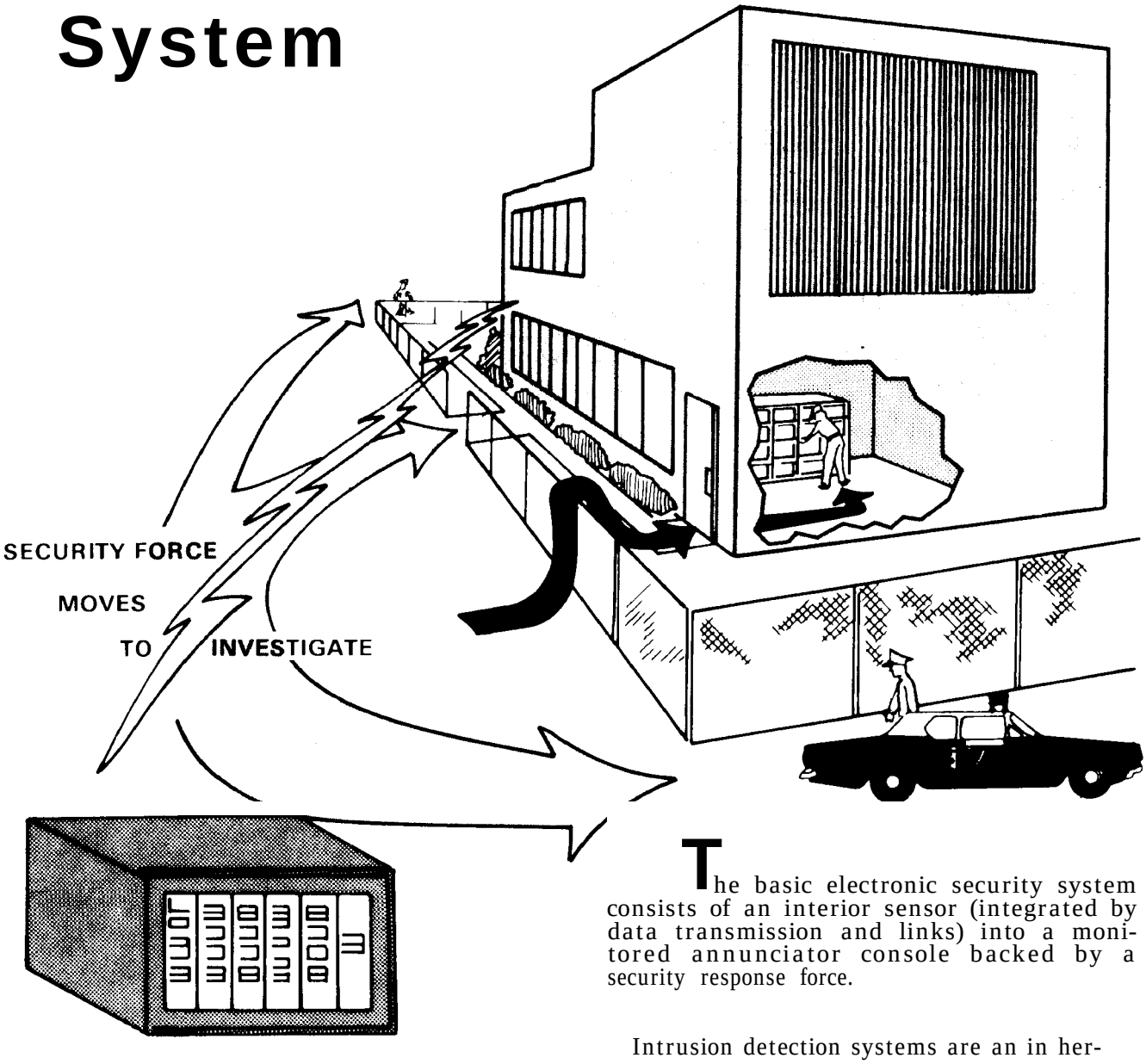
Chapter 7

Intrusion Detection System



The basic electronic security system consists of an interior sensor (integrated by data transmission and links) into a monitored annunciator console backed by a security response force.

Intrusion detection systems are an in herent element of the Army's security in depth ring and play a vital part in the overall

protection of military installations, activities, equipment and materiel assets. These systems detect through sound, vibration, motion, electrostatic and/or light beams. Basically, for an item to be secure, the system must focus upon detecting unauthorized individuals at the entry point (gate, door, fence, etc.), area (building, etc.), and at a specific object (vault, file, safe, etc.).

The basic electronic security consists of an interior sensor (integrated by data transmission links) into a monitored annunciator console backed by a security response force.

These systems can be applied to both tactical and nontactical situations. The systems are designed to detect entry of unauthorized persons into the protected area. Individuals responsible for physical security planning must be aware of the advantages and limitations of these systems so they can be incorporated effectively into the security plan.

There are a variety of commercially manufactured and militarily procured systems designed to detect approach or intrusion. Certain systems are suitable only for outdoor protection, while others are suitable only for indoor uses. All have weak points by which their functioning can be minimized or completely interrupted.

It is important for security managers to remember that any detection system is useless unless it is supported by prompt security force action when the system is activated.

The Basics

Section I

7-1 Definitions

The definitions in appendix S are provided for common understanding of intrusion detection systems and their component parts. The definitions apply to commercially produced and militarily procured systems. You will discover that the terms defined may overlap/impinge on other definitions provided or commonly used in the security/intrusion detection field. Some are frequently used in fields other than security, and may have added or different definitions in use. You should review appendix S prior to reading this chapter.

7-2 Technical Review And Approval

Plans and specifications for installation of intrusion detection systems estimated to cost more than $5,000.00 must be forwarded through command channels to: Chief of Engineers (ATTN: DAEN-MCE-D) for final technical review and approval (AR 190-13).

7-3 Purposes

Intrusion detection alarm systems are used to accomplish one or more of the following:

a. Economize — permit more economical

and efficient use of manpower by requiring smaller mobile responding guard forces instead of larger numbers of personnel for patrols and fixed guard posts.

b. Substitute— use in place of other physical security measures which cannot be used because of safety regulations, operational requirements, appearance, layout, cost, or other reasons.

c. Supplement— provide additional controls at critical points or areas.

7-4 Principles of Operation

a. The following are some basic principles upon which intrusion detection systems operate:

(1) Breaking an electrical circuit.

(2) Interrupting a light beam.

(3) Detecting sound.

(4) Detecting vibration.

(5) Detecting motion.

(6) Detecting a change in capacitance due to penetration of an electrostatic field.

b. Each principle is discussed separately in paragraphs 7-7 through 7-12, including advantages and disadvantages.

7-5 Necessity and Feasibility

The following are factors that need to be considered to determine the necessity and feasibility of installing an intrusion detection system.

a. Mission of the installation or facility.

b. Criticality of the installation or facility.

c. Vulnerability of the installation or facility.

d. Accessibility to intruders.

e. Location of installation or facility (geographical) and locations of areas to be protected inside the installation.

f. Construction of building.

g. Hours of operation.

h. Availability of other forms of protection.

i. Initial and recurring cost of the system as compared to cost, in money or security, of possible loss of materials or information.

j. Design and **salvage value** of the system.

k. Response time by the security force.

l. Saving in manpower and money over a period of time.

m. Intruder time requirement.

7-6 Selection

Each type of intrusion detection system is intended to meet a specific type of problem.

a. Factors to be considered in selecting the appropriate components/system include but are not limited to the following:

(1) Location and response time capability of security personnel.

(2) Value of facility, material, or the sensitivity of classified defense material to be protected.

(3) Area environment, to include building construction, sound levels inside and outside, climate, etc.

(4) Radio and electrical interference.

(5) Operational hours of the installation or facility.

(6) Specific target to be protected.

(7) Availability of security personnel.

b. A consideration of these factors readily indicates the advisability of obtaining technical data to assist in making a wise selection. Often more than one type of sensor, or even system is necessary to give adequate protection for an area or structure.

Types of Systems

Section II

7-7 Breaking An Electrical Circuit

a. Possible points of entry into buildings or enclosures can be wired by using electrically sensitized strips of metallic foil or wire. Any action that breaks the foil or wire breaks the electrical circuit and activates an alarm. Metallic foil is frequently used on glass surfaces. Doors and windows may be equipped with magnetic contact switches which sound an alarm when the door or window is opened. Metallic wire running through concealed wooden dowels or between panels or walls, doors, and ceilings may be used.

b. Characteristics:

(1) Advantages. Consistently provides the most trouble-free service; causes few, if any, nuisance alarms. Adequate in low-risk applications.

(2) Disadvantages:

(a) Costly to install where there are many entry points to the protected area.
(b) Easily compromised when improperly applied; unprotected soft walls or ceilings may be penetrated without disturbing the alarm system; it may also be defeated by bridging the circuits.
(c) Has little salvage value–not recoverable.
(d) Will not detect "stay-behinds."

7-8 Interrupting a Light Beam

a. The photoelectric (electric eye) type of intrusion detection derives its name from the use of a light-sensitive cell and a projected-light source.

(1) A light beam is transmitted at a frequency of several thousand vibrations per second. An infrared filter over the light source makes the beam invisible to intruders.

(2) Alight beam with a different frequency (such as a flashlight) cannot be substituted for this beam. The beam is projected from a hidden source and maybe crisscrossed in a protected area by means of hidden mirrors until it contacts a light-sensitive cell.

(3) This device is connected by wires to a control station. When an intruder crosses the beam, he breaks contact with the photoelectric cell, which activates an alarm.

(4) A projected beam of invisible light can be effective for approximately 500 feet indoors and will cover an area up to 1,000 feet outdoors. The effectiveness of the

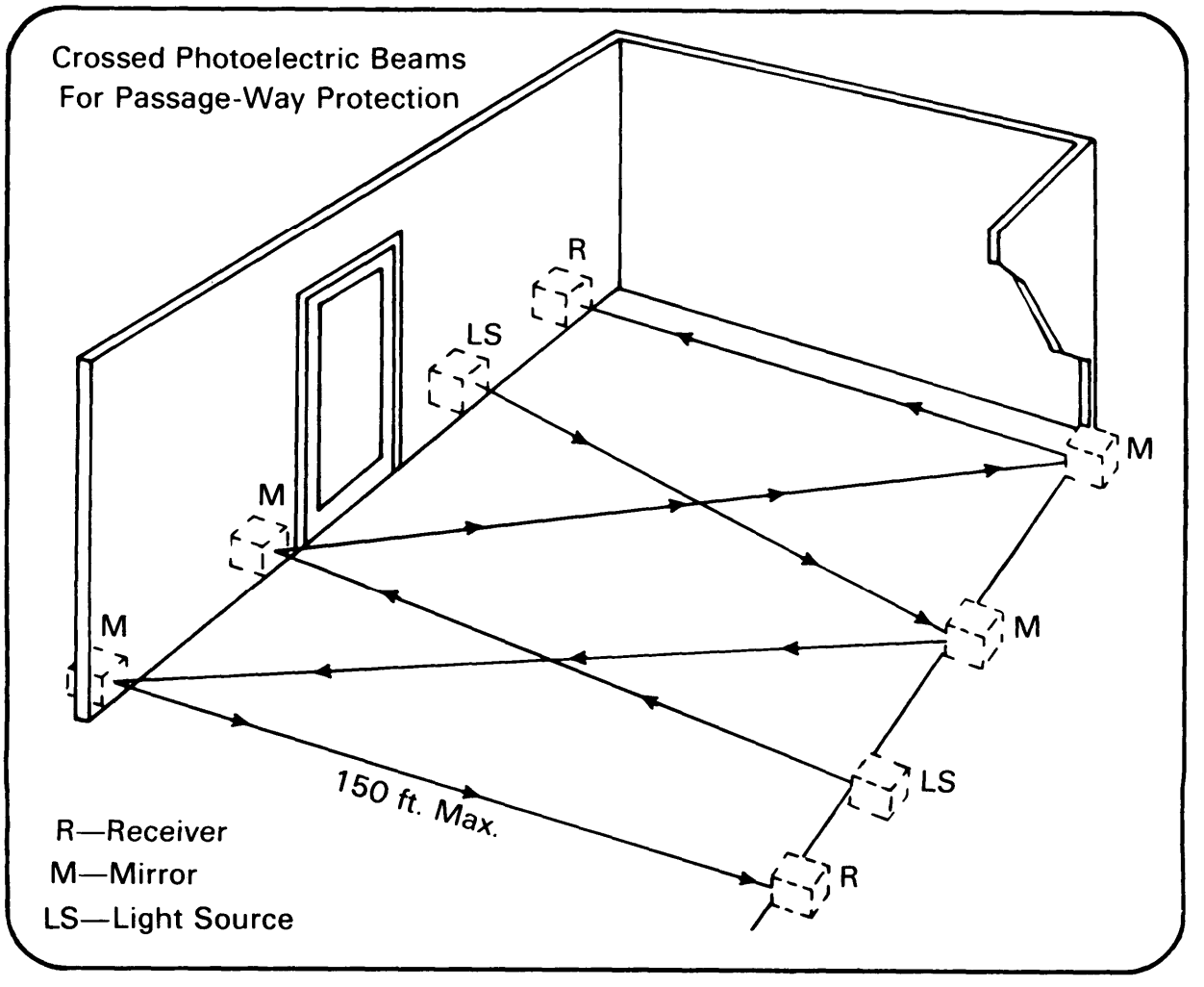


Figure 25—Sample of photoelectric intrusion detection device.

beam decreases from 10 to 30 percent for each mirror used. Figure 25 shows a typical light beam setup.

b. Characteristics.

(1) Advantages.

(a) When properly employed, affords effective, reliable notice of intrusion.
(b) Useful in open portals or driveways where obstructions cannot be used.
(c) Detects "stay-behinds."
(d) Has a high salvage value; almost all equipment is recoverable.
(e) May be used to actuate other security devices, such as cameras.
(f) May detect fires through smoke interruption of the beam.

(2) Disadvantages

(a) Employment is limited to those locations where it is not possible to bypass the beam by crawling under or climbing over it.
(b) Requires some type of permanent installation.

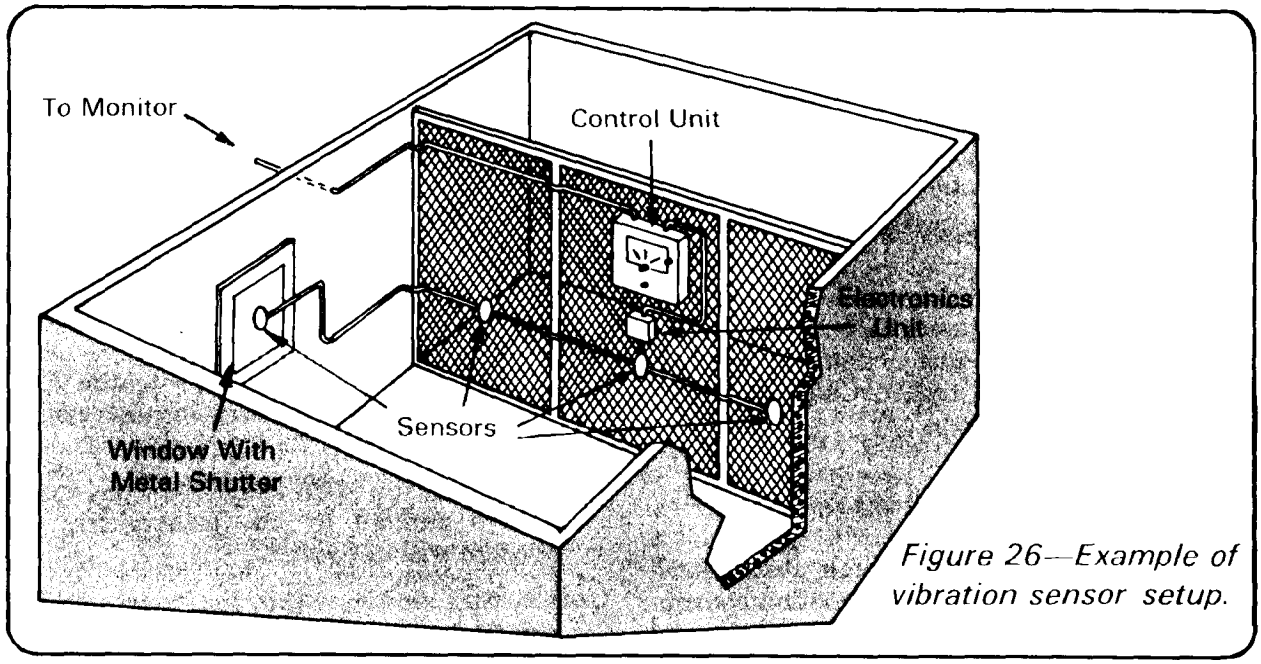


Figure 26—Example of vibration sensor setup.

(c) Fog, smoke, dust, and rain in sufficient density will cause interruption of the light beam.

(d) Requires frequent inspections of light producing components to detect deterioration.

(e) Requires keeping the ground beneath the light beam free of tall grass, weeds, drifting snow, and sand.

7-9 Detecting Sound

a. This type of intrusion detection system can be effectively used to safeguard enclosed areas, vaults, warehouses, and similar enclosures. Supersensitive microphone speaker sensors are installed on walls, ceilings, and floors of the protected area. Any sound caused by attempted forced entry is detected by the sensor. Sensitivity can be adjusted.

b. Characteristics.

(1) Advantages.

(a) Economical and easily installed.

(b) High salvage value.

(c) Microphone speakers may be used in more expensive sensors to monitor sounds coming from the protected area.

(2) Disadvantages. Can be used only in enclosed areas where a minimum of extraneous sound exists; not satisfactory where high noise levels are encountered, especially in proximity to aircraft and railroad traffic. Cannot be used effectively outdoors. Should not be used in areas where sensitive classified discussions occur unless the system is designed to prevent its use as a clandestine listening device.

7-10 Detecting Vibration

This type of intrusion detection system can be effectively used to safeguard enclosed areas in sound detection systems.

a. Vibration-sensitive sensors are attached to walls, ceilings, and floors of the protected area. Any vibration caused by attempted forced entry is detected by the sensors. Sensitivity can be adjusted. (See figure 26 for a sample setup).

b. Characteristics:

(1) Advantages.

(a) Economical and easily installed.
(b) High salvage value.
(c) Flexible application.

(2) Disadvantages. Can be used only in areas where a minimum of vibration exists; not satisfactory where high vibrations are encountered, especially in proximity to heavy construction, railroad, or automotive/truck traffic. Cannot be used effectively outdoors.

7-11 Detecting Motion

a. Intrusion detection systems using ultrasonic or microwave motion sensors can be very effective for the protection of interior areas. Such systems flood the protected area with acoustic or microwave energy and detect the Doppler shift in transmitted and received frequencies when motion occurs within the area.

b. Ultrasonic systems consist of transceivers (single unit containing a transmitter and receiver or separate transmitters and receivers), and electronic unit (amplifier) and a control unit.

(1) The transmitter generates a pattern of acoustic energy which fills the enclosed area.

(2) The receiver, connected to the electronic unit, picks up the standing sound patterns.

(3) If they are of the same frequency as the waves emitted by the transmitter, the system will not alarm.

(4) Any motion within the protected area sends back a reflected wave differing in frequency from the original transmission. The change in frequency is detected, amplified, and the alarm signal activated (illustrated example in figure 27).

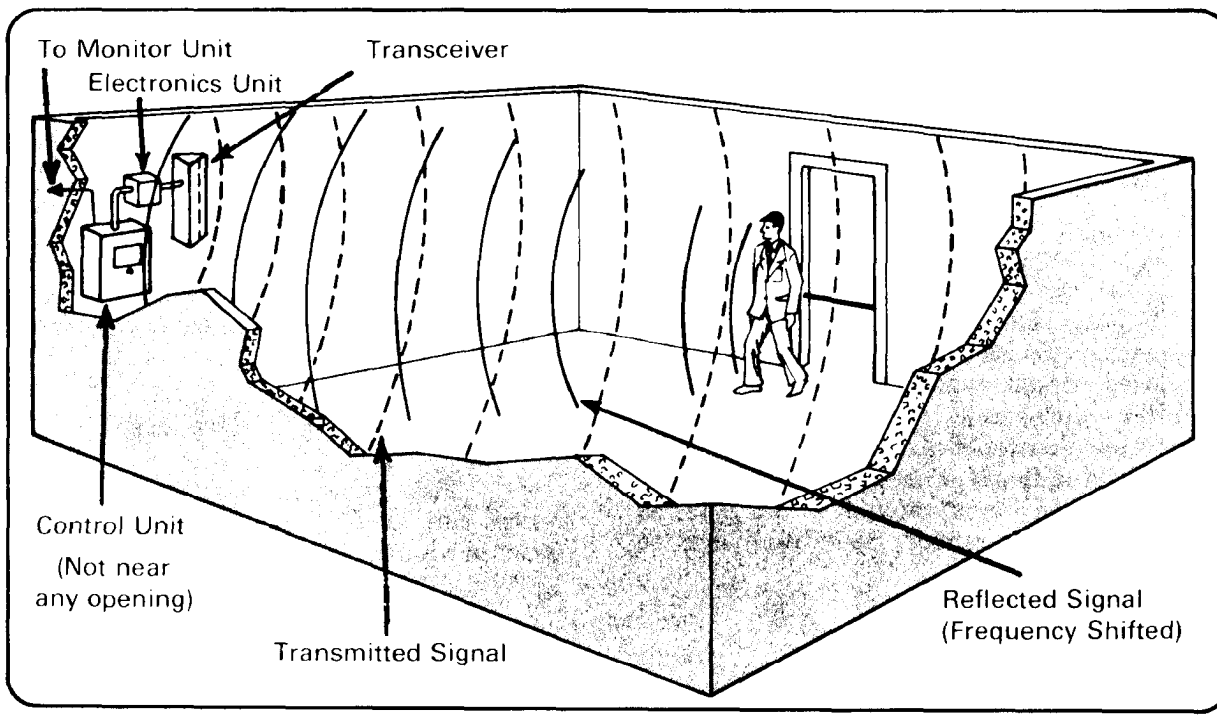


Figure 27—How an ultrasonic motion sensor works.

(5) Multiple transceivers or a transmitter and multiple receivers may be operated from the same control unit for more effective coverage of large or broken areas. This system can only be used indoors.

(6) Advantages.

(a) Provide effective security protection against intruders concealed within the premises.
(b) High salvage value.
(c) Protective field is not visible, therefore, it is difficult to detect the presence of, or to compromise the system.

(7) Disadvantages.

(a) May require reduced sensitivity to overcome possible disturbance factors in the enclosed area (such as telephones, machines, clocks, etc.).
(b) Can be set off by loud external sounds.

c. Microwave systems closely parallel the operation of ultrasonic systems. A pattern of radio waves is transmitted and partially reflected back to an antenna. If all objects within the range of the radio waves are stationary, the reflected waves return at the same frequency. If they strike a moving object, they return at a different frequency. The difference in the transmitted and received frequency is detected, thus initiating an alarm signal.

(1) Advantages.

(a) Good coverage is provided if antennas are properly placed.
(b) Not affected by air currents, noise, or sound.
(c) High salvage value.

(2) Disadvantages.

(a) Coverage is not easily confined to desired security area. Penetrates thin wooden partitions and windows and therefore may be accidentally activated by persons or vehicles outside the protected area.
(b) Fluorescent light bulbs will activate the sensor.

7-12 Detecting Capacitance Change In An Electrostatic Field

a. The capacitance or electrostatic intrusion detection system can be installed on a safe, wall, and/or openings therein in an effort to establish an electrostatic field around the object to be protected. This field is tuned by a balance between the electric capacitance and the electric inductance. The body capacitance of any intruder who enters the field unbalances the electrostatic energy of the field. This unbalancing activates the alarm system. (See figure 28, next page.)

b. Characteristics:

(1) Advantages.

(a) Extremely flexible type of system; it may be used to protect safes, file cabinets, windows, doors, partitions; in fact any unguarded metallic object within maximum tuning range may be protected.
(b) Simple to install and operate.
(c) Provides an invisible protective field, making it difficult for an intruder to determine when system has been set off.
(d) High salvage value-may be easily dismantled and reinstalled.
(e) Compact equipment size.
(f) High grade of protection.

(2) Disadvantages.

(a) Can be applied only to ungrounded equipment.
(b) Housekeeping of protected area on object must be carefully watched.
(c) Accidental alarms can occur if protected area or object is carelessly approached, such as by porters or cleaners at night.

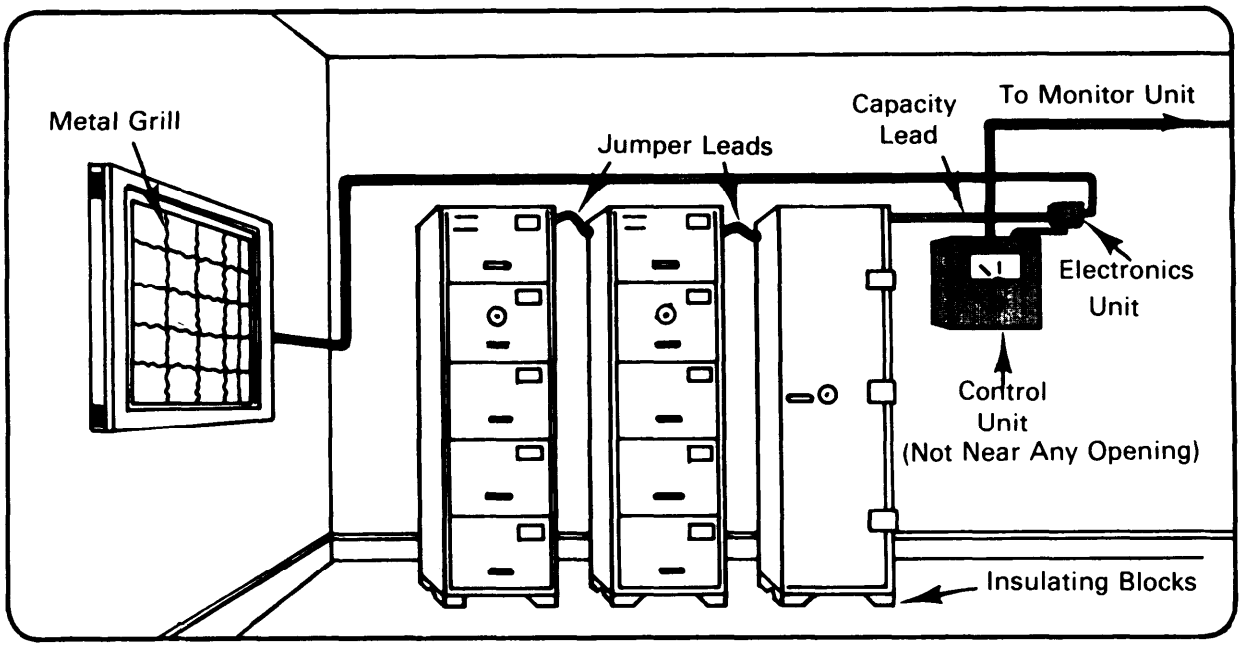


Figure 28—Example of capacitance proximity sensor setup.

7-13 Penetration Sensors

Modern penetration alarm sensors can be used at any installation or activity for additional security protection. Their versatility lends to use on windows, interior or exterior doors, ceilings, walls and other potential entry areas.

a. Exterior doors. To guard against unauthorized entry, the door can be equipped with one or more balanced magnetic switches as shown in figure 29. The surface of an interior door or wall can be covered with a grid wire sensor (figure 30) or any type system using the principle of breaking an electrical circuit, as discussed in paragraph 7-7 of this chapter.

b. Interior doors. These sensors are subject to the same considerations that govern the choice of systems for exterior doors.

c. Solid walls, floors and ceilings. To monitor attempts to penetrate solid walls, floors, and ceilings, the interior surface may be covered with a grid wire sensor, or the room equipped with a passive ultrasonic sensor (see figure 31, page 102). Sound detection systems (par. 7-9) and vibration detection systems (par. 7-10) may also be used to detect penetration through such areas.

d. Open walls and ceilings. Wire cage walls and ceilings present distinct problems. To protect this type of construction, certain modifications are necessary. The wall and ceiling may be enclosed with building material on the outside of the cage. This permits use of passive ultrasonic or grid wire sensors.

e. Windows. Wherever possible, windows should be eliminated. Where windows are necessary, consider the use of interior metal shutters which can be closed and locked. This allows use of passive ultrasonic sensors. If the character of the room does not allow the use of a passive ultrasonic sensor, the vibration sensor (par. 7-10) or capacitance proximity sensor (par. 7-12) can be used instead. Any system using the principle of breaking an electrical circuit can also be considered.

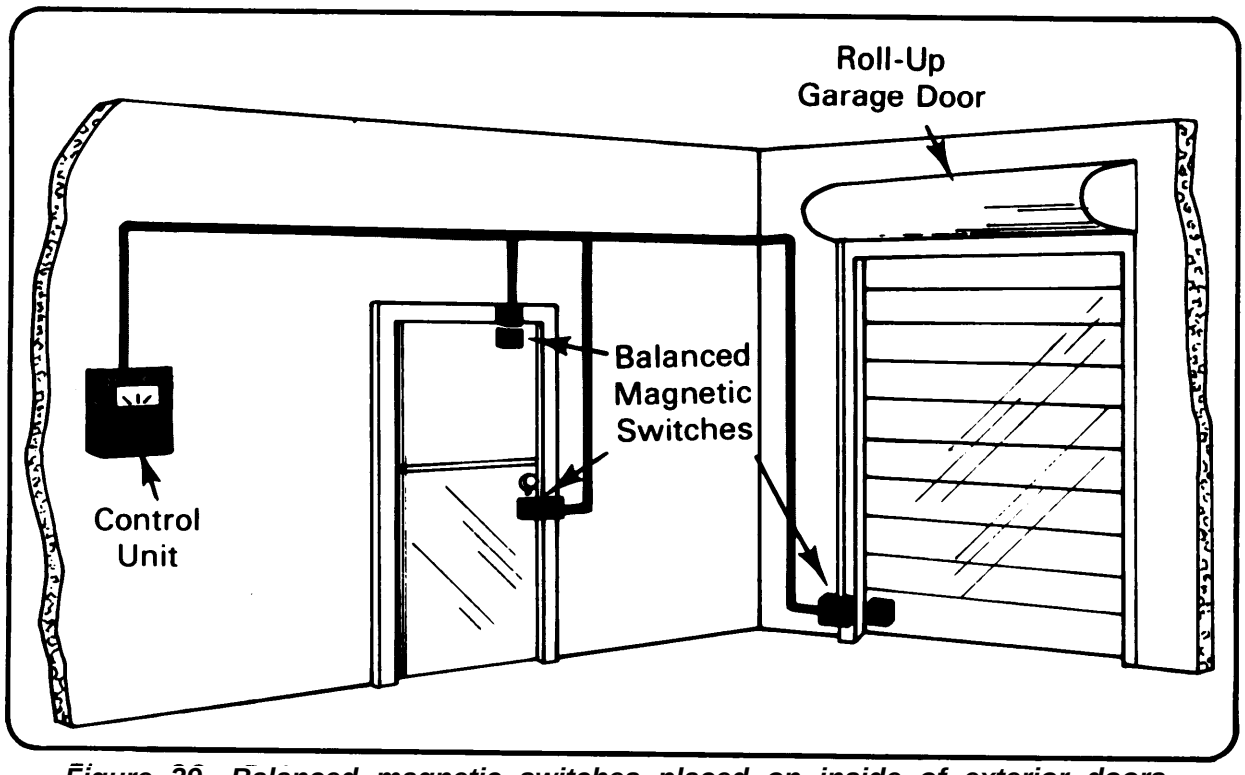


Figure 29—Balanced magnetic switches placed on inside of exterior doors.

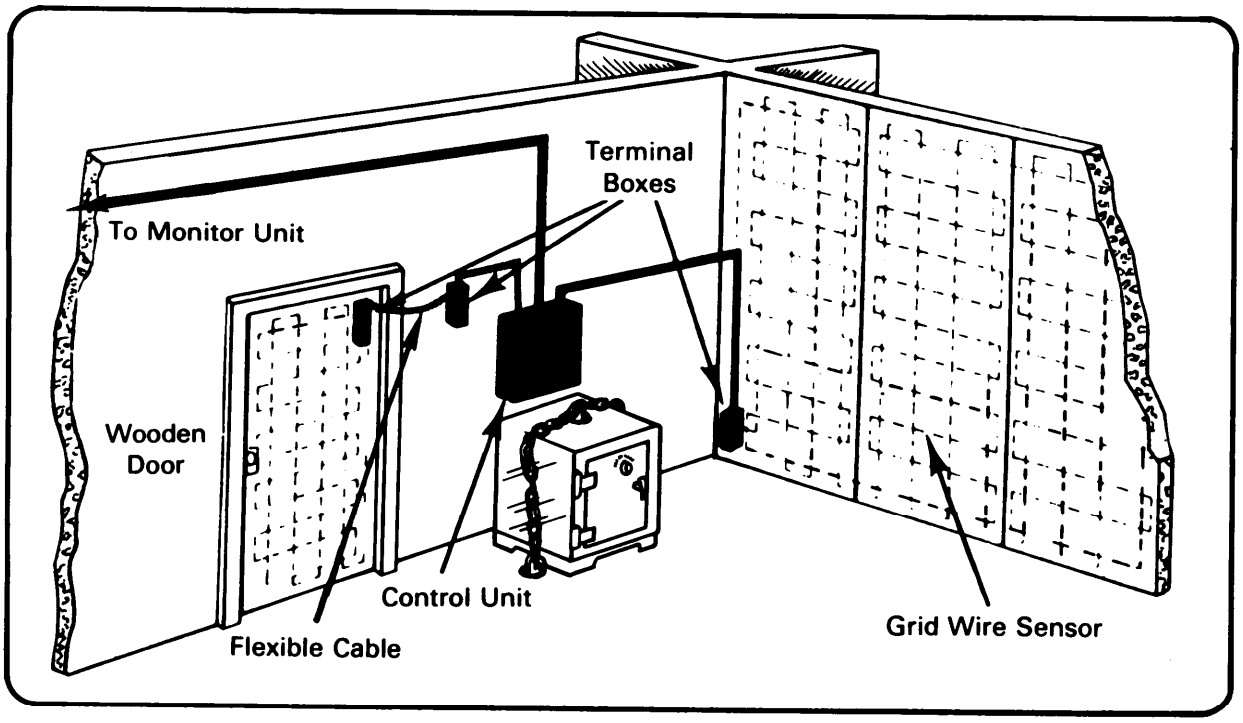


Figure 30—Grid wire sensors used on interior surfaces.

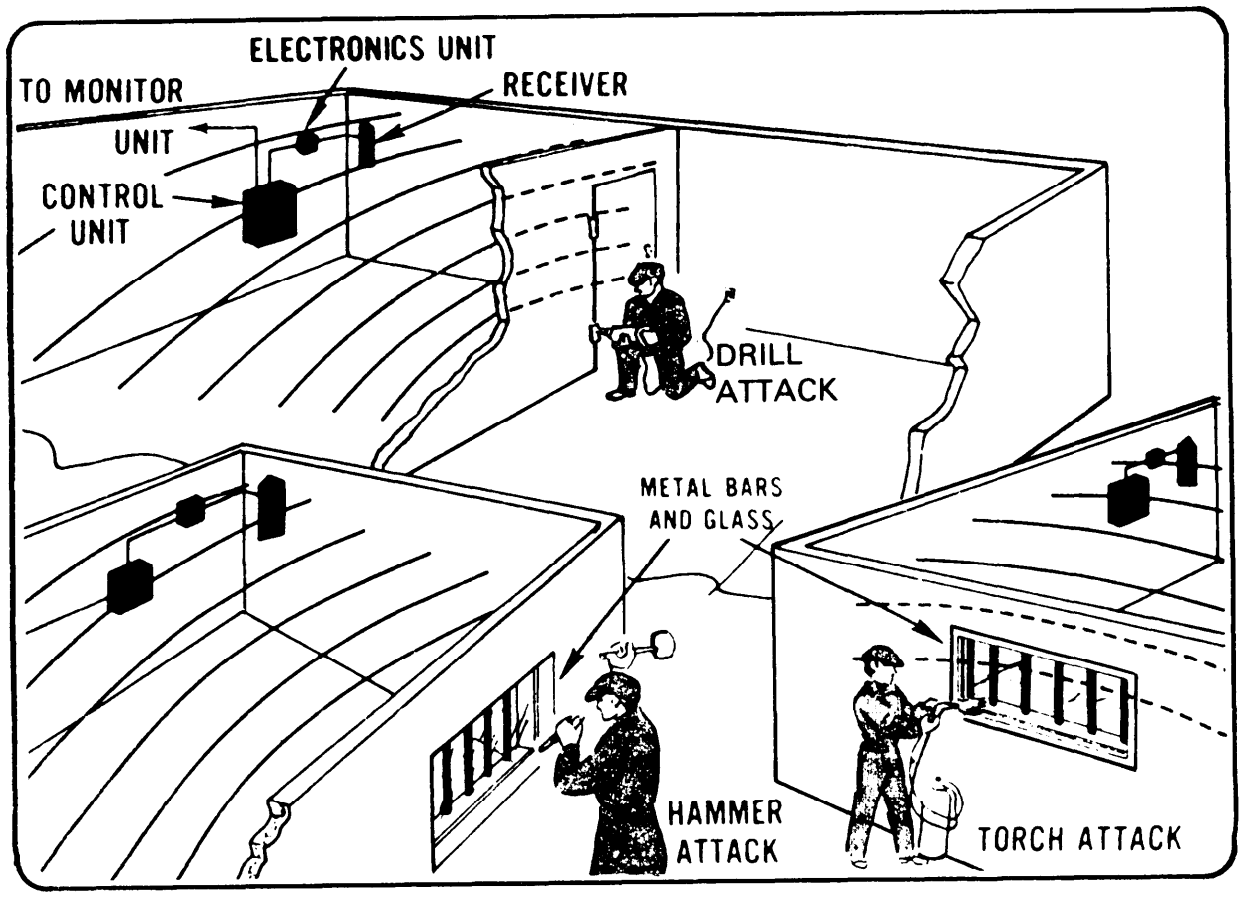


Figure 31—Examples of passive ultrasonic sensor effectiveness.

f. Ventilation openings. These are any openings in the ceiling, walls, or doors to allow the free passage of air. They are generally covered with steel bars, mesh, or louvered barriers. For maximum protection, you should consider eliminating ventilators. Where it is not possible to seal ventilators, consider the use of locked metal shutters. Intrusion through the ventilators then can be detected with the passive ultrasonic sensor or the vibration sensor. Where the ventilators are required to be open all the time, a metal grill can be placed over the inside of the ventilator opening and the capacitance proximity sensor can be used.

g. Construction openings. These are unsecured openings from incomplete construction. The openings can be covered with a grid wire sensor installed on plywood. Where the opening is required to stay open, a capacitance proximity sensor can be used on the inside of the opening.

h. Air conditioners. To monitor for intrusion through an air conditioner aperture, the capacitance proximity sensor can be used on a metal grill extending into the room in front of the unit.

7-14 Motion Sensor

To detect the motion of an intruder inside a protected area, an ultrasonic motion sensor (par. 7-11) can be used, provided there

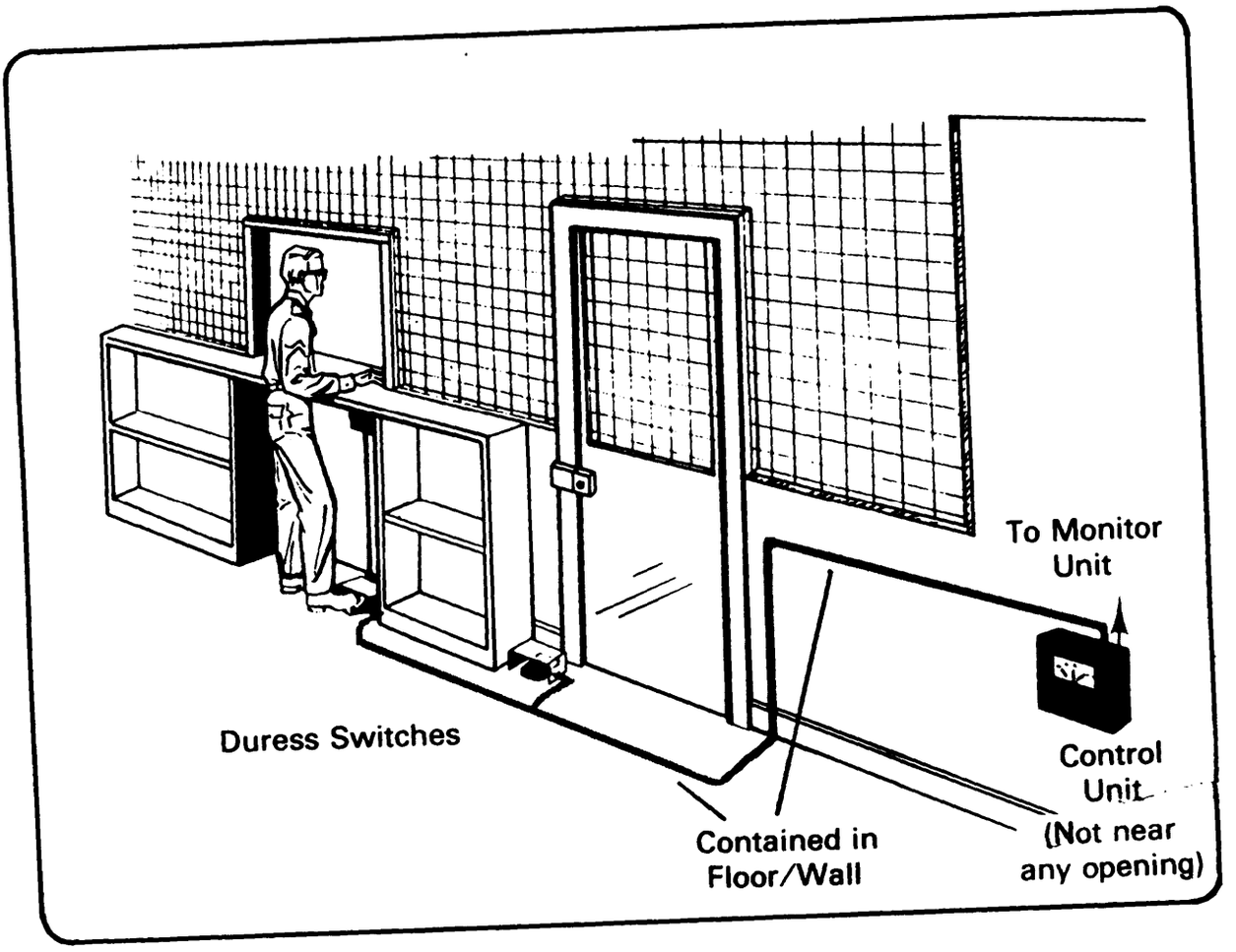


Figure 32—Examples of fixed duress sensor placement.

is a minimal flow of air from heating units, air conditioned, cracks in the protected area, or any other possible source of air turbulence, as this may reduce the effectiveness of the sensor or cause nuisance alarms. A microwave system (par. 7-11) may also be used to protect an enclosed area.

7-15 Duress Sensor Considerations

Fixed. This sensor is used to call for assistance of other personnel. It consists of a foot- or hand-operated switch located in a position most likely to be occupied by personnel working in the protected area (figure 32).

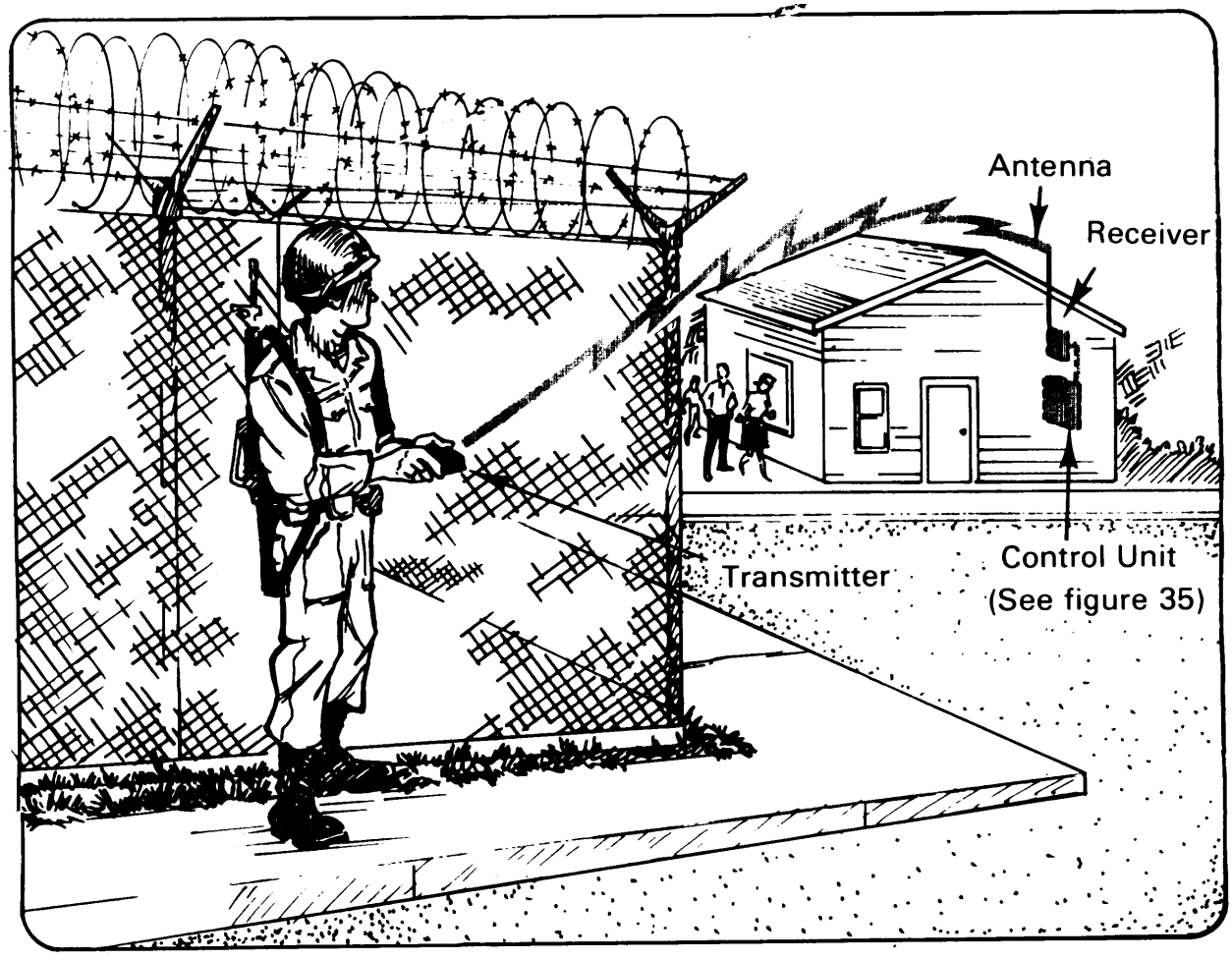


Figure 33—Examp/e of portable duress sensor use.

Portable. An alternate to the fixed duress sensor, the portable duress sensor is a UHF transmitter which can send an alarm to a receiver located at the control unit. The effective range will be restricted depending upon inside or outside use (figure 33).

7-16 Point Sensor Considerations

a. Storage cabinets and safes. To detect movement near to or contact with any part of a storage cabinet or safe, the capacitance proximity sensor can be used.

b. Weapons. To detect removal of weapons from a standard weapons rack, a magnetic weapon sensor (figure 34) can be used. (Also see Section IV, The Systems, for security of arms and ammunition.)

7-17 Control Unit

One control unit (figure 35) is required in each secure area to receive signals from the sensors and to transmit signals to the monitor unit and local audible alarm.

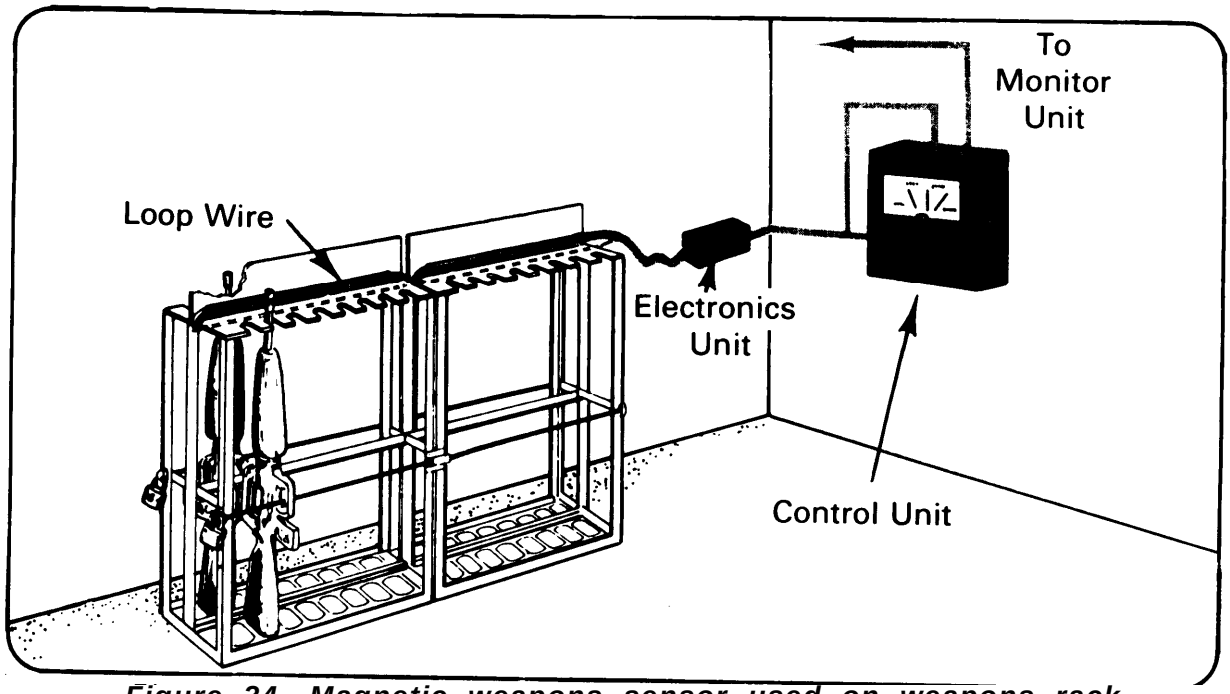


Figure 34—Magnetic weapons sensor used on weapons rack.

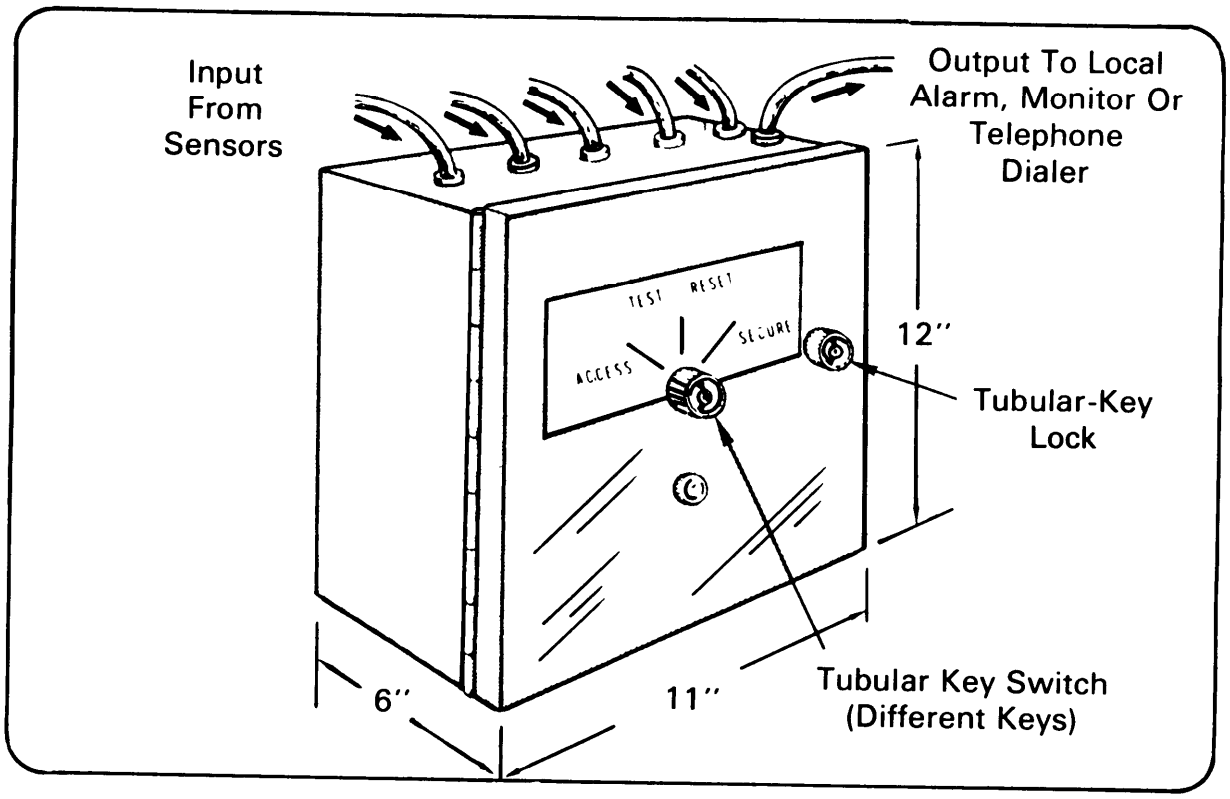


Figure 35—Sample details of control unit.

153-846 0 - 94 - 7

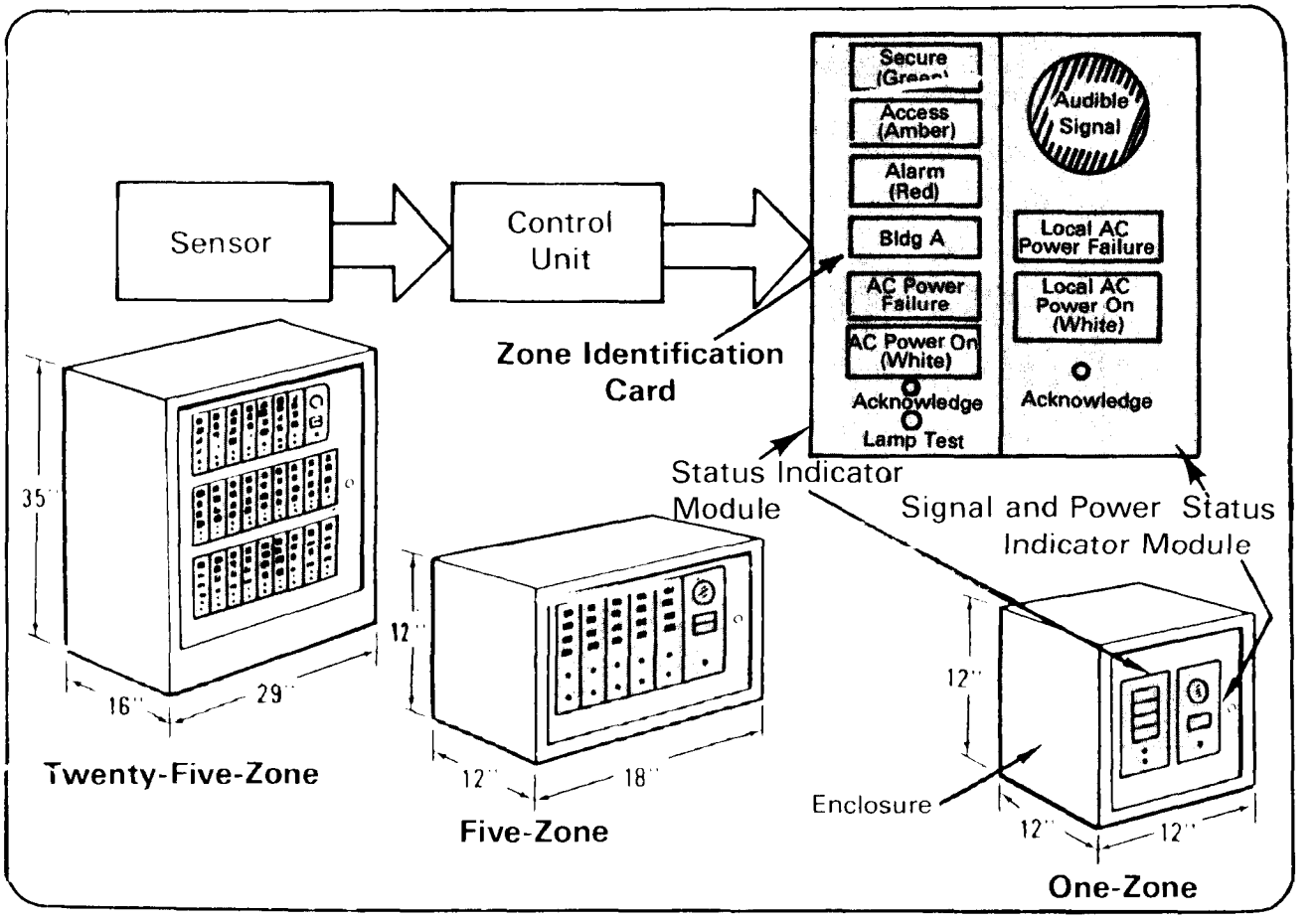


Figure 36—Monitor unit examples.

7-18 Monitor Unit

Each control unit must report to a separate monitor unit status indicator module (see figure 36). Each monitor unit must contain one signal and power status indica - tor module.

7-19 Local Audible Alarm

A local audible alarm (see figure 37) may be installed outside the protected area. This alarm serves two purposes. Initially, it may scare the intruder away. Secondly, it alerts local guard and police forces in the area. This alarm has limited value for areas where there are no response personnel. A local audible alarm should not be used without a remote monitor unit.

7-20 Telephone Dialer

A telephone dialer (figure 38) maybe employed where it is not possible to install a monitor unit. This device telephones an alarm to a number of preselected phones. Telephone dialers are recommended only for low-security application. Telephone dialer lines may be tied up by calling the number which receives the alarm notification message. They are subject to other tampering and interruption and do not alarm when they are out of order, cut, or grounded.

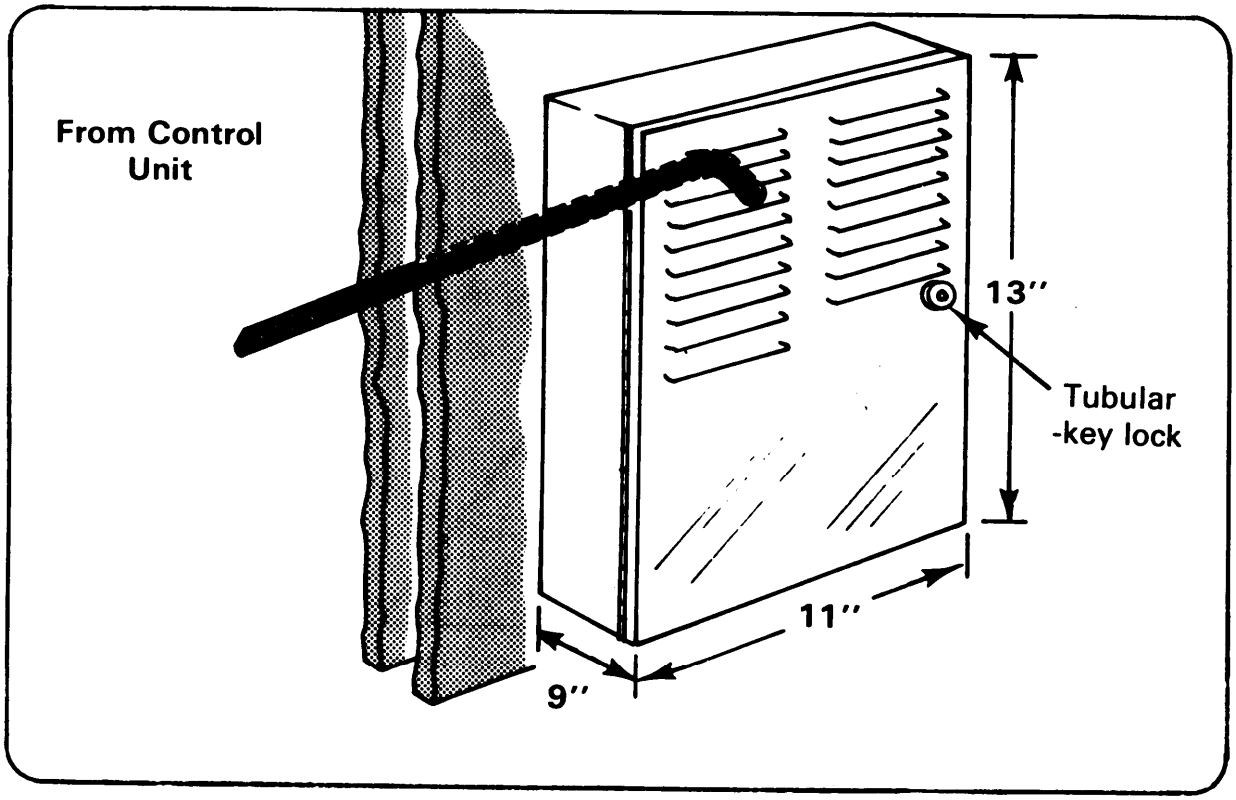


Figure 37—Example of local audible alarm.

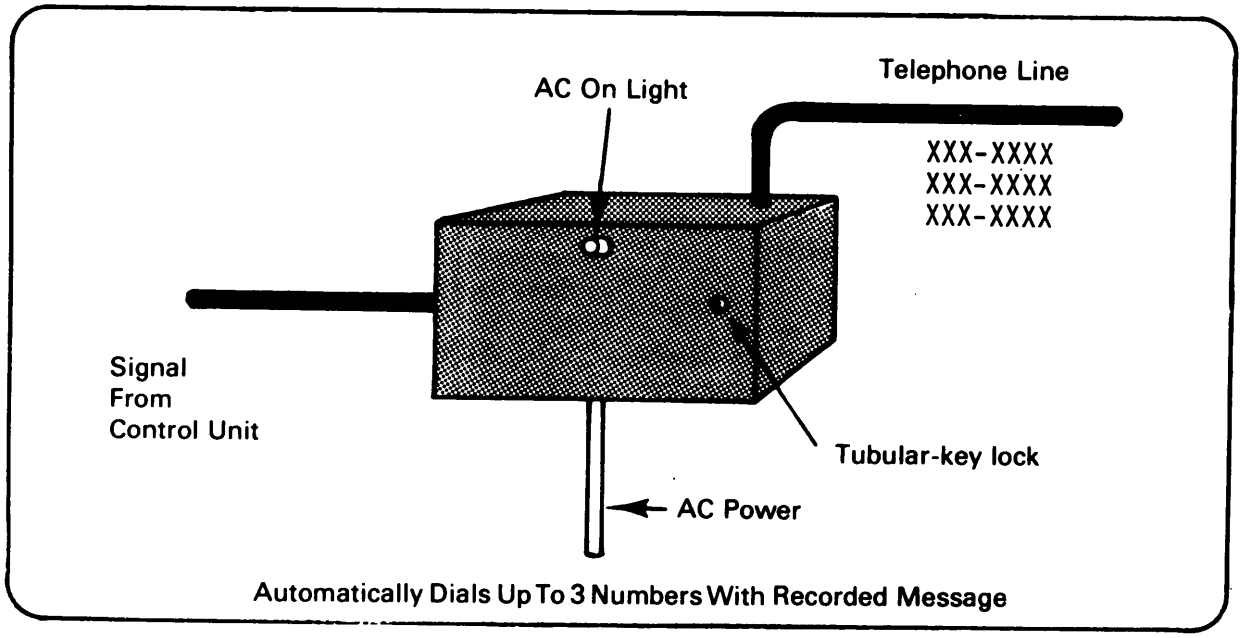


Figure 38—Telephone dialer example.

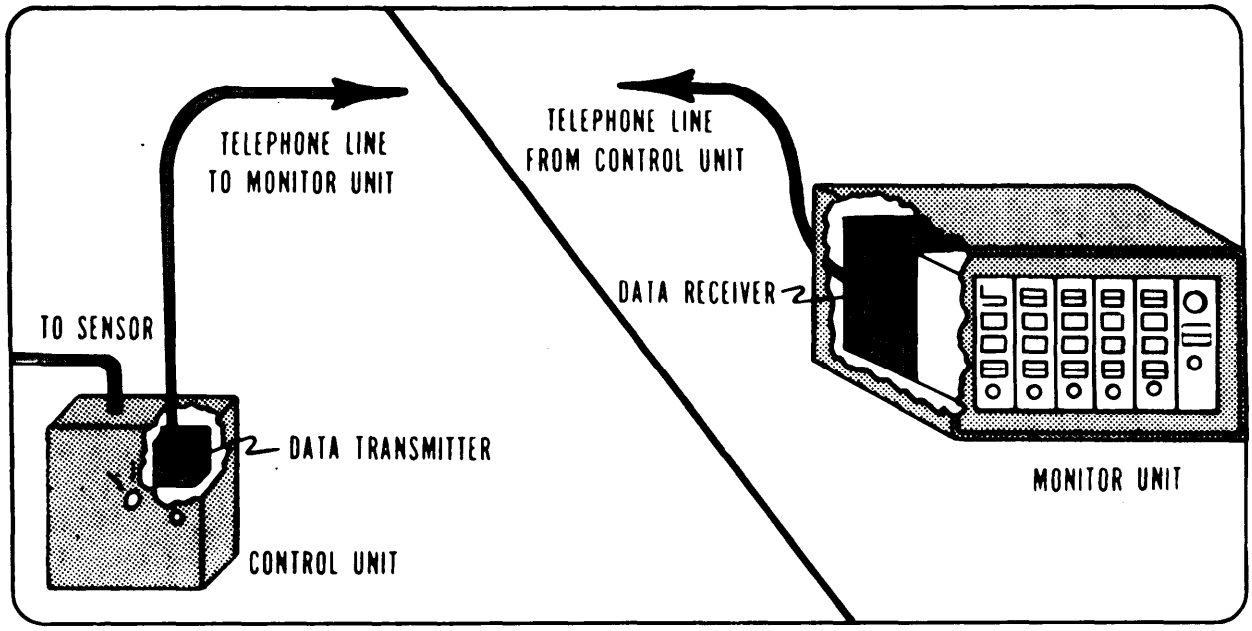


Figure 39—Example of data transmission system.

7-21 Data Transmission System (Type I

The data transmission system (figure 39) is used wherever there are segments of the signal transmission line accessible to tampering, or wherever the signal is transmitted over commercial conductors. One data transmission system is required for each security zone covered by a control unit connected to such a line.

7-22 Intrusion Detection Alarm Report

Alarm and communications detection systems are closely allied in any comprehensive protection system. Telephone and radio communications are so common in everyday usage that their adaptation to a protective system poses few new problems. An alarm detection system is simply a manual or automatic means of communicating a warning of potential or present danger. Types of alarm detection systems include the following:

a. Local alarm system. In a local alarm system the protective circuits or devices actuate a visual or audible signal in the immediate vicinity of the object of protection. Response is by the local security force or other personnel within sight or hearing. The light or sound device should be displayed on the exterior of the building, and should be fully protected against weather or willful tampering. It should be connected to the control element by a tamperproof cable, and should be visible or audible for a distance of at least 400 feet. This system can also be used in conjunction with a proprietary system, as described in paragraph 7-22d.

b. Auxiliary system. An auxiliary system is one in which the installation-owned system is a direct extension of the civil police and/or fire alarm systems. This is the least effective system and because of dual responsibility for maintenance is not favorably considered by many protective organizations.

c. Central station system. A commercial agency may contract to provide electric

protective services to its clients by use of a central station system. The agency designs, installs, maintains, and operates underwriter-approved systems to safeguard against fire, theft, and intrusion; and monitors industrial processes. Alarms are transmitted to a central station outside the installation from which appropriate action is taken such as notifying local police or fire departments.

Note. Direct connected systems or central station systems may be appropriate for armories/buildings used by the Army National Guard, Army Reserve, and/or Army ROTC. The main consideration is lack of an organic or supporting response force.

d. Proprietary System. A proprietary system is similar to the central station system except that it is owned by, and located on, the installation. Control and receiving equip ment is located in the installation security or fire department headquarters. Response to an alarm is by the installation's own security or firefighting personnel. In addition, this type of system may be connected with the civil police and fire departments, and with a commercial central station.

7-23 Signal Transmission Lines

An intrusion detection system is no better than the security of the conductors that transmit the alarm signal to the monitor unit. These conductors must be sensitive enough to cause an alarm in the event of tampering.

a. An intrusion detection system may be defeated regardless of the effectiveness of its sensor if the signal transmission line is not functioning properly. Conductors may be made ineffective by an intruder who has sufficient knowledge of electricity and the necessary equipment to adjust the resistance in the signal transmission lines.

b. Signal transmission lines maybe supervised in a variety of ways, according to location of the lines and the security required.

(1) The simplest means of line supervision is to monitor whether an electrical circuit has been broken, grounded, or shorted.

(2) The most common means is to monitor whether a predetermined variation to an electrical current has occurred. For example, an alarm light might be created if a 30-milliamp current has been increased or decreased five percent.

(3) A more sophisticated means is to monitor two or more features of a complex signal, such as current and frequency. If the signal is changed on a random basis, the likelihood of the signal being recorded and replayed successfully is very remote.

(4) Another approach is to monitor a digital- or tone-type signal transmitted through a telephone system. An investigation and reply scheme is ordinarily employed. Since an electrical current is not being monitored in this case, the distance limitation (a few miles) of the other types does not apply.

c. The need for constant electronic or other type surveillance of signal transmission lines must be emphasized to insure awareness of security personnel that this is normally the weakest link in the system. Emphasis must also be placed on the necessity to maintain records of both nuisance alarms and scheduled/unscheduled maintenance to insure proper operation of the system at all times.

d. Signal transmission lines can be secured by locating them on high overhead poles, burying them, leading into buildings as high as possible, locking terminal cabinets, and comparable measures.

Protective communication systems vary in size and type with the importance, vulnerability, size, location, radio receptivity, and other factors affecting a specific installation, and must be largely subject to local determination.

7-24 Primary Communication Systems

In many situations, the regular communication system of an installation is not adequate for protective security purposes. It is desirable for security forces to have their own communication system with direct lines outside and an auxiliary power supply. Although principal dependence is on the telephone and the teletype, interior and exterior radio communications play an important part in the protective net of large installations.

One or more of the following means of communication should be included in the protective system.

a. Facilities for local exchange and commercial telephone service.

b. Intraplant, interplant, and interoffice telephone systems using either Government-owned or rented circuits and equipment; but not interconnected with facilities for commercial exchange or toll telephone service.

c. Radiotelephone and\or radiotelegraph facilities for either point-to-point or mobile service.

d. Telegraph and teletype facilities for either commercial service or private line operation.

e. Hand-carried portable radios and\or receivers, with transmitters stationed strategically throughout the installation.

f. A security supervisory system consists of key-operated electric call boxes located strategically throughout an installation. By inserting the key in the call box, security personnel can make routine tour reports or summon emergency assistance. Tampering with the transmitting key or the call box automatically locks the latter, causing a failure of the signal. This signal failure would prevent future routine/scheduled calls, a cause sufficient for immediate investigation.

7-25 Alternate Communication Systems

Alternate communication systems must be provided for use in emergencies. The flood of inquiries that follow emergency conditions added to the normal flow of messages may, overload the existing system at the very time that sure and rapid communication is vital. The most efficient emergency reporting system consists of direct connection to the security or communications center from telephones strategically placed throughout the installation. The use of these telephones should be restricted to emergencies and security force reporting only. The wires of alternate communication systems should be separated from other communication lines,

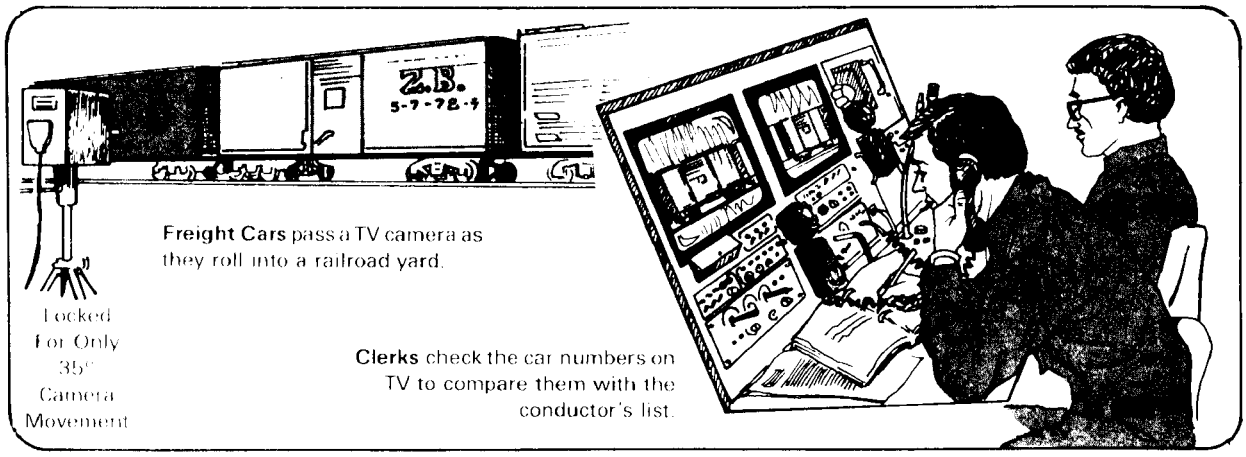


Figure* 40—TV *monitoring of cargo movement.

and should be in underground conduits. For emergency communication with agencies outside the installation, leased wires or a radio adjustable to civil police and fire department frequencies should be available.

7-26 Wiring, Inspection, And Testing

a. Whenever practicable the signal transmission lines of communications systems should be on separate poles or in separate conduits from the installation com - munication and lighting system.

b. Tamper resistant. wire and cable. with she ath of foil that transmits a signal when penetrated or cut, provides added protection.

c. All communication circuits should be tested at least, onto during each tour of duty, preferably when the new shift assumes duty. At small installations that do not employ security forces, a test should be made immediately before closing for the night. Some commerically manufactured systems have self-testing features which should be checked periodically by the security patrol or operating force. All equipment must be inspected periodically by the technical maintenance personnel who will repair or replace worn or failing parts.

7-27 Closed Circuit Television

Closed circuit television (CCTV), while not an intrusion detection system in itself, is very useful in physical security operations and is frequently used to complement such a system.

a. This may be accomplished by placing cameras at critical locations to provide direct visual monitoring from a vantage point. Closed circuit television may be used on gates or other security areas not manned continuously. This system normally consists of a television camera, monitor, and electrical circuitry. The camera may be remotely controlled by monitoring security personnel.

b. Normal use of TV on entry points includes the use of a two-way communication system between the monitor panel and the gate, and an electrically operated gate lock. With this device, the person at the monitor panel can be alerted on the speaker system by a person desiring to enter, converse with the person, observe him on the monitor to determine his authority to enter, and then release the gate lock. An adaptation may be added to this equipment to enable the monitor personnel to make a side-by-side comparison of a person's face with the picture of his identification badge.

c. CCTV can also be used for surveillance of security cages, high value goods in warehouses, fence lines, movement of cargo (figure 40) and parking lots.

d. TV controls should be enclosed in metal housing and properly secured to preclude attempted adjustment by unauthorized personnel. Delay caused by camera warmup and adjustment may be eliminated by keeping the camera in contiguous operation.

e. Normally, surveillance TV is of the low light level type (LLLTV) and can operate under marginal light conditions. A key consideration is maintenance of the TV system and supportive artificial lighting system.

7-28 Perimeter Intrusion Detection

The primary means of perimeter protection continues to be personal observation. However, such observation is usually limited to that performed by periodic patrols. Intrusion detection systems (IDS) may be valuable additional security aids if the perimeter requires continuous surveillance.

a. The decision to use IDS depends upon:
- Vulnerability and sensitivity of the protected area.
- Degree of protection necessary.
- Security aids currently in use.
- Availability of manpower.
- Cost effectiveness.

b. Usually, gates are protected by locks and intermittent patrol checks, or with security personnel on continuous duty. Intrusion detection systems at gates are not normally justified. However, if the gate is used only intermittently, or if additional protection is desired for the gate portion of the perimeter fence line, some system, such as a photoelectric system, may be used for this purpose.

Section IV
The Systems

7-29 Joint Service Interior Intrusion Detection System

The Joint Service Interior Intrusion Detection System (J-SIIDS) is a standardized set of intrusion detection system. components developed to provide physical security for interior areas. Protection of arms rooms was a prime concern in interior areas. Protection of arms rooms was also a prime concern in the development of J-SIIDS.

a. J-SIIDS has been **certified for use** in the following areas:

(1) Finance offices

(2) Post exchanges

(3) Class VI stores

(4) Narcotics storage areas

(5) Accountable property storage areas

(6) High value item storage areas

(7) CID evidence rooms

(8) Conventional weapons storage areas

(9) Billets and offices

(10) Aircraft hangars

(11) Nonconventional weapons and chemical weapons storage areas.

b. J-SIIDS is not certified for use in the following areas:

(1) Sensitive weapons storage areas (RED-EYE, DRAGON, LAW, and STINGER)

(2) Nuclear fuel storage areas

(3) Nuclear reactor facilities

(4) Computer centers

(5) Classified storage areas

(6) Areas where cryptographic devices are stored, used or maintained

(7) Ammunition and explosives storage and manufacturing areas

(8) Radioactive isotope storage areas

(9) Communication centers

c. This system consists of a family of sensors that can be used singly or in combination to provide detection of intrusion. Sensors are grouped into four categories-penetration, point, motion and duress. Signals from sensors are reported to the control unit (see figure 41), processed and transmitted to the monitor unit or audible alarm some distance from the protected area.

d. A J-SIIDS can be adapted for use in any arms room configuration by proper selection and installation to provide detection of unauthorized attempts to enter the protected area. A representative arms room installation is shown in figure 42 (next page).

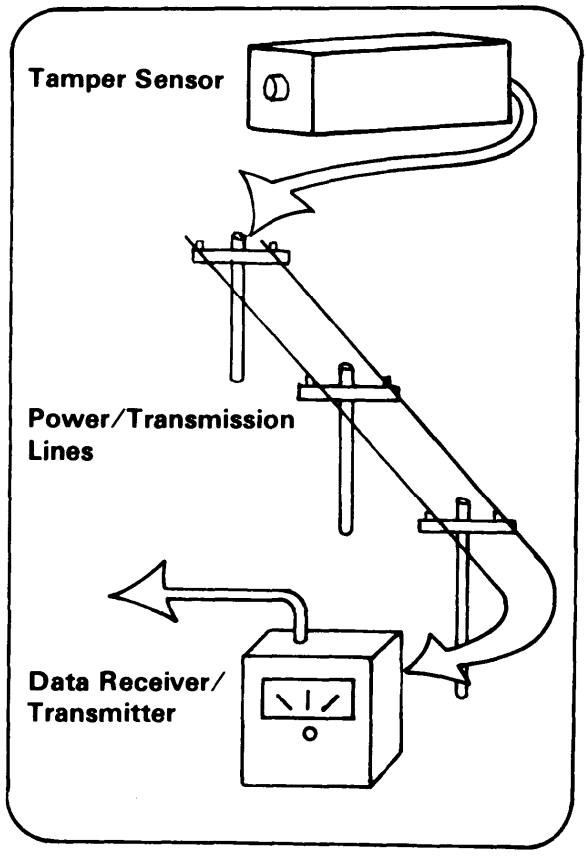


Figure 41—Control unit process.

e. The control unit for J-SIIDS is inside the protected area. It has tamper switches and dedicated telephone lines to carry a coded transmission to the monitor station. Any attempt to tamper with the telephone lines will cause an alarm.

7-30 J-SIIDS Component Categories

a. Sensors.

(1) Penetration sensors:

(a) Balanced magnetic switch
(b) Capacitance proximity sensor
(c) Grid wire sensor
(d) Vibration sensor
(e) Passive ultrasonic sensor

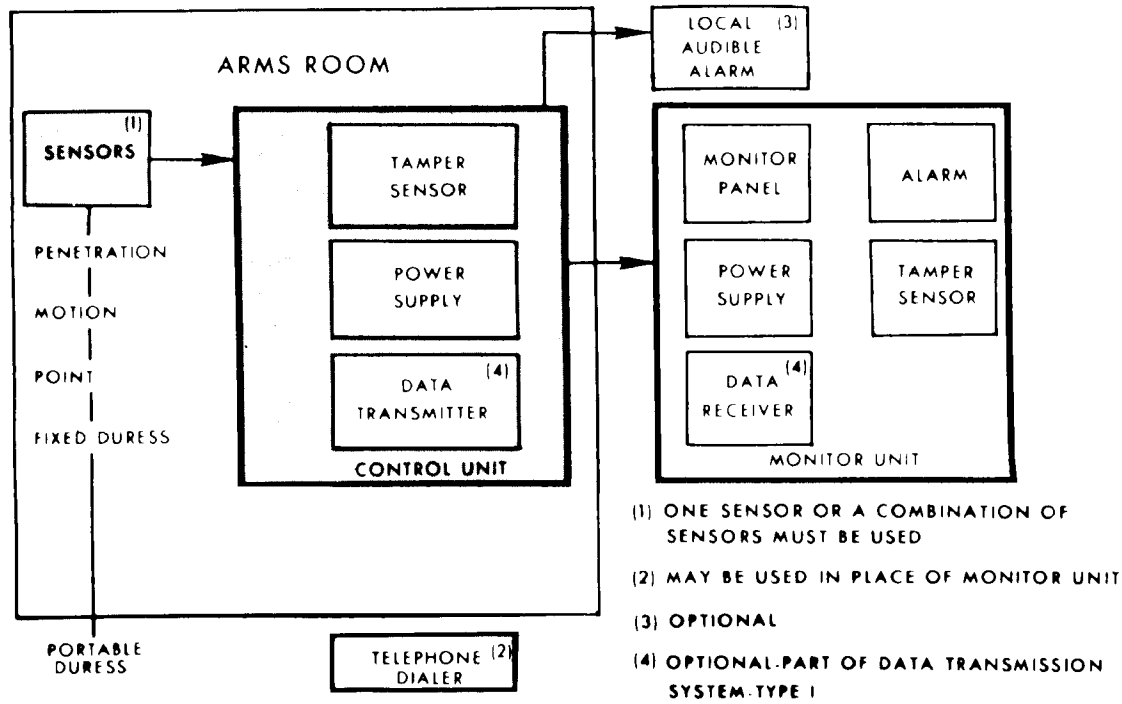


Figure 42—Example of arms room application of J-SIIDS.

(2) Motion sensor: Ultrasonic motion sensor.

(3) Point sensors:

(a) Magnetic weapons sensor
(b) capacitance proximity sensor

(4) Duress sensors:

(a) Fixed duress sensor
(b) Portable duress sensor.

b. Control unit.

c. Monitor unit.

d. Local audible alarm.

e. Telephone dialer.

f. Data transmission system (Type I).

g. The selection of components to make up each intrusion detection system depends on the physical characteristics of the specific area to be protected, operating characteristics of various systems, and the overall security program of the particular command or activity.

7-31 Addable J-SIIDS Components

a. Additional J-SIIDS components have materialized to provide more capabilities for protection of arms rooms and improve protection flexibility for areas other than arms rooms. In short, the components fill security voids in a basic J-SIIDS setup. Addable J-SIIDS components include:

- Commercial Alarm Monitor Interface (CAMI)
- Alarm Line Security Attachment (ALSA)
- Special Application Alarm Monitor System (SAAMS)
- Data Transmission System Resynchronization Kit (DTSRK).

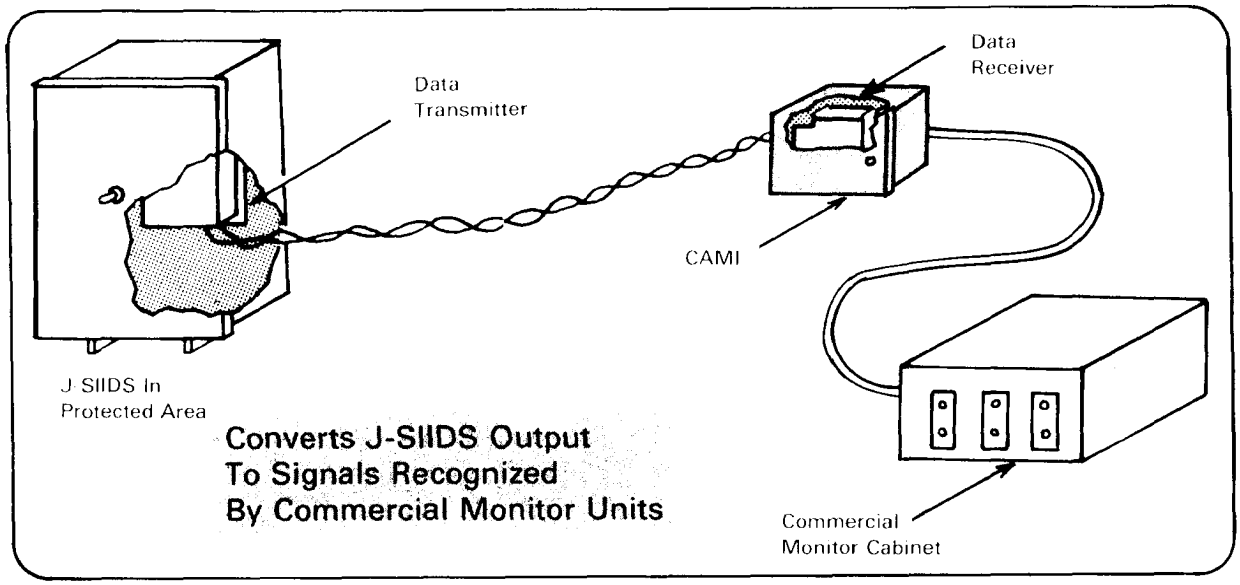


Figure 43—Commercial / J-SIIDS Alarm Monitor Interface (CAMI).

b. Commerical/J-SIIDS Alarm Monitor Interface (CAMI) (figure 43) will receive alarm-secure-access signals from an internal mounted J-SIIDS data receiver and electrically convert these signals to a format that will activate standard commercial alarm monitors. Many existing commercial alarm monitor stations are modular, allowing new modules to be plugged into a spare location in the monitor panel when additional protected areas are added to the system. For these areas, J-SIIDS can be monitored on the already available commercial type alarm monitor panel through the use of the CAMI rather than installing a J-SIIDS monitor unit.

c. Alarm Line Security Attachment (ALSA) (figure 44) consists of a printed circuit card mounted in the production J-SIIDS control unit and a complex terminating impedance mounted in each sensor signal processor enclosure. Circuitry on the card continuously monitors both the phase and amplitude of an a.c. signal on the alarm lines between the sensor signal processor and the control unit. If an attempt is made to inhibit a sensor alarm output by bridging across or

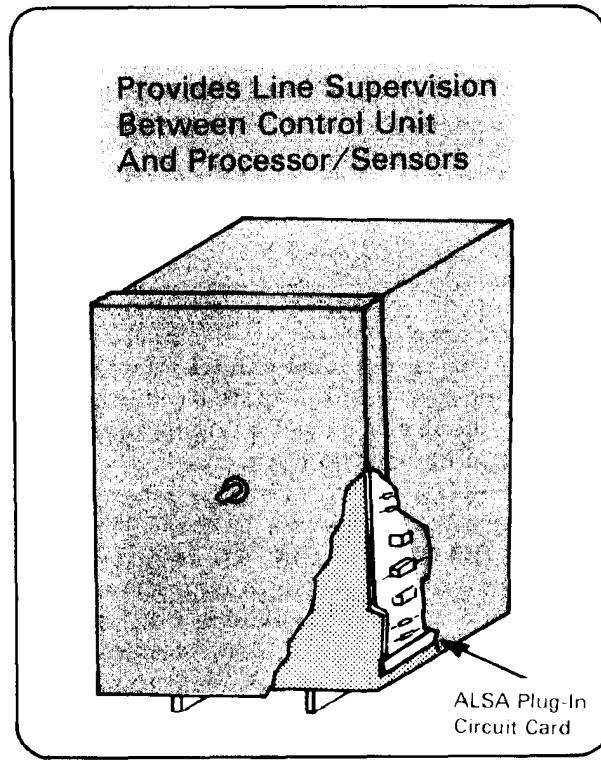


Figure 44—J-SIIDS Alarm Line Security Attachment (ALSA).

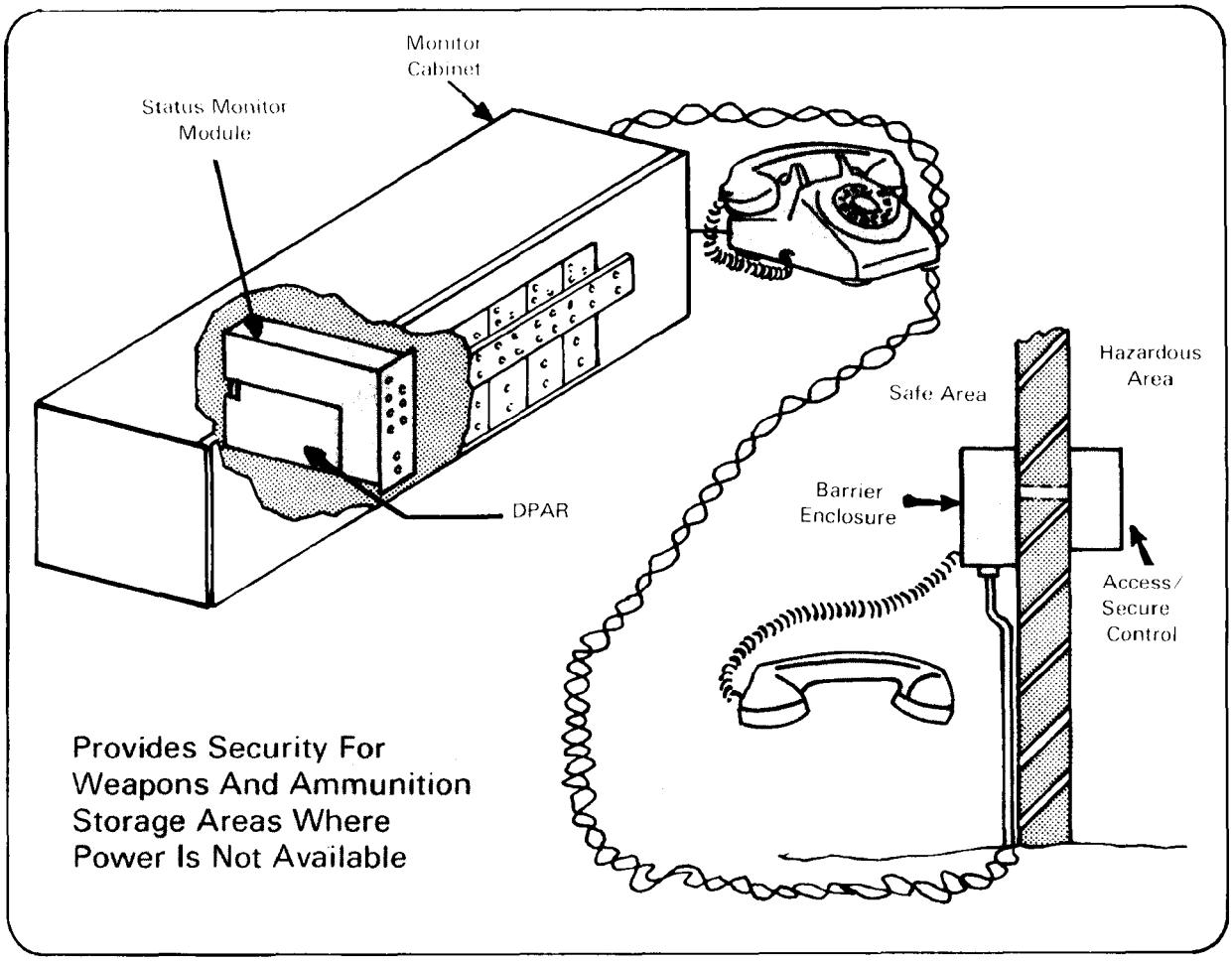


Figure 45—J-SIIDS Special Application Alarm Monitor System (SAAMS).

opening the sensor alarm lines, the ALSA will detect phase and amplitude changes in the a.c. signal and output a tamper alarm to the control unit alarm circuitry.

d. Special Application Alarm Monitor System (SAAMS) (figure 45) is an alarm monitor system designed to be intrinsically safe for use in Class I, Division I hazardous locations. The system uses nonpowered sensors, such as the J-SIIDS balanced magnetic switch and gridwire sensors, and interfaces with the J-SIIDS monitor cabinet. SAAMS consists of an access/secure enclosure (mounted inside the hazardous area), barrier enclosuere (mounted outside the hazardous area), a dual P annunciator receiver (DPAR) and a modified status monitor module which interface with the monitor cabinet, and a telephone circuit which allows voice communication between the hazardous area and the monitor site. The only voltages present in the SAAMS at the hazardous location are low level (less than 3 volts) a.c. signals placed on the transmission lines by the DPAR to monitor alarm and access/secure status of the hazardous location.

e. Data Transmission System Resynchronization Kit (DTSRK) (figure 46) is an electronic device designed to allow resynchronization of the J-SIIDS data transmission system from the monitor cabinet. This device

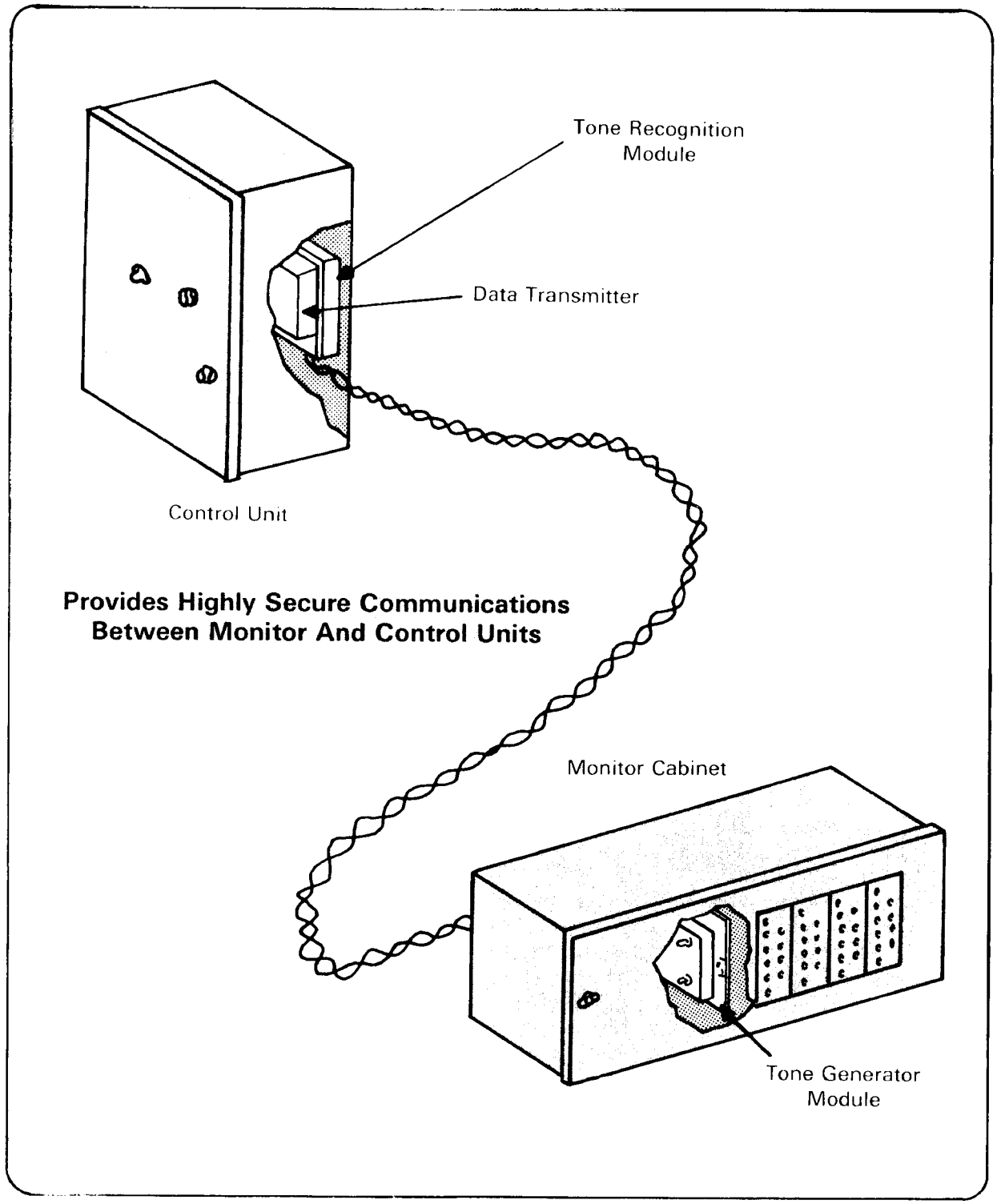


Figure 46—J-SIIDS Data Transmission System Resynchronization Kit (DTSRK).

will function over transmission lines up to 10 miles in length. The device consists of a tone generator module which interfaces with the monitor cabinet and a tone recognition module which interfaces with the control unit and data transmitter.

7-32 Facility Intrusion Detection System (FIDS)

FIDS (figure 47) is a joint service project, intended to provide DOD with a system to detect intrusions into, theft and pilferage from, or espionage/sabotage activities against all types of facilities worldwide. A valid requirement for FIDS exists because J-SIIDS did not meet the physical security requirement of the areas mentioned previously. FIDS is being developed for areas that presently are not protected by a standardized IDS.

a. Purposes:

(1) Developed for worldwide application containing improved communications, control, and display functions.

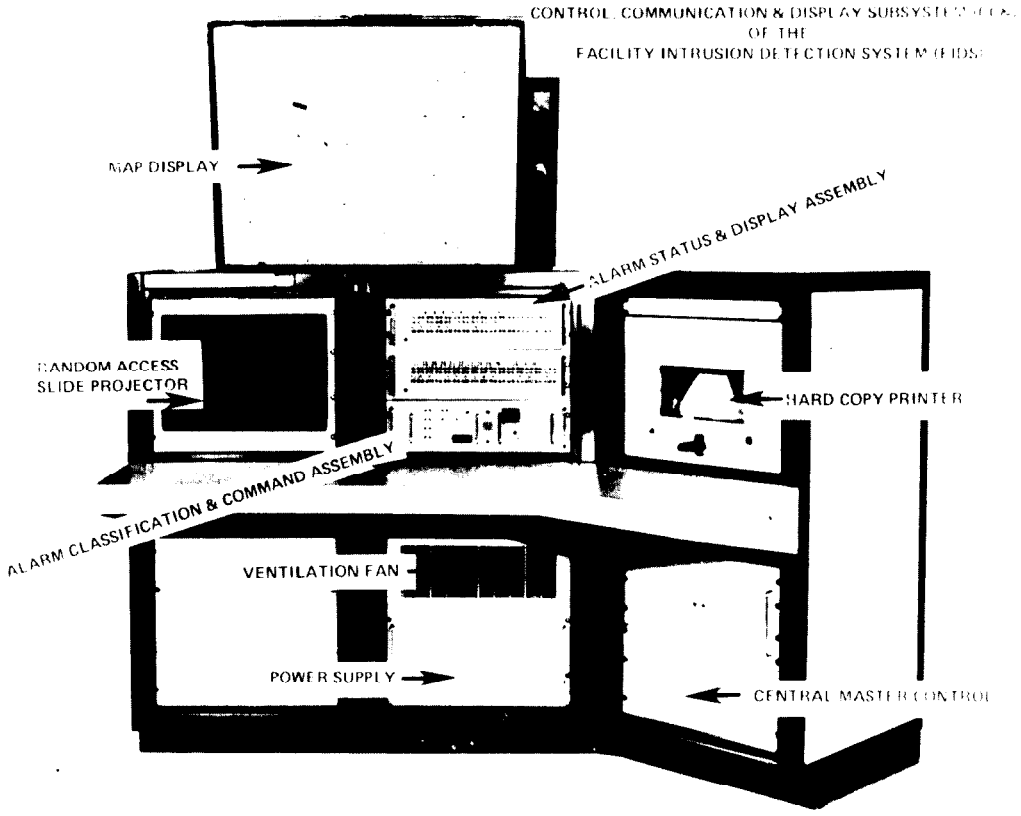


Figure 47—FIDS control unit examples.

(2) Provides an advanced additional detection and response capability that is not all inclusive with the J-SIIDS.

b. Additional capabilities:

- Worldwide operation
- Higher defeat resistance components
- Additional sensing capabilities
- Command capability
- Centralized processing and display capability
- Improved control unit and monitor unit
- Contraband sensors
- Entry control
- Improved duress sensors
- Response/deterrent system.

c. FIDS sensors come in four basic types, each with advanced characteristics. The four types are:

- Point
- Penetration
- Motion/Presence
- Duress.

(1) Basic characteristics for the point sensor involves capacitance proximity and magnetic weapon while the advanced characteristic concerns point contact strain only.

(2) Characteristics of the penetration sensor device in the basic configuration involves employment of:

- Vibration settings
- Grid wire
- Passive ultrasonic role
- Balanced magnetic switch(s).

The advanced stages of the penetration sensor involve point contact strain thermal and gamma effects.

(3) For the **motion/presence** sensor, its basic role concerns ultrasonic and large area motion. Advanced stages of the sensor concerns employment in a passive motion or a combination of ultrasonic/ microwave and ultrasonic/ infrared.

(4) Duress sensors' basic characteristic involves fixed duress situations and portable hand activated. It contains a physiological application in the advance stages.

d. FIDS' control, communications, and display system involves items, basic, and advanced uses as shown in fig. 48, page 120.

e. FIDS ancillary equipment has four characteristics—local alarm, entry control system, response force, and surveillance equipment.

(1) The local alarm in basic application involves an audible capability, while it displays a visual (flashing light) alarm signal in the advanced stage.

(2) In the basic stage, the entry control system uses keys, control card or pushbutton for entry application. In advanced application, the system uses:

- Fingerprint identification
- Voice analysis
- Handwriting analysis.

(3) The equipment's response device in the basic phase employs light activation, and is used in the advanced stage with:

- Electronic activated gates
- Recordings (warning, deterrent, etc.).

(4) FIDS ancillary equipment concerning

FIDS Control, Communications, and Display System

Items	Basic	Advanced
Control	Control Unit	
Data Transmission Link	Hardware (Interrogate/ Response)	Radio Frequency, Fibre Optics, and Strain Sensitive
Display System	Alarm and Status Display	
	Alarm, Classification, and Command Assembly	
	Hard Copy Printer	
	Map Display (Alarm Only)	
Power Supply (Backup)	Protected Area (d.c.)	
	Monitoring Area (d.c.)	

Figure 48.

surveillance capability identifies by audio in the basic stage, and identifies intruders through visual (CCTV) in the advanced stages.

f. FIDS is **certified for use in the following areas** (not for J-SIIDS application, par. 7-29b):

(1) Sensitive weapons storage areas (REDEYE, DRAGON, LAW, and STINGER)

(2) Nuclear fuel storage areas

(3) Nuclear reactor facilities

(4) Computer centers

(5) Classified storage areas

(6) Areas where cryptographic devices are stored, used, or maintained

(7) Ammunition and explosives storage and manufacturing areas

(8) Radioactive isotope storage areas

(9) Communication centers

(10) Nonconventional weapons storage areas and chemical weapons storage areas.

7-33 Fixed Installation Exterior Perimeter Sensor System (FIEPSS)

FIEPSS is a standardized security system to detect/prevent intrusion, forcible entry and/or unauthorized access into installations or facilities. This system consists of a family of sensors and a monitor unit. The sensors are classified as perimeter, barrier penetration, imaging, point, limited access, contraband, and duress. The system must be monitored from a central control.

a. Operational concept.

(1) The system must be deployed to detect the intrusion or attempted intrusion across installation perimeters, and boundaries of areas inside or outside the installation perimeter.

(2) It must also detect the unauthorized presence of personnel within the areas mentioned in the preceding paragraph and the unauthorized entry or removal of protected items within the area boundary.

(3) Security personnel in duress situations

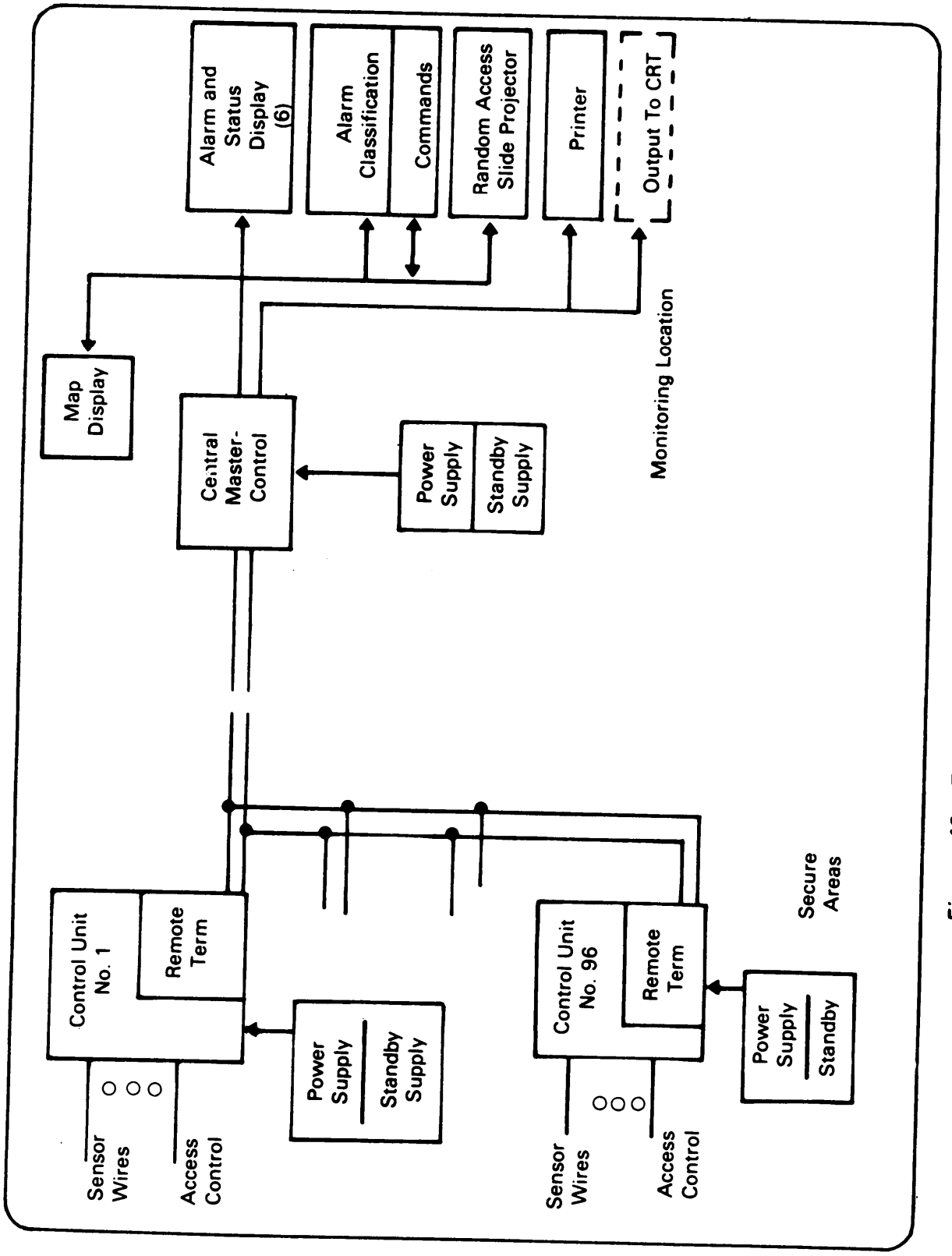


Figure 49—Example of FIDS component interface.

must be able, using this system, to activate a duress sensor to indicate a need for assistance.

(4) Each sensor component must be capable of announcing evidence of intrusion or unauthorized presence through a control unit to monitoring and display equipment located at the control center.

(5) The FIEPSS must provide the user flexibility and modularity in tailoring the system to the particular requirements of the installation and must be operated by installation security personnel.

(6) .Unmanned sensors will be employed along perimeters and/or around key facilities.

(7) A member of the security force must monitor the system in total and dispatch security forces to investigate alarms when activated.

b. Organizational concept. This system must be employed on an installation-by-installation basis in CONUS and OCONUS.

(1) Size and configuration of the system to be employed will be determined by the installation security manager.

(2) Some installations could employ a FIEPSS to completely cover its installation perimeters, while other installations might employ the system to cover an area within its perimeter, such as an ammunition storage area or a warehouse complex.

(3) Using units could vary from a total installation to selected units with special security requirements; such as ASA detachments. It is possible to have more than one FIEPSS on an installation.

c. Characteristics. The system will increase the mission reliability of personnel securing and protecting installation perimeters and areas of interest within and without the perimeter. It reduces losses due to pilferage, sabotage, espionage, organized ground attack, or other physical intrusion. The system includes following essential characteristics:

(1) Service and storage life of 10 years.

(2) Capable of operating continuously.

(3) Capable of being stored and operated in climatic categories 1-8, AR 70-38. The requirements of which can be met by means of a cold weather kit.

(4) Provide operation from primary and backup power sources. Backup power sources (batteries) must provide 24-hour minimum operation.

(5) Design consistent with electronic magnetic impulse (EMI) requirements of intended operational environments.

(6) Employed so that individuals cannot gain information by electromagnetic exploitation or other means that will enable them to defeat the system without an alarm being activated.

(7) Incorporate a self-test capability at the monitor unit to check functioning of the system.

(8) Capable of protecting several zones simultaneously.

(9) Consist of appropriate mixes of the following sensors:

(a) Perimeter sensors–Detect intrusion across or under a land boundary line to a minimum height or depth of five meters, or across or under a line on the surface of a body of water, which defines the perimeter of the area to be protected.

(b) Barrier penetration sensors-Sense intrusion or attempted intrusion through a physical barrier; such as a chain link fence, which is part of the perimeter of the area to be protected.

(c) Imaging sensor–Detect intrusion or

confirm the presence of an intruder announced by another type sensor.

(d) Point sensors—Detect someone approaching and/or touching a protected item; such as aircraft, vehicles, etc.

(e) Limited access/contraband sensors—Detect movement of persons or items into or out of the protected area.

(f) Duress sensors—Permit the stationary or roving guard force to signal for help in case of emergency.

(10) Have a control unit to provide primary power to sensors. The unit shall relay status of the sensor monitored area to the monitor unit. The system shall individually identify alarms from each sensor. Control unit shall monitor security of surveillance area by providing supervision of sensors, indication of change of power source and tampering or change of line integrity status. Unit shall automatically switch to self-contained emergency power should primary power supply fail. It shall provide the capability of simultaneous zone alarm in a guard tower as well as in the control center.

(11) Monitor unit displays the status and location of sensors by zone and/or sensor. Unit shall provide both audible and visual alarms, hard copy of all alarms and status changes and an output for a map display.

(12) Map display capability to indicate sensor locations with numbered light system keyed to a standard map or chart.

(13) Central console shall be capable of integrating data, providing display compatibility with the facility intrusion detection system and the remotely monitored battlefield area sensor system and commercial intrusion detection system and will include a map display capability.

(14) High probability (95-99%) of detection of skilled and semi-skilled intruders and organized forces.

(15) Data transmission system providing hard wire and/or RF data transmission capability between monitor and control unit. This system must provide for security of both hard wire and RF transmission, to include protection hardening of wire and encrypting of radio frequency (RF) transmission, if and when required. The system must provide the capability for initiating reactions, such as deterrent systems, lighting, imaging and listening devices, and responding to a systems test.

(16) Response unit to provide a command capability for illuminating an area and initiating deterrents, ranging from broadcast voice warning to application of force.

(17) Capability to identify and reject nuisance stimuli (false alarms) initiated by natural or manmade environments, either at the sensor or control unit, with a high degree of probability.

(18) Designed to have a specified mean-time-between-failure (MTBF) of 720 hours, assuming a system comprised of no more than 12 components. A failure of any of the 12 components is considered a system failure.

(19) Mean-time-to-repair (MTTR) for each subsystem shall not exceed 30 minutes for organizational maintenance and 60 minutes for DS and GS maintenance. Scheduled maintenance shall not exceed 2 hours for every 1000 hours of operation.

(20) Must to the maximum extent, be designed to modular replacement of reparir parts.

(21) Not susceptible to electromagnetic deception/countermeasures.

(22) Fail in the alarm mode for all faults.

(23) Safe to use at nuclear weapons storage installations.

(24) Designed to overcome these three

possible TEMPEST (compromising emanations) hazards:

(a) Flooding phenomena (as defined in NACSI 4000.3).

(b) Fortuitous conduction of compromising emanations from the facility being protected.

(c) Electromagnetic radiation of compromising emanations from the facility being protected.

(25) Designed for installation in accordance with Military Standardization Handbook (MIL HDBK) 232 whenever the facility being protected processes classified information electrically.

d. Data transmission system. Data transmission and display equipment being developed for J-SIIDS and Base and Installation security System (BISS) can be adapted to meet requirements of the basic system.

(1) The basic system consists of the following components:

(a) Control unit at installation perimeter to collect alarms from sensors and supply primary power to sensors.

(b) Hard wire/RF data transmission system from control unit to monitor unit.

(c) Monitor unit with status display modules.

(d) Status display map to be used with monitor unit when required.

(e) A buried line sensor for protecting land perimeters.

(f) A sensor for protecting perimeter fences.

(2) The complete system contains additional features such as:

(a) Central console equipment.

(b) A sensor for detecting penetration over or under water boundaries.

(c) A sensor for detecting human motion.

(d) Limited access/contraband sensors.

(e) Duress sensors.

(f) Response unit.

7-34 Base and Installation Security System (BISS)

BISS is a product of the US Air Force and is a standard for DOD. It has the capability of interfacing with other intrusion detection and sensor systems.

a. Functional role of BISS:

(1) Electronic surveillance
(2) Electronic detection
(3) Identification of intruders.

b. System description. The system being developed under this program consists of a wide variety of equipment and system segments, which when selected, configured and integrated for specific security situations will comprise electronic systems (such as, BISS) for particular situations.

(1) A single system configuration for all applications will not be the eventual product; but will be various types of equipment developed against a standard system specification. The important factor is that equipment can be integrated in various configurations and function

together as a system that will accept interior facility sensors (such as J-SIIDS and others).

(2) Such a system when employed provides a completely integrated electronic security system comprised of internal and external elements functioning under central command and control.

(3) The situations in which the BISS capability is applicable to worldwide are many and varied. These have been grouped into three categories (or modes of deployment) for system engineering-permanent installations, semipermanent installations (transportable mode) and mobile (quick reaction mode). Considerations in employing systems in these three distinctly different situations are varied, and are factors in engineering the BISS. However, they are factors which directly influence equipment and system segment engineering, and only indirectly the total system.

c. Application. Viewed from an operational application or functional standpoint, the initial system will consist of equipment in the following two subsystems.

(1) Detection is the basic subsystem for any system, and is comprised of sensors, and a sensor data transmission and display segment. Sensors that employ various techniques to detect the presence or movement of people and vehicles are being developed. Data transmission must be by hard wire with line security, and radio frequency (R/F). Either or both can be employed, depending on the situation.

(2) Surveillance uses various techniques to present on a remote monitor visual presentation of an area or location under surveillance. Surveillance may be for observing activity within a wide area, or assessing causes for sensor activations. (When a motion detection feature is incorporated, visual equipment can also be used as a sensor to signal movement.)

d. Intelligence. BISS is charged with developing enhanced intelligence capabilities for the security forces, enabling them to provide for physical security of DOD bases and installations.

(1) BISS will have application literally to every conceivable geographical location, operational environment, and external threat intensity. The common threat in defining the BISS threat model is, therefore, to be found in the operational concepts of its users. The shared threat for BISS is any individual, or group of individuals, who penetrate or attempt to penetrate a boundary, or who enter into an area of denied access. BISS provides detection, surveillance, and warning of such an intrusion, and, when possible, aids in response to an alarm stimulus.

(2) The operational response evoked from local security forces by the detection of intrusion must reflect the level of threat represented by the ingress depth of the intrusion. This reflected threat level depends on the existing external threat (hostile vs. nonhostile), ingress extent of the intrusion (area, boundary, or point), and the intrinsic value of the protected resource.

(3) In selecting the components of BISS, as well as in planning a specific BISS configuration, consideration must be given to both the nature of the threat and to the reflected level of the threat. (These are discussed more filly in following paragraphs.) When a user defines his BISS installation requirements, he must define his general threat level, including all possible escalations from that level. The user depends on his own intelligence channels to assist in his defining and maintaining the specific threat definitions associated with each of his specific configurations.

(a) Nature of threat. In general, BISS must function against both external and internal threats.

(b) Internal threats. Personnel who work in, or have intimate knowledge of the area and the security system are the source of internal threat. This threat is generally considered to be a human reliability problem. Susceptibility of this threat can be reduced by incorporating certain security measures and procedures into hard wire design, system installation and system operation. For example, boxes, sensor covers, and cables can be designed to make them less vulnerable to tampering; and communication networks can be provided with tamper detection capability through line supervision.

(c) External threat. The external threat can generally be divided into five categories—skilled, well-equipped, semi-skilled, organized force, and casual intruders.

■ Skilled and well-equipped intruder(s). These intruders would attempt penetrations to conduct military operations, espionage, sabotage and theft of sensitive or very high value items. They could be expected to plan their entry thoroughly and to carefully select the time and method of entry. Highly skilled intruders using professional, advanced techniques would probably attempt to covertly defeat or circumvent your intrusion detection and other physical protective measures. An intrusion detection system, however, can deter intrusion and can increase the difficulty of such an intrusion, resulting in a higher probability of detection.

■ Semi-skilled intruders. These intruders would attempt penetration to conduct terrorist or paramilitary activities, theft for profit, and/or vandalism. In addition, highly motivated and capable dissident groups or individuals may try to reduce confidence in the military establishment, embarrass the government, or create a dramatic incident to attract public attention. They would be expected to attempt entry without detailed planning or highly sophisticated equipment. They may evaluate the security posture by considering appropriate time factors, location vulnerability, and personnel/guard presence. They may attempt to bypass or otherwise defeat an intrusion detection system by covert means.

■ Organized force. Well organized units can be expected to use overt force and diversionary actions to gain entry. Efficiency, depth of planning, execution, and size of acting force may vary greatly. Altering intelligence will be necessary to upgrade the defense or security posture required to effectively counter this threat.

■ Casual intruders(s). These intruders would attempt penetration with little or no advance planning and without apparent rational purpose. They include thrill seekers and individuals who are mentally deranged or intoxicated. While they represent no military threat in the usual sense, it is possible they might inadvertently or with malicious intent cause considerable damage. An intrusion detection system should detect these intruders with very high confidence.

(d) Levels of threat. For convenience, the general levels of threat have been designated low, medium and high. The essential point is that each BISS configuration must take into account this general threat level and its possible escalations. BISS must contain a sufficient variety of modules to permit tailoring each configuration to meet its existing threat and yet provide the required interface capability to upgrade with minimum difficulty and expense in the event that the level of threat escalates. An **analysis of threat levels** is presented in figure 50. This figure also indicates appropriate levels of response by local security forces. Note that as the

Threat Level	Nature of Threat	Required Capabilities
Low	Stand off surveillance/espionage. Minimum/occasional penetration. Limited pilferage. Minor demonstrations.	Denial of surveillance and penetration. Detection and deterrence of intruders. Selective surveillance of critical areas. Deter intruders. Apprehension of pilferers.
Medium	All of low threat intensified. Sabotage. Harassment. Minor destruction and disablement. Dissident demonstrations.	Intensify response to low threat. Earlier detection. Immediate response (small groups). Increased mobility of response forces. Identification and location of sabotage. Capture of intruders.
High	All of medium threat intensified. Organized attack/armed conflict. Major destruction. Combat Intelligence.	Intensify response to medium threat. Complete penetration denial. Immediate response (large & small groups). Armed resistance, capture, destroy. Sabotage detection and prevention. Remote controlled and/or automated response capability. Interface with allied forces.

Figure 50—Threat analysis guidelines.

threat level escalates, requirements for probability of detection, reliability and degree of security required, as well as the speed and intensity of the local security response forces, also escalates.

7-35 Integration of Systems

When electronic protective systems are integrated there is great improvement in the overall security posture of an installation or activity.

A simple example of how DOD sensors would be integrated on an Army installation is shown in figure 51.

7-36 Remotely Monitored Battlefield Sensor System (REMBASS)

REMBASS, as an element of the sensor family, is used primarily in tactical situations in remote areas and acts as a squad or platoon early warning system.

a. REMBASS sensors.

(1) Target detection. Sensors must be able to detect personnel, vehicles, and aircraft (rotary wing only) using as few different technologies as possible.

(2) Target classification. Sensors must be able to classify the following:

Wheels	Tracks	Personnel
Heavy	Heavy	Armed
Light	Light	
(no bikes)		

(3) Sensor emplacement. Sensors must be emplaced by several different means, each offering its own operational advantages to the particular tactical operation. Methods of emplacement are hand, air, and ballistic. Sensors may be employed underground, on top of the ground, or in trees. Permanently or semipermanently emplaced line sensors to be used primarily for base defense are not considered part of REMBASS. However, base defense sensors which may be developed under other programs should be compatible with REMBASS readout elements.

(4) Disposition. Ballistically emplaced sensors must be expendable. Hand and air emplaced sensors must be retrievable during training and expendable during tactical operations.

(5) Emplacement accuracy. Emplacement accuracy is not a REMBASS requirement, but is the responsibility of the delivery platform or individual performing the emplacement. For target acquisition, this accuracy is critical; however, for general surveillance and early warning roles, less accuracy is required. Regardless, employment accuracies must be sufficient to accomplish the three REMBASS target classification roles. For surveillance and early warning, the emplacement accuracy of the individual or delivery platform is considered sufficient. Target acquisition sensors must have an emplacement accuracy sufficient to accomplish a 50-meter circular error probable for target location.

(6) Detection range. In general, sensors should have adjustable detection ranges. Maximum sensor detection ranges should not exceed:

(a) 100 m for personnel (single)X
(b) 1,000 m for vehicles
(c) 500 m for aircraft.

(7) Transmission range. All sensors must have an RF output capable of transmitting to an intended receiver (radio relay or readout unit) at a line-of-sight range of:

(a) 15 km ground-to-ground
(b) 100 km ground-to-air.

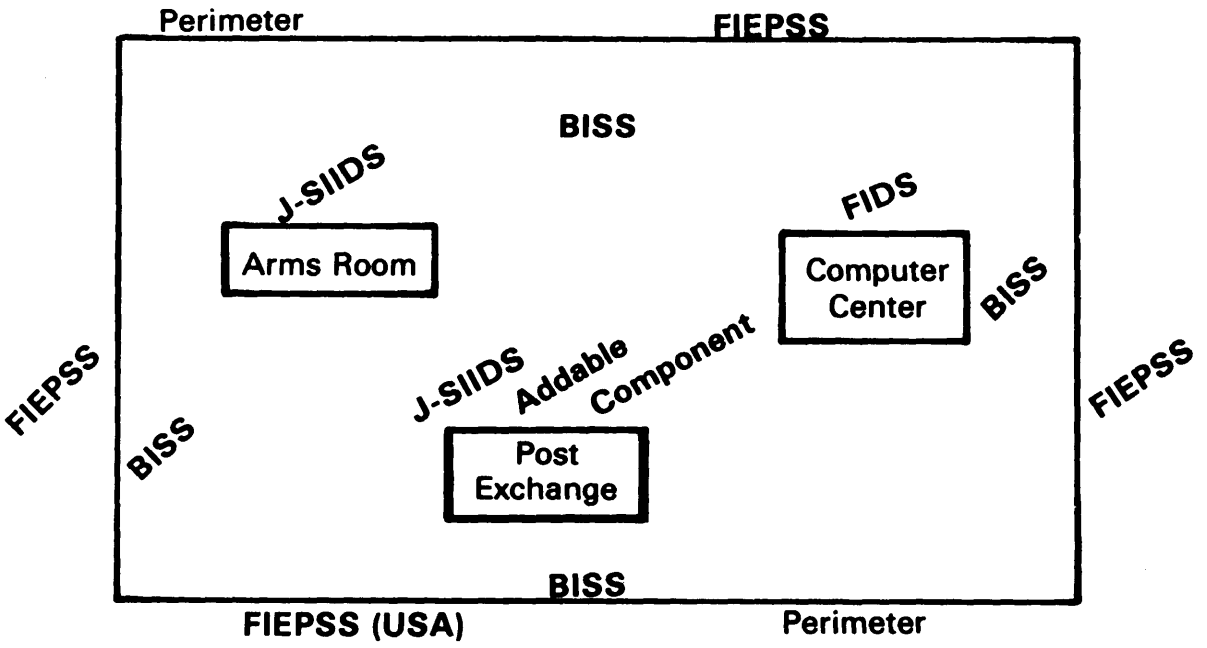


Figure 51—Simplifed example of an installation integrated protective system.

(8) Commendable features. A require ment exists for a commendable imaging sensor. Desired features are: on, off, transmit, and change viewing direction.

(9) Features required in all sensors:

(a) Selective mission duration (7, 15, or 30 days).

(b) Selective classification (if cost and operationally effective).

(c) Selective detection range sensitivity.

(d) Frequency and ID code that can be easily changed prior to mission.

(e) self-disable circuit to automatically activate upon end of programed life, malfunction, and/or tampering.

(10) Weight and size, including batteries. Hand emplaced sensors should be easily man-transportable. They should be less than 3 pounds and 100 cubic inches in size. Air emplaced sensors must be less than 20 pounds and 800 cubic inches. Ballistically emplaced sensors must be compatible in size and weight to the munitions for the anticipated delivery means.

(11) Mission life and reliability. All sensors must be capable of operating for 7 to 30 days. Strings of three or more sensors will have a 0.97 probability of successfully completing a 7-day mission.

(12) False alarm rate. Sensors will be designed so the system will experience an average false alarm rate per sensor of not more than 3 percent of alarms, or not more than one false alarm per 24-hour operational period.

(13) Channel and ID selection. The capability to select frequency channel, and ID code by emplacement personnel in the field is required. Although such occurrences are expected to be relatively infrequent, the procedure and/or techniques to accomplish selection must be simplified.

(14) Realtime/nonrealtime outputs. Realtime outputs are desired for all sensors. Digital sensor alarms should be

realtime with an inhibit (update) time of 10 seconds. Since analog outputs from special acoustic and image sensors require much wider bandwidths, analog-to-digital conversion with delayed transmission times is acceptable, if the delay is not greater than 1 minute.

(15) Power supply. Each sensor requires an internal power supply that will function for the required mission duration in hot and cold environments. Hand emplaced sensors should have the capability to connect to an external alternating current (AC) or direct current (DC) power supply to extend mission life as much as 24 months.

b. Radio relays.

(1) Types. The depth of sensor emplacements in the division area of interest requires a variety of emplacement techniques for relays (hand, air, and ballistic). If size and cost constraints permit, each relay should be capable of transmitting the digital sensor and command signals as well as the signals from imaging or acoustic sensors. Hand emplaced relays must be capable of operating from the ground, from a vehicle, or in an aircraft (without requiring a dedicated vehicle or aircraft).

(2) Channel selection. Selections of desired channels or desired frequency bands for relays may be required in the field by emplacement teams. If narrow band frequency shift keying (FSK) is used for a data transmission system, each type of relay will require a dual channel capability .

(3) Disposition. All relays must be expendable during armed conflict. In peacetime, relays must be recovered and used to the maximum extent.

(4) Transmission range. All relays must have an RF output capable of extending each transmission link by 15 km. That is, the relay must be able to transmit to an intended receiver at a line-of-sight range of 15 km ground-to-ground. Airborne relays must have a line-of-sight range of 100 km.

(5) Storing and time tagging. Each relay, with the addition of an attached module, must be capable of storing and time tagging activity and providing this data upon command.

(6) Self-disable features. These features, which must automatically activate upon end of programed life, malfunction, tampering, and/or end of battery life, should be included in all relays.

(7) Size and weight. Hand and air emplaced relays should not exceed 1.5 cubic feet and 30 pounds. Ballistically emplaced relays must conform in size and weight to the munitions for the anticipated delivery means.

(8) Mission life and reliability. All relays must be capable of operating for a 1 percent duty cycle for up to 30 days on internal power sources. The reliability of three relays in a series must equal 0.87 for a 7-day mission.

(9) Power supply. All air and ballistically emplaced relays require internal battery supplies. Hand emplaced relays should have provisions for external power supplies. Airborne relays require provisions for using aircraft power.

(10) Storage capability. To retransmit near realtime audio or image information, a store and forward feature may be required.

c. Basic readout unit.

(1) The readout unit must be the basic sensor monitoring device in the REMBASS. The readout unit must consist of a receiver, hard copy printer or chart record, and a backup visual display.

(2) Input/output features. Readout input will be RF from the sensors or relays. The primary output from the readout should be hard copy. A visual light display

backup is also necessary. Output should provide the following information:

(a) Sensor identification
(b) Type target (classification)
(c) Timing information.

Auxiliary outputs must be provided for image and acoustic processing devices.

(3) Frequency selection. Manual selections of frequency channels will be necessary. There is a requirement for a dual channel receiver in the basic readout unit for limited electronic warfare (EW) protection and for monitoring flexibility.

(4) Power requirements. Readout devices require an internal battery and external AC/DC power capability. The readout must function continuously for 15 hours without requiring battery change.

(5) Computing requirements. When fewer than three readouts are collocated, limited computing capability is required. This may involve a simple nomogram or a small electronic calculator. The sole purpose of the nomogram or calculator is to assist the operator in determining REMBASS functions.

(6) Weight and size. The readout should be man-portable, weigh less than 8 pounds, and be no more than 0.5 cubic feet in volume.

(7) Reliability. Readout reliability must equal 0.94.

d. Command transmitter.

(1) The command transmitter must provide signals to the commendable relay. It must be separate from the readout unit so each can be employed independently.

(2) Power requirements. The command transmitter should have an internal battery and an external AC/DC power capability. It must function. for a 7-day mission without requiring battery change.

(3) Transmission range. A command transmitter must be capable of transmitting over a line-of-sight path of 30 km to either a relay or sensor.

(4) Command outputs. A command transmitter must be capable of addressing commendable sensors and relays on appropriate frequencies and with appropriate ID codes. (In-band command is preferred.)

(5) Weight and size. The command transmitter should be man-portable, weigh no more than 4 pounds, and not exceed 0.4 cubic feet in volume.

(6) Reliability. The command transmitter must have a 0.80 probability of successfully completing a 7-day mission.

e. Special processing unit.

(1) The special processing unit must provide a processing and computing termination for three or more basic readout units. This is a nonessential device used to expand and facilitate operator functions when readout units are stacked within the monitoring site. Sensor activation information from the readouts would be processed so that the printout from the special processing unit will provide:

(a) Sensor activation by ID and time.
(b) Target classification.
(c) Target location in universal transverse mercator grid coordinates.
(d) Direction of movement.
(e) Speed.

(2) Inputs. The processing unit must provide with minimal human interface the same computational capability required of the nomogram or calculator used with a single readout unit. The processing unit must receive inputs from one to six readout units. These units should be either plugged or cabled to the processing unit.

(3) Outputs. The primary output for sensor information would be page print. There may be a need for a paper tape or ADP link which can conveniently interface with the integrated battlefield control

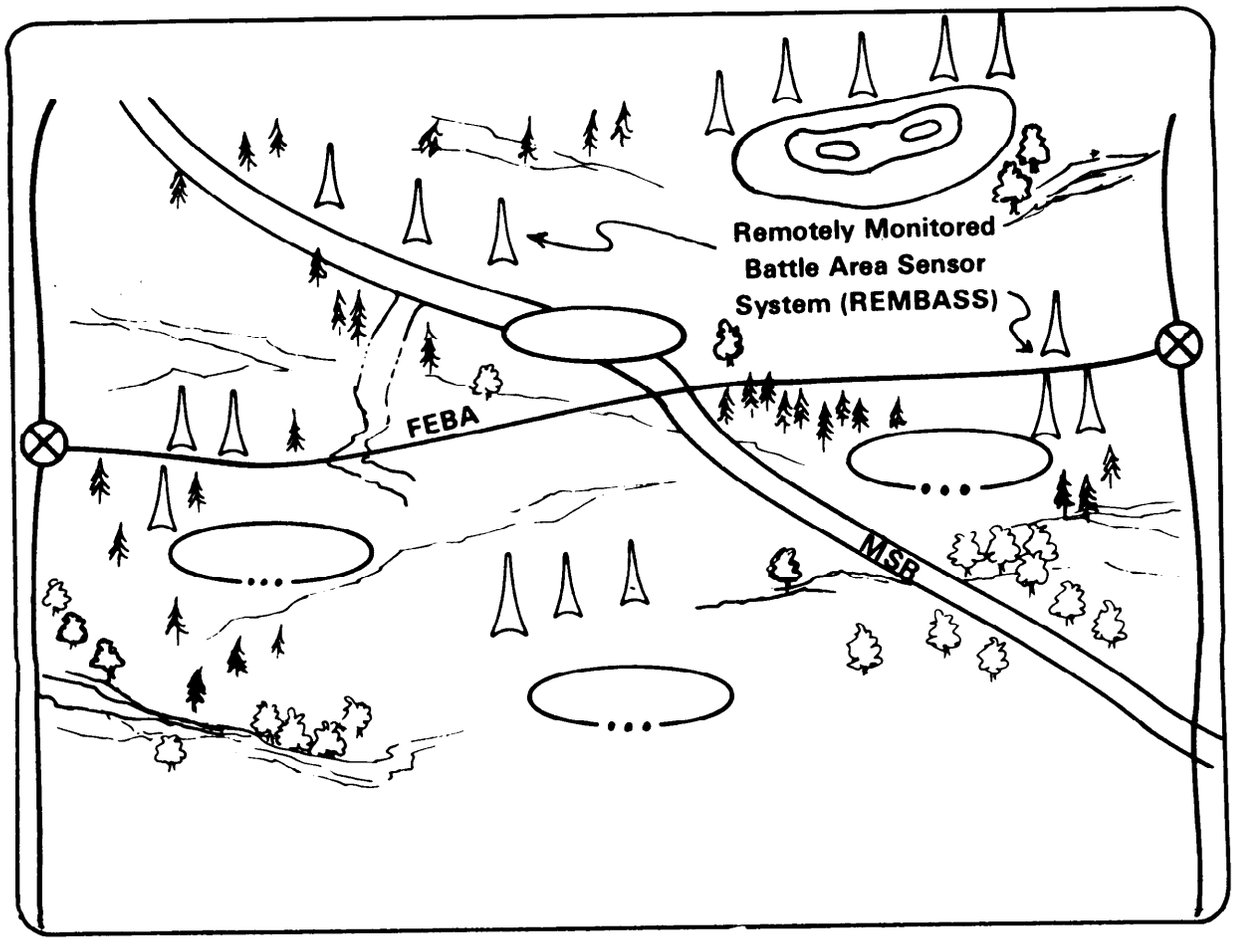


Figure 52—Example of REMBASS tactical employment.

system (IBCS) or tactical operations svstem. This need cannot be established until the IBCS concept is defined explicitly. Auxiliary imaging and audio display/ monitors can be attached to the processing unit for special applications.

(4) Power requirement. The special processing unit should not require internal battery power. An external AC/DC power capability must be provided. The special processing unit should be capable of operating from aircraft and vehicular sources, tactical generators, and external commercial AC sources.

(5) Weight and size. The processing unit should weigh no more than 30 pounds and should not exceed 1.0 cubic feet in volume.

(6) Reliability. The special processing unit must have a 0.948 probability y of successfully completing a 7-day mission.

7-37 Intrusion Detection System for Nuclear Storage (AR 50-5)

a. The **basic electronic security system** must consist of an interior sensor integrated by data transmission links into the annunciator console.

(1) All nuclear weapons storage structures at permanent sites must be protected by primary intrusion detection systems. Alternate backup systems, operated on a different principle of detection, and remote annunciator panels are desirable.

(2) Systems must provide both audible and visual alarm indications and must be dependable, easy to maintain in their operational environment, and adequately protected against tampering. They must give an alarm in case of failure, have low nuisance-alarm rates, and be equipped with a protected, prompt, online alternate source of power or an emergency battery power source.

(3) Systems must be installed and designed so that all portions of the system, including data transmission lines, are protected against tampering.

(4) At sites supporting Allied units, some additional monitor equipment may be required to facilitate US and user-nation coordination.

(5) If the telephone communications system is owned by the Government and maintained and operated by military or civilian employees who have suitable security clearances, wires in the cables may be used for intrusion detection circuits. Otherwise, detection circuits must not be earned in cables that also contain telephone or other electrical circuitry.

b. Interior sensor equipment. As a minimum, protection must be provided to detect entry into a storage structure or maintenance facility used for overnight storage.

c. Control/data transmission (communications).

(1) Hard wire data transmission links must be used for interior sensor components. All transmission lines for alarm circuit should be completely contained in a secured area and must be adequately safeguarded to preclude tampering. If the transmission lines must leave the secured area, they must be inspected frequently by guards. A line supervision system should be installed to monitor lines connecting the intrusion detection devices to the monitor panel. Supervision may be accomplished by monitoring various modes/deviations/ random line signals (such as digital, tone, frequency encoding, and others) and must at least equal the following acceptable mode and supervisory criteria, activating an alarm signal when any of these criteria are exceeded:

(a) As much as 5-percent change in normal line signal, if it consists of direct current from 0.5 milliampere through 30 milliamperes.
(b) As much as 10-percent change in normal line signal, if it consists of direct current from 10 microampere to 0.5 milliampere.
(c) As much as 5-percent change in any component of the normal line signal, if it consists of an alternating current of a frequency from 1 through 100 Hz and 0.5 milliampere through 30 milliamperes.
(d) As much as 15-percent change in any component of the normal line signal, if it consists of an alternating current of a frequency of higher than 100 Hz superimposed on a direct current that has any value from 0.5 milliampere through 30 milliamperes.

(2) Alarm circuits with a remote test capability must be tested at least once during each guard relief. When a remote test is not possible, circuit tests must be conducted at least once every 24 hours by activating detection devices. Inspections must be made at least semiannually by maintenance personnel qualified to repair or replace worn or failing components and to detect evidence or indications of tampering with any portion of the system.

(3) Prior to maintenance or repair, the system must be tested, as in (2) above, and a record made of each sensor/alarm

operating status. The monitoring operator must deactivate only that portion of the system to be repaired and continue to monitor the balance of the system. Immediately after completion of repair or maintenance, the entire system must be tested again, as in (2) above. In addition, those circuits on which repair or maintenance was performed must be tested by physically activating the detection devices.

d. Records. Commanders must insure that personnel monitoring primary annunciator panels maintain records of the data listed in (1) through (9) below. These records, retained for 1 year, will be used for evaluating intrusion detection system effectiveness (including reliability, sensitivity, required adjustments or maintenance, and other information intended to maintain or increase security):

(1) Date, time, and prevailing weather conditions when an alarm signal is received.

(2) Identity of the guard recording the alarm.

(3) Identity of the area from which the alarm was activated.

(4) Cause of the alarm.

(5) Action taken in response to the alarm.

(6) Total elapsed time required by responding personnel to reach the scene.

(7) Tests of detection circuits.

(8) Malfunctions.

(9) Servicing and/or maintenance of the systems .

7-38 Intrusion Detection System for Arms Rooms (AR 190-11)

a. All structures designated for permanent storage of firearms except as specified in AR 190-11, must be protected with an intrusion detection system or be under surveillance by a guard, closed circuit television, or onduty personnel. The IDS used must contain a duress signaling component. Alarms must be annunciated at a location from which a designated response force can be immediately dispatched. Alarm signaling with only a local audible alarm is unauthorized.

b. As a minimum, IDS installed for protection of arms rooms must consist of two types of sensors with different methods of activation (such as a balanced magnetic switch on the doors and ultrasonic motion sensors inside the arms room). Additional levels of protection, where practical, are encouraged. In selecting the mode of operation desired for each arms room, it should be emphasized that an interior IDS is designed to detect, not prevent, an intrusion. Therefore, a comprehensive physical security plan must contain appropriate physical security measures and procedures for an effective reaction force. To insure this, IDS must be installed so that alarm signals can only be cleared by entering the protected area. Remote clearing of alarms prior to entering and checking the alarm is not authorized.

c. The Joint Services Interior Intrusion Detection System (J-SIIDS) will be used as the initial IDS or as replacement for installed commercial systems at onpost facilities. Installation of J-SIIDS at offpost facilities is optional depending upon cost effectiveness, ease of maintenance, and monitoring. Commercial IDS are authorized for installation in facilities off post where J-SIIDS is not employed.

d. Installers and maintainers of the J-SIIDS must have as a minimum, a favorable national agency check or foreign country equivalent prior to having access to J-SIIDS. This includes military personnel, DAC, foreign national employees, civilian contractors or contract foreign nationals. A current list of cleared installer/maintenance personnel must be maintained by the facility

engineer. The **key to access test/retest switch** must be maintained and only those persons on the arms room key roster will be authorized access to these keys on a need to have basis. Keys to the control unit door and monitor must be secured separately from the access test/retest keys, and only authorized maintenance men, whose identity has been verified at the direction of the unit/activity commander, will be authorized access to these keys. Commanders must insure unit personnel will not have access to the interior of the control unit or monitor. All keys to J-SIIDS or commercial equipment must be under control of the commander whose storage area is being protected. Keys must be secured in containers as required for arms room keys; however, they must not be retained together with arms room keys. Wiring diagrams or other instructions developed by the installer to assist maintenance personnel must be stored inside the control unit door in the space provided. Such documents must be marked FOR OFFICIAL USE ONLY (FOUO).

e. When intrusion detection systems are used at arms storage rooms in civilian communities, arrangements must be made to connect alarms to local civilian police agencies, campus police headquarters, or private security companies. There must be a designated response force that can be immediately directed to respond in case of an alarm from the protected area.

f. A daily log must be maintained by monitor stations of all alarms received from arms/ammo storage facilities. The log must indicate, as a minimum: time, date, and location of alarm; identity of individual receiving alarm; nature of cause of the alarm; and action taken in response to the alarm. The logs must be maintained for 3 months. Problem areas identified must be brought to the attention of the troop support command.

g. Transmission lines from control units to monitor panels that are open or accessible to tampering must be electrically supervised. As a minimum, a 24-hour backup power source most be provided for each control unit and monitor panel.

h. Commercial IDS equipment is authorized when J-SIIDS is not available or considered impractical. When government type-classified systems are to be employed, the applicable installation manual must be used. Plans and specifications for installation of commercial IDS equipment must be forwarded through command channels to the Chief of Engineers, HQDA (DAEN-MCE-D), WASH, DC 20314 for final technical review and approval.

i. Periodic systems operational checks must be made and logged by unit security personnel, to include visual inspection of components and conduit for evidence of tampering, operational checks of sonsors to insure stimuli activate the sensor.

j. Installation physical security inspectors should include a check of each IDS during any announced security inspections. Checks should include visual inspection of components and conduit for evidence of tampering, operational checks of the system in accordance with procedures outlined in section V, chapter 5, TM 5-6350-262-14/14 under abbreviated system check test. This same test can be modified and applied to any commercial system. Checks should also be made of unit log entries and records regarding operation and inspection of IDS.

7-39 Maintenance of IDS

a. Intrusion detection systems should remain in **continuous operation** during nonoperational hours of the protected activity if they are to be effective security aids. In some situations it may be necessary to have continuous 24-hour operation. Therefore, preventive and corrective maintenance should be performed properly. Each system should be capable of operating from a stand-by power source to compensate for the vulnerability of power sources outside the

installation. The time requirement for such capability must be evaluated in each case dependent upon such factors as alternate power supplies, maintenance support, hours of active operation, and so forth.

b. Maintenance is not a difficult problem if proper care is routinely exercised. Most malfunctions, if the system has been properly selected, installed, and adjusted, result from improper maintenance. To prevent malfunctions, all component parts must be regularly inspected and tested by qualified personnel as often as recommended by manufacturers. Spare parts, such as fuses, condensers, relays, and other parts as recommended by the manufacturer, should be stocked locally.

c. Normally, the manufacturer will train and advise personnel on maintenance of their equipment. To insure proper operation of detection systems, the following should be observed.

(1) Designated unit personnel should be available and capable of effecting immediate minor repairs, to include replacement of burned out bulbs, replacement of fuses, maintenance and replacement of the auxiliary power unit, and correction of obvious causes of malfunctions and invalid alarms. All other forms of replacement parts and repairs should be provided by support maintenance personnel.

(2) If an installation cannot furnish support maintenance personnel, a service contract should be negotiated with the manufacturer. In either case, maintenance service must be available on a 24-hour basis. Maintenance response time to critical areas should be no more than 3 hours.

d. Operating and maintenance personnel should be cleared for access to classified information to the degree necessary for access to the area concerned. Plans and diagrams showing location and technical data of installed systems, signal transmission lines, and monitor units should be classified and protected accordingly.

e. The alarm receiving area should be designed to give adequate protection to monitor personnel, as this will be a prime target for intruders. Provision for emergency assistance to this area should be established. Appropriate measures should be employed to insure that monitor personnel maintain the system's integrity. Admittance to this area should be restricted to supervisory and maintenance personnel.

f. Personnel on duty at monitor units at installations or facilities using intrusion detection systems should maintain a daily record of all systems including the number of alarms and any malfunctions experienced. Operational records should reflect the following:

(1) Date, time, and prevailing weather conditions.

(2) Identity of person recording alarm signal.

(3) Identity of area from which alarm signal is received.

(4) Action taken in response to alarm signal received.

(5) Total time required by responding personnel to arrive at the scene of an alarm.

(6) Cause for alarm signal to be activated.

(7) Tests of alarms.

(8) Malfunctions, including nuisance alarms.

(9) Servicing/maintenance of detection systems.

g. Maintenance for the J-SIIDS, J-SIIDS addable components, FIEPSS, FIDS, and BISS must be in accordance with the technical manuals published in support of the equipment.