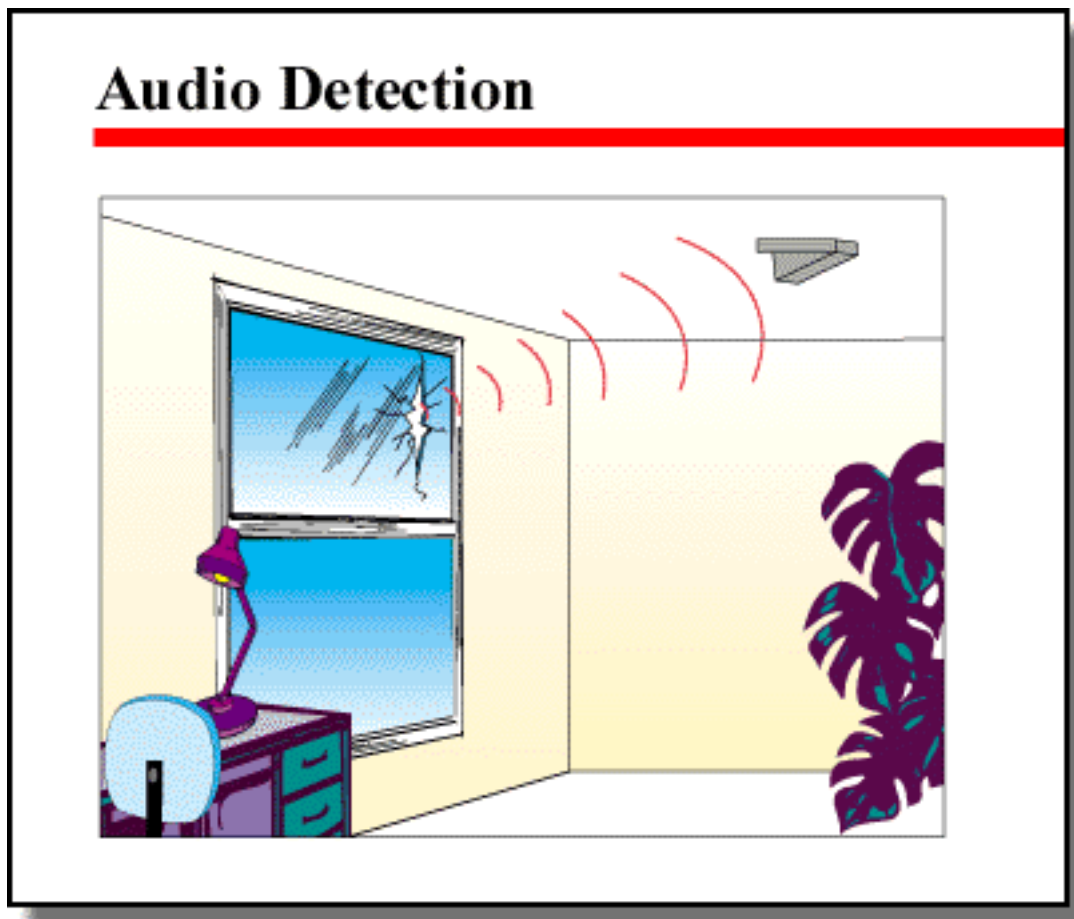
- ◆ standard window glass
- ◆ plate (heavier than standard window glass)
- ◆ safety (tempered)
- ◆ laminated (plastic layer between two pieces of glass)
- ◆ showcase/jewelry case glass
- ◆ embedded wire

Each of these different types of glass present a somewhat different breakage "sound signature," and an effective audio glass breakage detector system must be able to recognize all of these signatures. Note that with other types of intrusion detectors, audio glass breakage

detection systems can also combine dual technology solutions; that is, two types of detectors may be employed in a single application, thus reducing the possibility of false alarms.

Location environment may effect the performance of audio glass breakage detectors. Environmental factors include curtains, blinds, or other window treatments, floor and wall coverings, and objects between the glass and detector.

In addition, placement of the detector is also important. All glass breakage detectors must be mounted in accordance with the specifications determined by the manufacturer.



Intrusion Detection: Magnetic Switches/Contacts

Various types of intrusion switches are additional tools in providing Intrusion Detection. There are two basic types of switches:

- ◆ mechanical
- ◆ magnetic

Switches may either recessed (or "embedded"), that is, inserted into the window or door, and thus invisible, or surface-mounted on the door or window. While surface mounting is easier and faster to install, the switches are easily visible, and thus more susceptible to compromise.

Mechanical switches may be either plunger or lever types. Both are mounted on the moving portion of the door or window. These switches are normally closed. When mounted on a door or window, closing the door or window, closes the switch, and the current applied, completes the circuit. Opening the window or door, returns the switch to the open state, breaks the circuit, and initiates an alarm.

A third less common type of mechanical switch is a two-contact device, with one side attached to the fixed part of the window or door jamb and the other side side attached to the moving window sash or the door itself. When the door or window is closed, the two sides are in physical

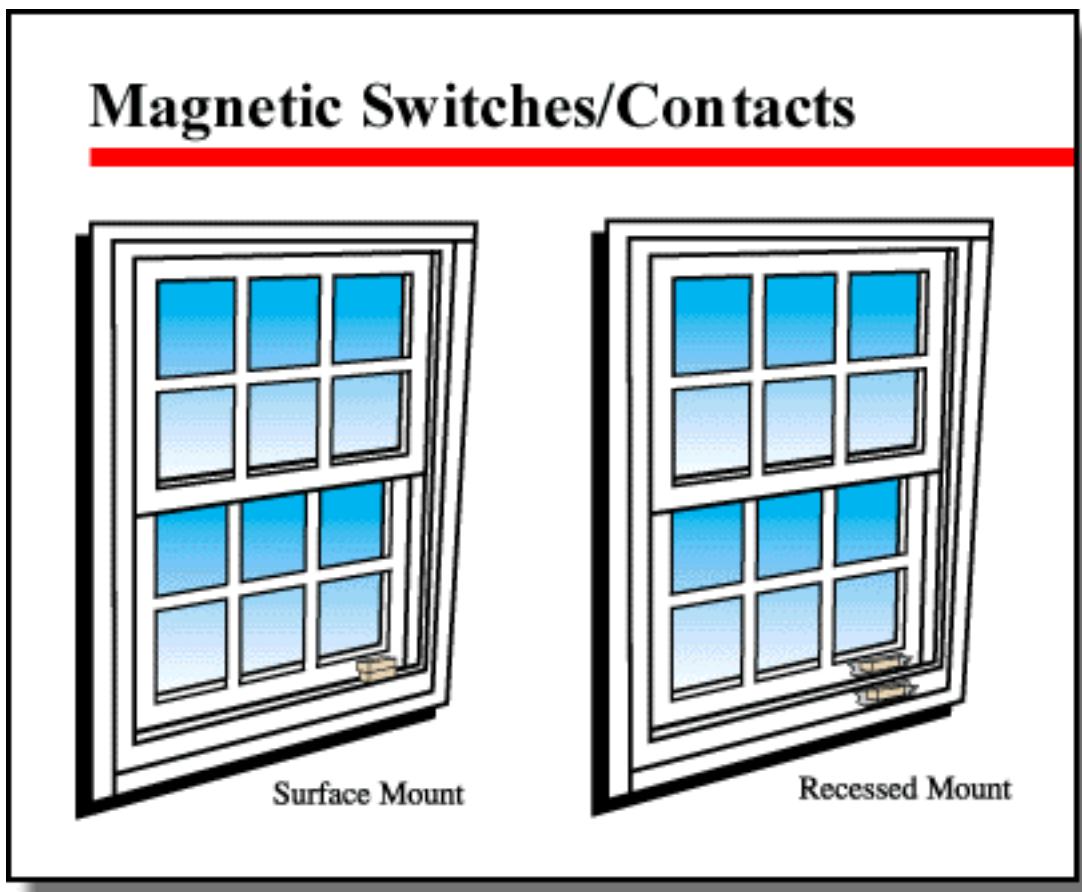
contact, thus completing the circuit. Opening the door or window breaks the circuit, thus initiating an alarm.

Mechanical switches may be susceptible to extreme environmental conditions such as wetness and temperature. In addition, such switches may be susceptible to vibration caused, for example, by passing vehicular traffic. Finally, roll-up door contacts are susceptible to wear and vibration. Such contacts must be sufficiently durable to withstand the excessive movement that often results from opening and closing a roll-up door.

Magnetic switches involve two components arranged so that they are next to each other when the door or window is closed. The first component, a magnet, is placed in the moving portion of the door or window unit. The second compartment, the actual switch, is mounted in the jamb. The switch is magnetically sensitive. With a magnet close to it, the switch remains closed. When the magnet is moved between a 1/2" and 2" away from the switch, the circuit is broken and an alarm is initiated. For this reason, a magnetic switch must be mounted no more than 2" from the door jamb.

By applying a magnetic field to the switch, an intruder may defeat a simple magnetic switch. To counter such a possibility, more sophisticated magnetic switches may be used. These devices are called "balanced magnetic switches," and they actually "balance" the switch to the unit's magnet. These high security switches utilize a glass reed switch with mercury for balance. When an additional magnetic source is present, the switch is pulled "out of balance," and the switch closes, thus initiating an alarm.

A final note regarding mechanical switch devices. Occasionally, you may encounter pressure mats, although these are typically utilized more in residential applications and "older" commercial applications. Similarly, wire grid systems were utilized in mechanical rooms to cover fresh air openings in ducts. Grids were also used in special government type applications including within wallboard to prevent penetration directly through a wall to a secure area.



Area/Space Intrusion Protection

Select the first topic below to begin this lesson:

- [Passive Infrared Detector](#)
- [Microwave Intrusion Detection](#)
- [Passive Infrared Detectors - Theory and Operation](#)
- [PIR Detectors - Application](#)
- [Dual Technology Sensors: Combining Detectors](#)

Passive Infrared Detector

For some applications, it is not enough to know if an intruder has breached a perimeter. In some instances, it may be every bit as important if an intruder has entered an interior space.

There are several technologies to accomplish this:

- ◆ Microwave - using radio waves
- ◆ Passive Infrared (PIR) - using heat energy
- ◆ Ultrasonic - using sound waves
- ◆ Dual technology - combining two of the above technologies

Passive Infrared Detector



Microwave Intrusion Detection

The theory and functioning of microwave detectors has already been discussed in Section Two of this PACE Book. We simply note here that microwave technology may also be used inside a building as well as in exterior applications.

Keep in mind that microwave detection devices are available to meet a wide range of coverage requirements, but also remember that microwave detection systems are application dependent. Their effectiveness may be severely impacted by a number of environmental factors

such as climate, localized electrical or radio interference, etc. This limitation, combined with their higher cost, may make other alternatives a better choice.

Passive Infrared Detectors - Theory and Operation

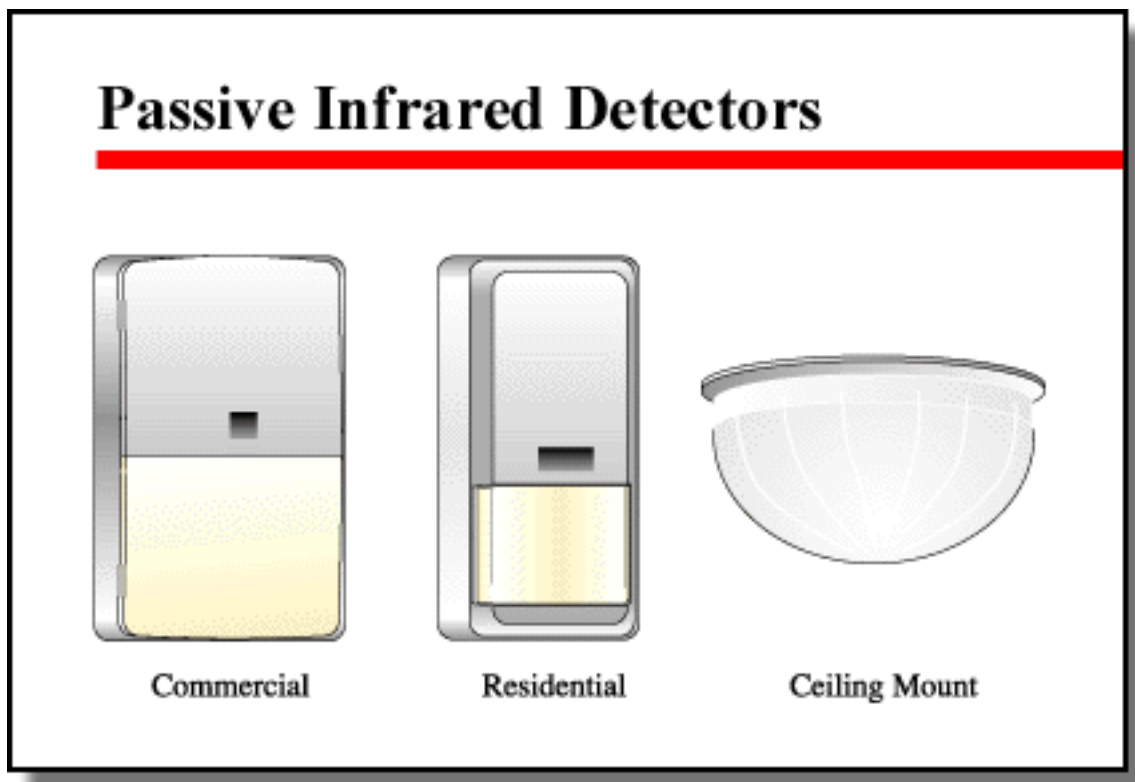
Infrared light is invisible. Actually, on the spectrum of electromagnetic energy, infrared energy falls between visible red light and microwaves. Any object with a temperature above absolute zero (virtually every object, therefore), radiates infrared energy. Infrared is blocked by solid objects and while it can pass through glass, infrared energy is distorted. Further, infrared can be degraded by dust or moisture (rain or fog). This energy, while invisible to the human eye, behaves in many respects like light; therefore, it is possible to make infrared photographs, using a special film.

It is also possible to design sensing devices that can detect infrared. Passive infrared (PIR) detectors do not generate an energy (unlike active infrared devices which do generate infrared energy). Rather, passive infrared detectors are designed to make use of infrared energy which virtually all objects generate. Using a lens or mirrors to determine coverage patterns, the detector focuses the radiated energy on the sensor face. The area of coverage of a PIR device may be adjusted using circuitry built into the detector. In addition, such detectors have an externally mounted LED which provides a visual indication that the device is functioning. A detector's

sampling rate may also be adjusted to sample infrared sources. Note that the LED flashes each time the detector samples the area for changes in the infrared "signature." Thus a higher sampling rate will be evidenced by more than frequent LED flashes.

The sensor then converts the infrared energy to electrical energy. Finally, using specially designed processing circuits, the detector unit determines whether or not changes in the levels of received energy represent an intruder in motion. If the energy signature meets predefined criteria, the detector initiates an alarm.

PIR detectors contain circuitry to cancel noise and help eliminate the possibility of false alarms. These detectors may be configured for standard and high sensitivity, wide and narrow focal lengths, and distance of coverage. Note that the distance of the PIR detector from the area to be covered has an impact on both the degree of sensitivity and the size of the area that the detector can monitor. As the distance between the detector and the coverage area increases, the size of the area that can be monitored diminishes. This is because the PIR detector's field of sensitivity narrows.



PIR Detectors - Application

Placement of PIR detectors is critical for successful detection of intruders. Begin by determining what areas you wish to keep secure. Next, analyze the most likely route(s) that an intruder might use to get to those locations. In general, these are the same halls, stairways, and other spaces used by authorized personnel.

Infrared detectors are most effective when the rate of change in the infrared signal is most dramatically visible. 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 significantly more effective than positioning the detector so an intruder would walk head on toward the detector.

Most PIR detectors have a recommended mounting height (as specified by the manufacturers). Exactly where a detector is located — height and angle of view, for example — will effect how well the detector identifies intruders. The proper placement of the detector is a function of the sensing pattern of the detector. A detector with a narrow sensing pattern and which is mounted too high, may fail to detect the presence of an intruder underneath the detector's sensing pattern.

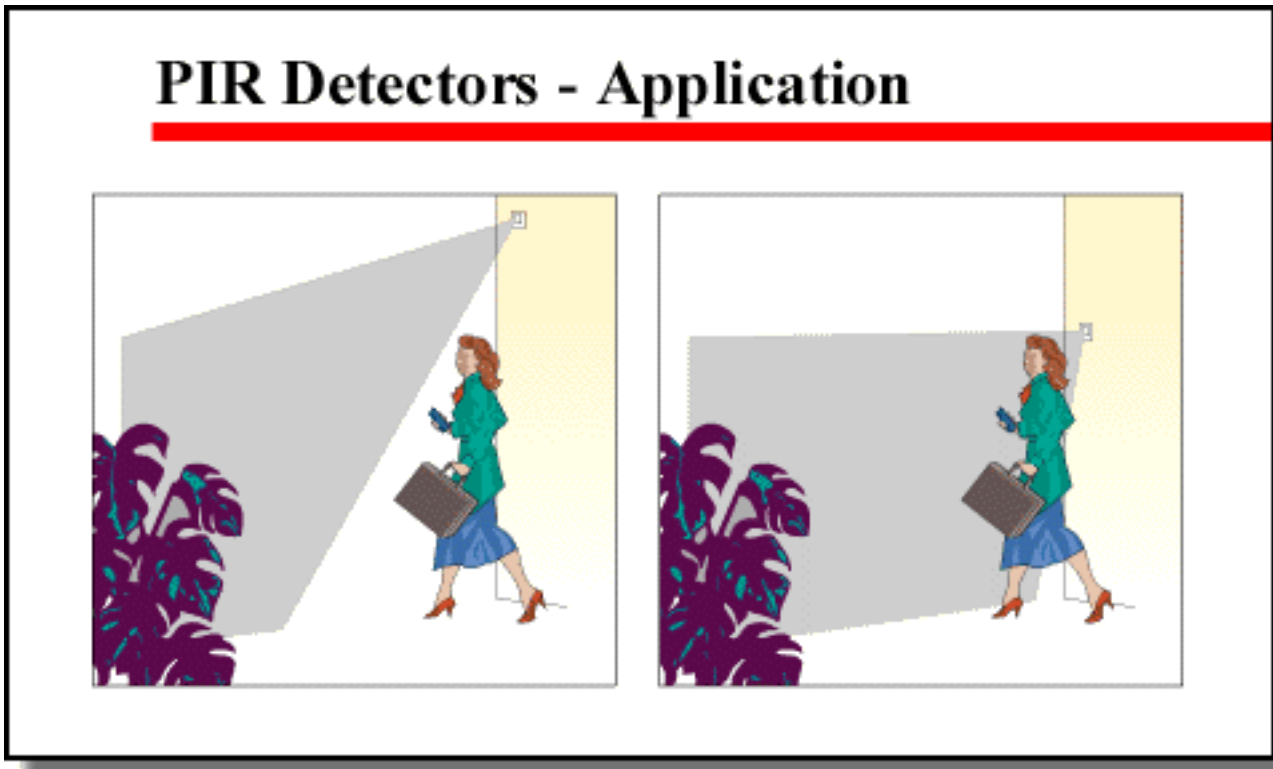
On the other hand, mounting a PIR detector so it's sensing pattern reaches the floor may generate a number of false alarms, particularly if there are animals present in the area. In such instances, dual technology solutions may provide superior detection.

Also note that heat (from radiators, vents, etc.) and cold (from air conditioning) can affect a detector's ability to sense moving sources of infrared energy. Direct sunlight and even uninsulated walls and large windows are also sources of variable infrared energy. Try to minimize the use of PIR detectors in areas where there are such temperature regulating devices. Detection patterns should match application. Some PIR detectors, for example, provide 360° coverage; others provide narrow-beam and long-range capabilities. The nature of the area of coverage — e.g., hallways, warehousing, plenum ceilings, areas around rollup doors, etc. — helps define the exact type of PIR detector required.

Keep in mind that infrared energy is blocked by solid objects; therefore, position PIR detectors accordingly. PIR detectors

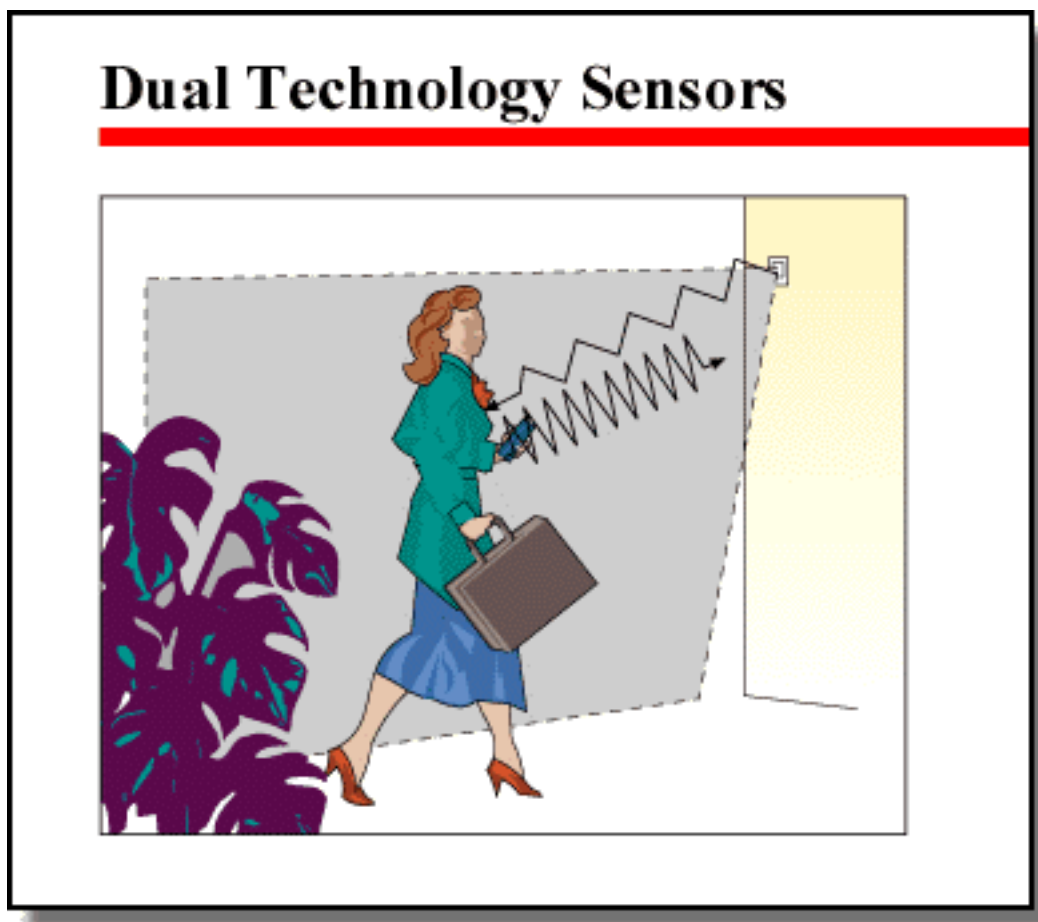
may have limited effectiveness in a large space filled with cubicles, for example.

Finally, in many applications, multiple detectors may be required in order to provide continuous overlapping coverage with no dead spots. This approach helps ensure the highest levels of security coverage in large areas such as warehouses.



Dual Technology Sensors: Combining Detectors

Dual technology devices are able to provide additional levels of detection because their ability to discriminate between true and false alarm conditions are greater. In such applications, it is essential that both technologies complement each other and do not cancel each other out. The ability of both detectors to work together without conflict is known as "handshaking." By combining both passive infrared and ultrasonic technology, for example, an alarm may be generated only when both technologies recognize an intrusion. Thus the strengths of both types of detection technologies help eliminate false alarms and further enhance the capabilities of the system to detect intrusion.



Object/Spot Protection

Select the first topic below to begin this lesson:

- [Object/Spot Protection](#)
- [Vibration Detectors](#)
- [Capacitance Proximity Sensor](#)

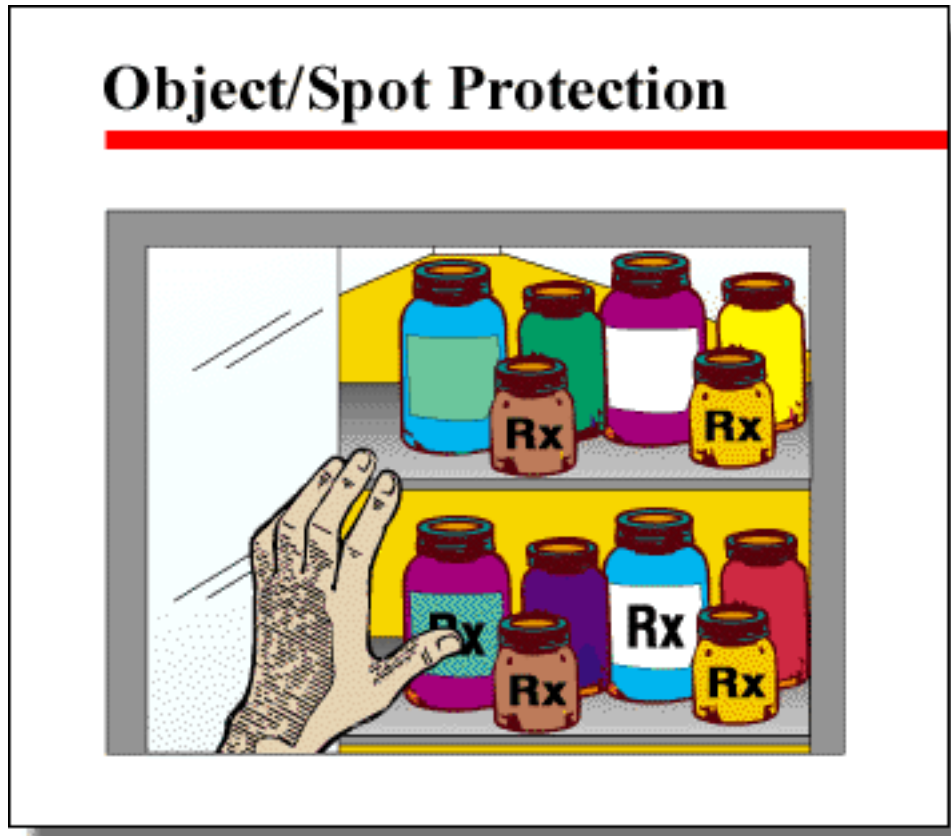
Object/Spot Protection

In addition to Area/Space Intrusion Protection, specific objects or "spots" within a space may be protected with Intrusion Detection devices. There are three basic devices that can be used to protect objects:

- ◆ simple tamper switches
- ◆ vibration detectors
- ◆ capacitance proximity sensors

The specific object and location may dictate which of these devices individually or in combination will provide the most effective object protection. For the most basic security, a simple switch may be adequate. Consider a tamper switch mounted under a small statue or bust. Lifting the object will immediately initiate an intrusion alarm, although obviously such a switch alone may not

prevent a "snatch and grab." For increased protection, coverage utilizing more sophisticated technologies is required.

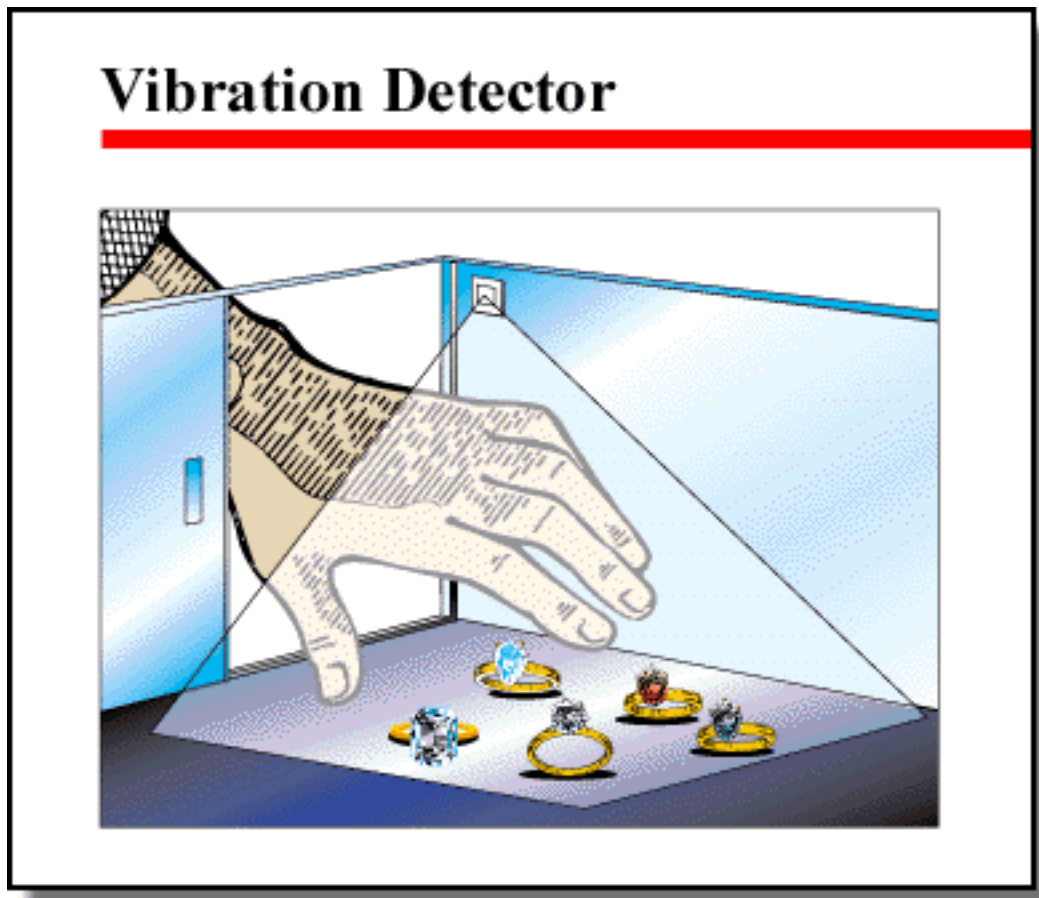


Vibration Detectors

A vibration detector is actually a component system composed of a processor unit and one or more specialized microphones. Usually, the microphone component is mounted on the object to be protected or within the protected area. The device is "tuned" to hear frequencies which are associated with the actions of an intruder, assuming that such actions create vibrations. Such vibrations may be either above or below the normal range of the human ear. These vibrations strike a membrane in the microphone, causing it to move, and

this movement creates variable electrical impulses. The impulses are analyzed by the vibration detector's processing unit. Comparing the vibration it is sensing to a "signature" stored in the device's memory, the unit is able to determine whether or not to issues an alarm.

A common application for vibration sensors is vault protection. Remember that virtually everything in our environment will generate a vibration. This may be undetectable to the human ear or touch, but such a vibration may be sensed by the proper equipment. When installed on a vault, a vibration detector, tuned to the appropriate frequency, will trigger an alarm when the vault's integrity is compromised.



Capacitance Proximity Sensor

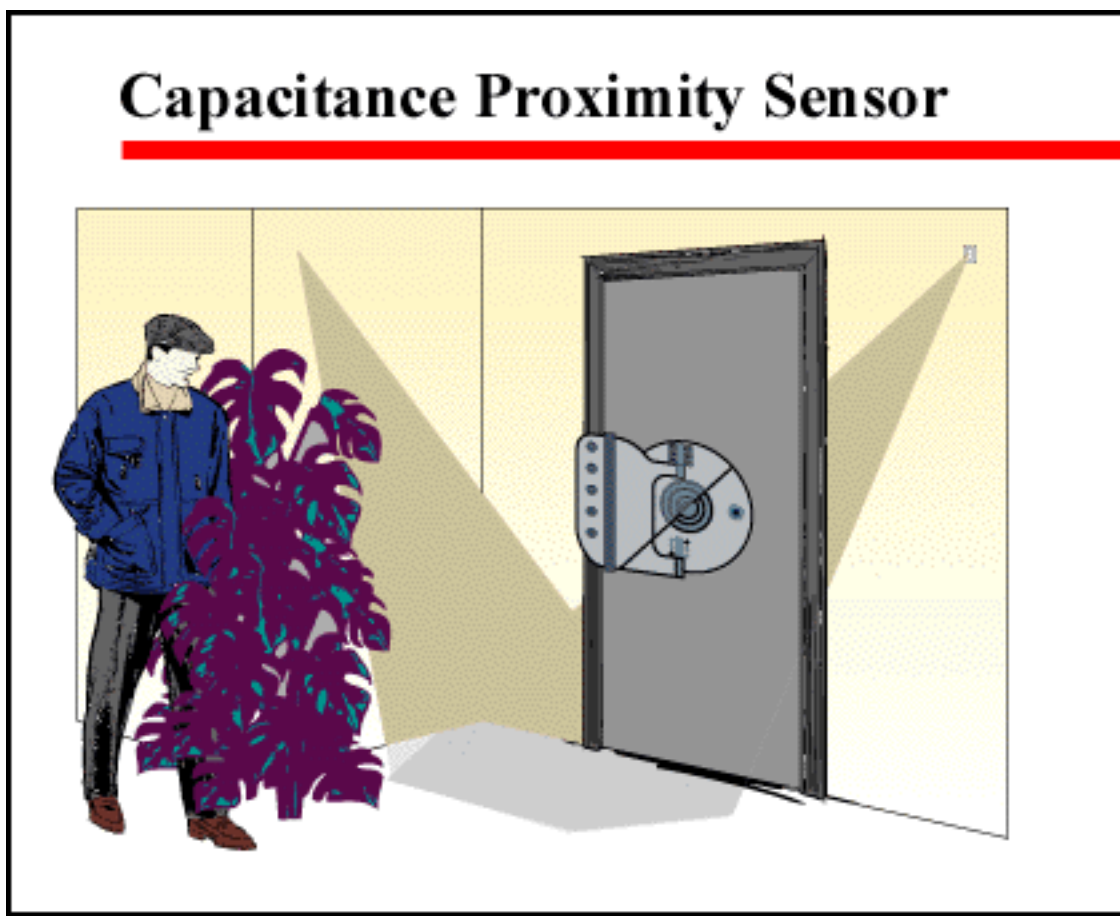
The Capacitance Proximity Sensor uses the electrical phenomenon of "capacitance" to detect persons approaching a protected object. Capacitance (which is different from resistance) is the ability of a "capacitor" to hold an electrical charge. Many elevator buttons use this principle. There are also lamps that glow when their metal base is touched. Both these devices rely on capacitance to function. Interestingly, it is not the "pressure" or touch that causes the switching effect; rather, it is the electrical properties of the human body (in this case) that cause it. Touching the lamp with a plastic pen, for example, would not cause the lamp to light.

A capacitor has three components: two metal plates and some sort of insulating material between them. It is important to recognize that any changes to the electrical properties of the insulating material will change the properties of the capacitor. Note that the insulating material may be air. Further, the human body has electrical properties that, when in contact with or near a capacitor's insulating layer, will affect the device's ability to hold an electrical charge. An explanation of exactly what capacitance does (and how) quickly gets rather technical.

For our purposes, think of a capacitance proximity sensor as an antenna and ground system. Consider a small portable radio. Often a person moving to a particular location around such a radio can improve reception. In a capacitance proximity sensor, these same principles are at work. The intruder's presence near the object interacts with the positive side (antenna) of the capacitor and the

negative side (ground/object to be protected). The sensor's change in flow of electrons causes the system to recognize a deviation in the norm and initiate an alarm.

Capacitance Proximity sensors must be carefully designed and installed to function effectively. Improperly installed devices are susceptible to open circuits or faulty grounding. Either condition can lead to either false alarms or failure to detect intrusions.



Holdup/Panic Protection

Holdup/Panic Protection

Holdup protection includes those devices that help ensure a victim will be able to issue a signal to a detection system that an intrusion is in progress and assistance is required. There are many types of devices available to perform this function:

- ◆ holdup switches
- ◆ Push button
- ◆ Foot Pedal
- ◆ "Money Clips"
- ◆ Wireless personal alarms ("Man down alarms")

Holdup switches are simple mechanical devices which when triggered initiate an alarm at the central station. Generally such switches are placed where they will be unseen by an intruder yet easily accessible to the user who would activate the switch.

A more advanced holdup protection — the personal alarm — is simple a variation on the holdup switch. Whereas a holdup switch is hard-wired into an alarm zone, the personal alarm is a wireless device which may be carried on the user's person or mounted in an unseen but accessible location in the person's workspace (e.g., under

a desk or countertop).

Depending on its technical sophistication, a holdup or panic device may function simply as a switch, or it may have the capability of providing basic user ID information.

A wireless personal alarm system may use either radio waves or ultrasonic sound. Ultrasonic systems claim fewer false alarms and, because sound will not penetrate walls, can report the exact location at which the alarm was triggered.

Holdup/Panic Protection



Signaling Devices

Select the first topic below to begin this lesson:

- [Signaling Devices](#)
- [False Alarms](#)

Signaling Devices

Once an alarm condition is initiated by any of the various detectors or switches within an Intruder Detection System, the system responds in a predefined manner, in accordance with either customer policy or existing codes. This may be through:

- ◆ audio (horn, sirens, and bells)
- ◆ illuminated devices (strobes)
- ◆ central station monitoring
- ◆ local directed monitoring using a remote dialing unit to notify appropriate local authorities off-site

Central stations are sometimes referred to as "monitored" and "non-monitored." Perhaps a clearer description of central stations is "commercial" and "proprietary." Commercial central stations are hired services that provide monitoring of a given facility. Proprietary central stations are often on-site and are staffed by employees of the facility being monitored.

Signaling Devices



False Alarms

We close with a word on false alarms. Increasingly, local authorities are charging companies and other institutions when local police and other emergency responders answer a false alarm. Further, a site known to have frequent false alarms may see a slower response time from emergency personnel. For these reasons, Intrusion Detection systems must be carefully designed and implemented with reliable and appropriate hardware. Following installation, appropriate personnel must be aware of all proper operating and maintenance procedures and function accordingly.