NUREG-0320

INTERIOR INTRUSION ALARM SYSTEMS

J. A. Prell

Office of Standards Development
U. S. Nuclear Regulatory Commission

Available from
National Technical Information Service
Springfield, Virginia 22161
Price: Printed Copy$4.50 ; Microfiche $3.00

The price of this document for requesters outside of the North American Continent can be obtained from the National Technical Information Service.

NUREG-0320

INTERIOR INTRUSION ALARM SYSTEMS

J. A. Prell

Manuscript Completed: January 1978
Date Published: February 1978

Division of Siting, Health, Safety and Safeguards
Office of Standards Development
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

ACKNOWLEDGEMENT

In the preparation of this report, the author drew heavily upon information presented by Sandia Laboratories in a report prepared for the Energy Research and Development Administration (ERDA) entitled "Intrusion Detection Systems Handbook." I am therefore indebted to Sandia Laboratories and ERDA for this information and for their review of an earlier draft of this report. Special thanks also go to Mr. Doss Ledbetter, Mason & Hangar, Silas Mason Company, Inc., for his constructive criticism and appraisal. I would also like to acknowledge the role of private industry whose help in both the preparation and review of this report helped to make it more meaningful.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 PURPOSE AND SCOPE

In meeting the requirements for the safeguarding of special nuclear material and the physical protection of licensed facilities, the licensee is required to design a physical security system that will meet minimum performance requirements. An integral part of any physical security system is the interior intrusion alarm system. The purpose of this report is to provide the potential user of an interior intrusion alarm system with information on the various types, components, and performance capabilities available so that he can design and install the optimum alarm system for his particular environment.* In addition, this report will discuss and recommend maintenance and testing procedures which, if followed, will help the user obtain the optimum results from his system.

1.2 GLOSSARY OF TERMS

Some of the terms related to intrusion alarm systems are presented below with their definitions as used in this report.

Access Mode - The mode of operation in which line supervision is maintained over the signal lines between the premises control unit and annunciator and over the tamper switches in the detector or in any other units of the interior alarm system but in which access is allowed into the secured area without generating an alarm at the central alarm station. Some systems also maintain line supervision between the premises control unit and the detectors while in the Access Mode. (See definition of Secure Mode.)

Active Detector - A detector designed to detect penetration into or movement within a secured area by flooding the area with either electromagnetic or acoustic energy and then sensing any changes in this energy caused by movement.

Annunciator - An electronic unit located in the central and secondary alarm station that is designed to monitor the status and control the mode of operation of remotely located alarm sensors. An annunciator provides both an audible and visual readout after receipt of an alarm signal and offers some form of switching between the access and secure modes of operation.

Circuit Supervision - A specially designed electronic circuit built into the detector to continuously monitor the detector's major circuitry. Upon detecting a circuit malfunction, the supervisory circuit initiates a signal that can be used to initiate an alarm signal at the annunciator.

*Some interior type alarm systems not discussed in this report have been excluded because of the ease with which they can be circumvented.

Detector - An electronic or electromechanical unit that is designed to detect entrance into or movement within the secured area in which it is located and to provide an alarm signal to the annunciator.

Equipment Enclosure - Any enclosure of security alarm subcomponents, access to which may offer the opportunity to defeat the security system or a part of that system.

False Alarm - An alarm received at the annunciator for which there is no apparent cause (reason unknown). The false alarm may be due to system malfunction, environmental changes, or electromagnetic interference. (See definition of Nuisance Alarm.)

Line Supervisory Unit - An electronic unit designed for transmitting in a secure manner over hard wire or via free space the status (alarm/nonalarm condition) of a detector unit to the annunciator unit. The line supervisory unit may be an integral part of the annunciator or the premises control unit.

Nuisance Alarm - An alarm received at the annunciator caused by the alarm system detecting changes in its operating environment that it was designed to detect, but that do not represent a security threat (reason known). (See definition of False Alarm.)

Passive Detector - A detector designed to detect penetration into or movement within a secured area by sensing changes to the natural environment of the area (e.g., passive infrared detectors). A passive detector does not radiate energy of any kind within the secured area, but senses energy produced by intrusion into the area.

Premises Control Unit - An electromechanical unit located at the entrance to or within the secured area that acts as an interface between the detector and the line supervisory unit and is used to switch, in conjunction with switching at the central alarm station, the interior intrusion alarm system between the secure and access modes of operation.

Portal Detector - A detector designed to detect penetration through portal openings such as doors, skylights, ventilation ducts, and windows. It is usually a passive electromechanical alarm used for surface protection.

Secured Area - Any area that has a physical security system in place to detect unauthorized penetration of or movement within the area. As used in this report, it refers to any enclosed volume that is protected by an interior intrusion alarm system.

Secure Mode - The mode of operation in which security supervision is maintained over detectors, the signal lines between detector units and the annunciator unit, and the tamper switches of all units in the interior alarm system. Penetration or movement in the secured area generates an audible and visual alarm at the central alarm station. (See definition of Access Mode.)

Surface Detector - A detector designed to detect penetration through the secured boundary of the space to be protected. May include portal detectors at portal openings of the secured boundary.

Transducer - A device used for converting energy in one form to energy in another form. As used in this report, a transducer either converts electrical energy to ultrasonic, microwave, infrared, or other type of energy or converts ultrasonic, microwave, infrared, or other type of energy to electrical energy.

Transmission Line - Wire or coaxial cable running from the secured area to the central alarm station to transmit the status of the detector units to the annunciator.

Volumetric Detector - A detector designed to detect movement within a specified volume. A volumetric detector can be either active or passive in operation.

1.3 GENERAL

Interior intrusion alarm systems are designed to detect the penetration, motion, or presence of an individual within a specified enclosed area (e.g., a vault or room within a building) and to transmit the information to a central alarm station where it can be acted upon. A basic interior alarm system may be composed of the following components: detector units, premises control unit, line supervisory unit, annunciator unit, and power supply (see Figure 1). The line supervisory unit may be an integral part of the annunciator unit, the premises control unit, or the detector unit.

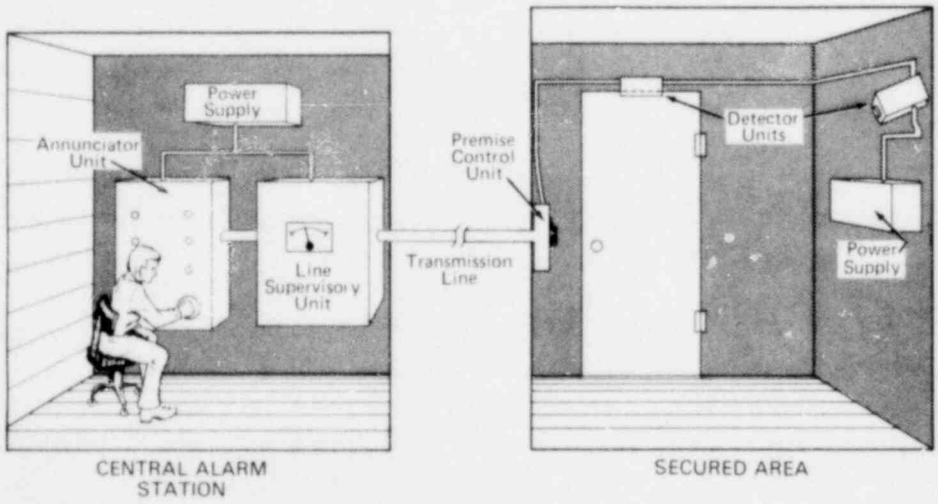

FIGURE 1. BASIC INTERIOR INTRUSION ALARM SYSTEM

There are features in any interior intrusion alarm system which, if incorporated by the user in specifying and designing the system, will enhance the overall security of the alarm system. Some general specifications that the potential user should keep in mind when specifying and designing each component of an alarm system are presented below.

1.3.1 Enclosures

All enclosures containing subcomponents of the alarm system can be equipped with tamper switches or triggering mechanisms that alarm whenever the enclosure is opened. This will help protect against surreptitious attack by an insider. However, it should be remembered that, whenever tamper switches or triggering mechanisms are used, they should be so wired that they can be continuously monitored in both the access and secure modes of operation.

Key locks or key-operated switches using Underwriters Laboratories approved locking cylinders will help provide greater security to the enclosure. Further information on locks can be found in Regulatory Guide 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials."

1.3.2 Controls

Any controls or switches that are not used in the normal daily operation of the alarm system and that affect the sensitivity of the system need to be mounted inside tamper-protected enclosures. This applies not only to detector units but also to security equipment in the central and secondary alarm stations.

1.3.3 Environment

The user needs to be constantly aware of the environment to which the system will be exposed. Detector units can be adversely affected by a variety of environmental conditions, such as electromagnetic, acoustical, radioactive, thermal, optical, meteorological, and seismic energies. Once the user is aware of the potential environmental effects on the system, he can specify types of systems that are not adversely affected, or he can reduce adverse effects so that they no longer degrade the system.

Some of the environmental conditions to which the alarm system may be exposed are:

1.3.3.1 Thermal Energy - Changes in temperature of an enclosed area caused by heating and air-conditioning systems, sunlight and weather, heat-producing equipment or processes, and lighting can affect the performance of an alarm system in three possible ways:

1. By causing electromechanical or electronic components of the alarm system to operate outside the range in which they were designed to operate. In most user applications, this effect can be offset by specifying that all sub-units of the alarm system must operate properly between 0°C and 50°C.

2. By causing thermal expansion and contraction movements of building structures such as doors, windows, or walls that may be detected by the alarm detectors. This effect can be reduced by proper maintenance of the heating and air-conditioning system, shielding of thermal sources, or reorientation of detector sensors.

3. By causing unstable air convection currents in the secured area that can be detected by passive infrared sensors. This effect can be reduced by proper maintenance of the heating and air-conditioning system, shielding of thermal sources, and reorientation of the detector sensors.

1.3.3.2 Humidity - High relative humidity can affect an interior intrusion alarm system by causing condensation of water vapor to occur on electronic and electromechanical components of the system, possibly degrading the performance and reliability of the system. The potential user can reduce humidity effects by specifying that the system be able to perform at the humidity levels expected (for most applications specifying proper operation of the system at 85% relative humidity at 30°C will be adequate), by specifying that all components and circuit boards have a conformal coating that is water resistant, and by placing desiccants in all alarm system enclosures.

1.3.3.3 Acoustic Energy - Various forms of acoustic energy (air particles that have been set into motion at a frequency of the audio source to produce air pressure waves) can have an adverse effect on certain types of detector units, primarily ultrasonic detectors. Acoustic energy can be generated both inside and outside the secured area. As acoustic energy is reflected from structures within the secured area, standing wave patterns are produced. These standing wave patterns may cause the detector to be less sensitive to movement in some portions of the secured area. In addition, acoustical energy in the secured area either may be within the bandpass of detection for the sensor, thus generating false alarms, or may cause such a high noise level background in the area as to reduce the detector's sensitivity. Also, acoustic energy could cause thermal air currents within the secured area that might adversely affect some systems such as a passive infrared sensor.

The effects of acoustic energy can be reduced by identifying and shielding the source, by reducing the number of hard surfaces from which the acoustic energy can be reflected (taking care that sensitivity to intrusion is maintained), and by selectively filtering out unwanted frequencies at the sensor (taking care that sensitivity to intrusion is maintained).

Listed below are some of the more common sources of acoustic energy that can adversely affect some detector units (Ref. 1):

1. Noise from meteorological phenomena:
   a. Heavy thunder
   b. Nearby lightning strikes
   c. Heavy rain

d. Hail

e. Wind

2. Noise from ventilating, air-conditioning, and heating equipment:

   a. Fans and blowers

   b. Compressors and furnaces

   c. Water heaters

   d. Associated pumps

   e. Water and steam hammer in pipes

3. Noise from warnings or other acoustic alarms:

   a. Timing signals

   b. Emergency-vehicle sirens

   c. Base sirens

4. Noise from machinery:

   a. Rolling doors

   b. Conveyors

   c. Drills, lathes, and milling equipment

   d. Electric motors

5. Noise from television equipment:

   a. Scan and sync circuits

   b. Magnetic transformers

   c. Cathode ray tube (CRT) yokes

   d. Pan, tilt, and focusing motors

6. Noise from telephone electronic equipment:

   a. Switching equipment

   b. Telephone instruments

   c. Intercoms

7. Noise from exterior sources:

   a. Aircraft

   b. Vehicular traffic

   c. Trains.

1.3.3.4 Electromagnetic Energy - Various sources of electromagnetic energy can have adverse affects on some types of detector units, some of the more common sources being lightning, power lines, power distribution equipment, radio-frequency transmitters, telephone lines and equipment, lighting, computer and data processing equipment, electric-powered machinery and vehicles, automotive ignitions, airplanes, and intercom and paging equipment (Ref. 1).

Many electromagnetic disturbances that are generated outside the protected room or building may not be adequately shielded by construction materials used in the room or building, i.e.,

low-density materials such as glass, wood, plaster board, and cement. Adverse effects of stray electromagnetic energy can be reduced by ensuring that all electromagnetic-energy-producing equipment or units are properly shielded and connected to a solid common electrical ground. If these steps are taken and a detector unit continues to false alarm because of electromagetic energy, the energy is probably entering through the sensor transducer itself. This can be eliminated by incorporating a filter within the sensor transducer, taking care that the frequency passband for detecting an intruder is not adversely affected (Ref. 1). Another method is to shield as many of the interior intrusion alarm system components as possible from electromagnetic energy.

1.3.3.5 Radioactive Energy - Nuclear radiation can degrade or damage various components within the sensor, and semiconductors are the most susceptible elements. Research activities associated with various phases of weapon development have demonstrated that present-day detector systems cannot be made totally invulnerable to the effects produced in some radiation environments. These systems can be made less vulnerable, however, through design and choice of components. Neutrons cause a degradation in the performance of semiconductor devices and integrated circuits that is dependent on total dose. Alpha particles and beta particles are usually not of concern because alpha particles are readily shielded and because a radiation environment does not usually contain beta particles in significant quantity. Gamma rays and X-rays can cause sensor damage by two basic mechanisms: energy deposition and charge displacement that results in generation of undesirable electrical transients. The levels of gamma rays and X-rays required to produce serious effects, however, usually will not be found where an intrusion sensor is located, i.e., in areas occupied by humans (Ref. 1).

The first step in combating the effects of a radiation environment is to characterize the radiation in the environment according to information usually available from the health physics organization of the facility. The second step is to determine components in the detector system that may experience performance degradation in the environment and to identify more tolerant replacement components. Assistance in predicting the effects of radiation on performance can be requested from the component manufacturer or the system designer (Ref. 1).

In general, detector equipment should be installed in a location with a low radiation field if such a location that will allow effective use of the detector is available (Ref. 1).

1.3.3.6 Optical Energy - The sources of optical phenomena that affect interior intrusion sensors include light from the sun, interior lighting, light-reflecting surfaces, and equipment sources of infrared or ultraviolet energy. Detectors such as infrared and closed-circuit television systems are sensitive to incident or reflected light and its movement within the field of view of the lens. Other systems are affected by the heat generated by light focused either on them or on nearby objects. These adverse effects can be reduced by repositioning the affected units, eliminating reflective surfaces, and shielding sources of optical energy.

1.3.3.7 Seismic Energy - Sources of seismic energy include earth tremors, vehicular traffic, airplanes, trains, thunder, high winds, and machine equipment. This energy can cause both

structural movement and movement of furnishings and equipment that would be detected by the alarm system. This effect can be reduced by repositioning the sensors to view a stable background, by shock-mounting the alarm sensors, and by securely fastening or storing objects that might easily be moved.

1.3.4 Safety

Safety standards for the construction of alarm equipment is included in Reference 2. By requiring that all alarm equipment meet the requirements of this standard, the potential user is assured of a safe system.

In addition, the National Electrical Code gives installation requirements applicable to running cables and wire through damp locations. Wire insulation can be specified to pass flame resistance tests of either Underwriters Laboratories Standard UL-83 (Ref 3) or the Insulated Power Cable Engineer Association standard IPCEA S-19-81 (Ref. 4).

1.3.5 Design

Each secured area should be designed with one or more separate alarm circuits that will annunciate independently of any other alarm systems and that will uniquely identify the secured area where the alarm has occurred. All signal lines between the detectors and the premises control unit for the secured area should meet the recommendations given in Sections 3.1, 3.2, and 3.5.1.

All interconnecting alarm wires or cables within buildings in the protected area should be installed in cable trays or conduit. When installed in cable trays, it is recommended that the security wires or cables have no readily decipherable markings to identify them from nonsecurity wires and cables and that some nonsecurity wires or cables be included in the same tray. All interconnecting wires or cables located in an outside environment should be protected by line supervisory units. Installation of the wires or cables in rigid steel conduit or covered cable trays if exposed and PVC/rigid-steel conduit if buried provides significant additional protection. Locating all interconnecting cables at least 3 meters (10 feet) inside the perimeter of the protected area will also reduce the threat of attack by an outsider.

1.3.6 Circuit Supervision

In order for security personnel to have confidence in an interior alarm system, they must have continuous assurance that the system is functioning properly. Some manufacturers of detector units provide self-checking circuitry or circuit supervision that will generate an alarm when the detector unit becomes insensitive to intrusion. For volumetric detectors this usually takes the form of monitoring certain key electrical circuits in the transmitter and receiver portion of the unit for proper signal levels. Fluctuations of the signal level outside prescribed limits will cause an alarm signal to be generated. In addition, the alarm relay in the detector is usually energized in the nonalarm state so that loss of both primary and standby power will

cause an alarm. For passive detector units (e.g., infrared) each detector head can be automatically checked in a random manner by turning on an alarm-initiating source at the sensor head (approximately once every 30 minutes) and verifying that this alarm source is detected at the control unit. (During the automatic test the alarm relay is bypassed unless a system malfunction is detected.) Again, the alarm relay in passive detectors is normally energized in the nonalarm state so that loss of power will cause an alarm. In the event a detector circuit does not come equipped with self-checking circuitry, the security force can verify its operability by remote testing or walk-testing the system daily. Line supervisory circuits are automatically self-checking since loss of signal on the transmission lines will generate an alarm. Annunciator units may be checked manually to verify their operability.

2. DETECTOR UNITS

Detector units are designed to respond to either changes to the environment in which they operate (e.g., ambient light, heat, or sound levels within the secured area or the opening or penetration of doors, windows, skylights, walls, or gates) or changes in an environment that they produce (e.g., ultrasonic or microwave energy generated by the detectors). The former design forms are referred to as passive detector units and the latter as active* detector units. Detector units are usually categorized by the geometry of protection they provide - volume protection or surface protection. Within each category can be found both active and passive detectors. This report will group detector units according to the geometry of protection they afford.

A detector should initiate an alarm signal under any of the following conditions: (1) when it senses a stimulus or condition to which it was designed to react; (2) when primary power fails and secondary power does not take over properly; (3) when the detector's component circuitry is opened, shorted, or grounded or has failed or aged to the extent that the device's normal operation is compromised; and (4) when a tamper switch or triggering mechanism is activated. All detector terminals should be located within the detector's enclosure.

2.1 VOLUMETRIC DETECTOR UNITS

Volume (or space) protection systems are sensitive to the motion or presence of individuals within a specified volume. For the protection of rooms and large volumes, volumetric protection systems generally offer a higher degree of security than do surface protection systems. Various physical phenomena are employed in order to provide volumetric detection. The first two systems discussed below are considered active volumetric detectors and the next two systems are considered passive volumetric detectors. Volumetric detector units that are installed and operated in such a manner that intrusion by a small individual into the secured area at all rates between 6 and 180 meters (20 and 600 feet) per minute and in various walking postures is detected within 1.5 meters (5 feet) from any direction offer a high degree of security.

2.1.1 Ultrasonic Motion Detector Units

2.1.1.1 Theory - Ultrasonic detectors consist of one or more transmitter and receiver elements and the necessary control circuitry. They are considered a line-of-sight device unless system enhancement features are employed. Some systems combine the transmitter and receiver into a single unit called a transceiver.

---

* The "active" intrusion alarm system required by paragraph (c)(4) of 10 CFR K 73.50 and paragraph (d)(7) of 10 CFR K 73.55 means a system that is turned on and operating properly, and thus these regulations do not prohibit the use of passive detector units.

An ultrasonic motion detector utilizes the Doppler principle (changes in the frequency of the received signal caused by movement) in detecting motion within a specified volume. The volume to be protected is virtually flooded with ultrasonic energy of a specified frequency, usually between 18 and 40 kHz - just above the typical range of human hearing. Motion within the volume both alters the distribution of ultrasonic energy within the volume and generates shifts in the frequency of the ultrasonic energy reflected back to the receiver. The receiver units sense the ultrasonic energy within the volume, and the electronics compare the received frequency with the transmitted frequency by either envelope detection of the combined signals or frequency difference of the two signals. A shift in the received frequency beyond a preset threshold from the transmitted frequency initiates an alarm signal.

2.1.1.2 Operational Considerations - Because ultrasonic detectors utilize the air within the secured volume as the medium to propagate the ultrasonic waves, any air turbulence within this volume reduces the sensitivity and lessens the effectiveness of the system. Since vibration of the acoustic transducers themselves is detrimental to their proper operation, they need to be rigidly mounted on vibration-free surfaces. Locating transducers near air ducts, fans, and loose fitting doors and windows is also detrimental to the operation of the system. In addition, high-pitched noise such as that generated by telephone bells, steam pipes, radiator valves, and electric motors tends to reduce the sensitivity of the system and may generate nuisance alarms. Ultrasonic detectors thus are susceptible to false alarms caused by acoustic, meteorological, and seismic energies.

Acoustic waves in the ultrasonic regions are more directional than audible sound but will still diffuse. This diffusion, assisted by reflection from hard surface walls and fixed objects within the volume, will tend to fill the entire volume with acoustic waves. It should be noted, however, that multiple competing reflections may render some points within the protected volume relatively insensitive to motion. Further, high absorbency of certain types of walls or objects (e.g., curtains) within the volume may tend to lessen sensitivity. Other objects may block or reflect the ultrasonic energy, thus producing "shadow" areas where the ability to detect motion is marginal or nonexistent. In such situations, relocation of transducers or provision of additional transducers may be necessary to provide adequate coverage.

For ultrasonic detectors that combine the transmitter and receiver units into a single monostatic unit, proper placement of the transceiver is all important in obtaining optimum operation. Transceivers typically provide an egg-shaped volume of coverage that tends to decrease in size as air turbulence and the number of transceivers connected to the signal processor increase. The number of transceivers required to cover a given area or number of rooms can be determined from the graphs in Figure 2, which relate the typical maximum range for each transceiver to the number of transceivers in the system and levels of background turbulence (Ref. 1).

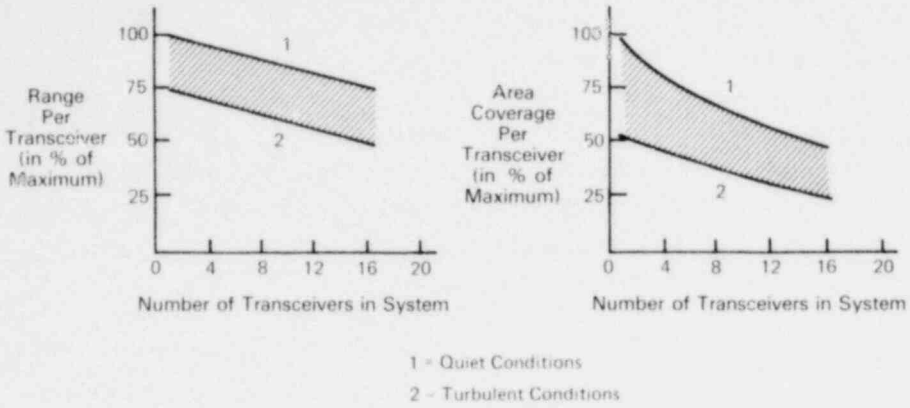

FIGURE 2. SHRINKAGE OF TRANSCEIVER COVERAGE WITH MULTIPLE TRANSCEIVERS (Ref. 1)

In order to obtain the maximum Doppler signal, ultrasonic transceivers need to be located so that the most likely intruder movements are either toward or away from the transceiver rather than perpendicular to the transceiver. When more than one transceiver is required to protect an area, they should be positioned so that they all face in the same general direction and thus reinforce one another. When two transceivers are used to protect a hallway, one transceiver should be placed at one end of the hallway facing the other end and the second transceiver should be placed midway in the hallway also facing the far end. When the hallway is over 30 meters (100 feet) long, the transceivers may be placed facing one another. For optimum results, place all ultrasonic transducers no higher than 2.5 meters (8 feet) above the floor.

Commercially produced ultrasonic detectors may not incorporate circuit supervision in the transmitter and receiver portions of the control unit. For this reason, it is recommended that, wherever ultrasonic units are installed, they be walk-tested at least daily or have a remote test capability. Some commercial systems are designed so that each transceiver can be independently tested to determine its operability without affecting other transceivers in the circuit. Thus proper sensitivity to intrusion can be easily determined for the area of coverage of each transceiver. Proper sensitivity for an ultrasonic detector would be detection of a small individual moving anywhere in the secured area at any velocity between 6 and 180 meters (20 and 600 feet) per minute in any position and direction.

In the access mode of operation, most ultrasonic transceivers or transmitter/receiver elements lend themselves to tampering. For this reason, it is strongly recommended that all ultrasonic transmitter/receiver elements be walk-tested just prior to placing the system in the secure mode of operation.

2.1.2 Microwave Motion Detector Units

2.1.2.1 Theory - An interior microwave motion detector is usually a monostatic unit consisting of a transmitter and receiver antenna housed in the same enclosure as the control circuitry.* Generally a microwave motion detector is a line-of-sight device unless extra system enhancement features are employed.

Like an ultrasonic motion detector, a microwave motion detector utilizes the Doppler principle for detecting human motion within a specified volume. The majority of these systems transmit a microwave signal of either 10.525 GHz or 915 MHz that is modulated at a frequency in the 10-30 kHz range. Microwave energy is much more directional than ultrasonic energy, and most units have an egg-shaped antenna pattern. This pattern can be varied somewhat to meet environmental constraints of the protected area by using various antennas and metallic microwave reflectors. Motion within the protected volume results in a Doppler shift in frequency of the microwave energy reflected from the moving body. The receiving antenna senses the microwave energy within the secured area, and the control circuitry electronically compares the received frequency with the transmitted frequency by either envelope detection of the combined signals or frequency difference of the two signals. If the received frequency is shifted above or below a preset level, an alarm signal is generated.

The purpose of modulating the microwave beam is to provide circuit supervision over the transmitter and receiver portions of the circuitry. The transmitted modulated microwave beam is reflected back to the receiver where it is detected and amplified. Somewhere in the first few stages of amplification (varying with the manufacturer), the modulated signal is detected. Loss of this signal due to tampering or system malfunction causes an alarm signal to be generated.

2.1.2.2 Operational Considerations - Depending on the frequency, the electromagnetic radiation produced by most microwave transmitters will penetrate construction materials comprising most interior partitions (e.g., glass, plastic, sheetrock, plywood, and wood paneling), and nuisance alarms caused by movement beyond such partitions may occur. However, walls made of such materials as concrete, masonry, and metal generally will attenuate or reflect the microwaves to the extent that movement beyond such walls will not be detected. Thus, an important consideration when locating a microwave motion detector system is the penetrability of the walls toward which the transmitter is aimed.

Microwaves are more highly directional and do not diffuse as much as ultrasonic waves. Each unit has a definite coverage pattern, and the location of microwave units is governed by these coverage patterns and the reflection of microwave energy from metallic objects located in the secured area. Microwave shadows occurring behind metallic objects may require installation of extra detectors. If effective coverage demands that the transmitter be aimed at a penetrable wall, detection of motion beyond the wall can be avoided by facing the wall (either side) with

*Bistatic microwave detectors are discussed in Regulatory Guide 5.44, "Perimeter Intrusion Alarm Systems."

an electrically grounded wire mesh screen. The largest dimension of the mesh should be less than 1/4 the wavelength of the transmitted microwave energy (approximately 5 to 50 mm).

Microwave detectors are generally more sensitive to small movements than are ultrasonic detectors. Air turbulence has no effect on a microwave system, provided the microwave beam is not directed at any object that could be moved by the air turbulence.

Small motions of metallic objects such as hanging signs, venetian blinds, and fans that may not present problems with an ultrasonic system will generate nuisance alarms in a microwave system. If such objects cannot be secured or removed from the beam of the transmitter it may be necessary to shield them with a grounded metal screen. Electromagnetic energy, primarily fluorescent lighting, will also interfere with the effective operation of a microwave system unless the system has been designed with a bandpass filter to compensate for such interference.

Microwave motion detector units can be quite effective in protecting long narrow volumes such as hallways because their antennas can be selected to provide the ideal pattern for the area. When several microwave detector units are to be used for protecting large volumes such as warehouses, it is recommended that each unit be purchased to transmit at a slightly different frequency from the others in order to prevent false alarms due to crosstalk. For most environments, microwave units that are mounted approximately 2 to 3 meters (7 to 10 feet) above the floor and at least 1.5 meters (5 feet) from fluorescent lighting provide optimum results.

When properly installed, a good microwave system will detect the movement of a small human being moving in any direction anywhere in the secured area at a rate between 6 and 180 meters (20 and 600 feet) per minute within 1.5 meters (5 feet) and while the human is in any position. Because microwave detectors are more highly directional than are ultrasonic motion detectors, they sometimes can be bypassed by redirecting the antenna away from the sensitive area while the system is in the access mode of operation. For this reason, it is recommended that the more sensitive areas in the secured area be walk-tested when switching from the access to the secure mode of operation.

2.1.3 Passive Infrared Detector Units

2.1.3.1 Theory - A passive infrared (IR) detector unit generally consists of a control unit and several infrared sensors called heads. Passive IR detectors are motion detectors, and for the most part are line-of-sight devices. The system detects movement within the volume protected by sensing the change in the heat pattern falling upon the detector head.

All objects emit various degrees of thermal (IR) radiation. The amount of radiation they emit depends on the object's temperature and emissivity constant. A passive IR detector senses and stabilizes on the IR radiation being emitted by the different objects in the secured area. The field of view for most IR heads covers an angle varying from 5° or 10° to 70° wide at an average range of 9 meters (30 feet). As an individual moves within the field of view of a particular head, the heat pattern falling upon the sensor head is changed, and the sensor head responds by either generating a current or modulating a carrier current. An array of thermal

junctions (of alternate polarity) located in the sensor head generates an undulating current when the junctions are heated and cooled as the infrared image focused upon the array changes size or shape or moves across the array.

A second type of IR system utilizes a ferroelectric bolometer and reticle to chop the IR image, thus allowing the bolometer to be alternately heated and cooled as the IR image changes size or shape or moves. The resultant variation in the temperature of the bolometer causes a variation of the dielectric constant of the bolometer. A carrier current passed through the bolometer will be modulated by the variation in the bolometer dielectric constant. When the degree of modulation exceeds a preset threshold, an alarm results. With both types of systems the sensitivity of detection is greater for movement perpendicular to the field of view of the head than for movement toward or away from the head (opposite to the sensitivity parameters of ultrasonic or microwave detectors.)

A certain degree of circuit supervision can be provided for passive IR detector units by having a light emitting diode at each head turn on for approximately 1 minute about every 30 minutes in a random manner. IR radiation provided by the light emitting diode causes the head to generate an alarm. During this test, all circuits are tested except for the alarm relay in the control unit which is momentarily locked out of the circuit to prevent nuisance alarms. If other IR heads are located in the same secured area, the degree of security for that area will not be significantly reduced while one head is momentarily being tested provided each head is tested in a random and independent manner.

2.1.3.2 Operational Considerations - Passive optical IR detectors generally work well in an environment where there are small amounts of movement occurring and where large air currents may exist, such as in a warehouse. Once the optical IR detector adjusts to the amount of IR radiation being emitted from the surrounding environment, it is sensitive to any sudden changes in emitted IR radiation. Small movements in the environment, such as an overhanging metal door moving with the wind, will go undetected. However, a body that has more than a 0.5°C temperature differential placed between the detector and the background upon which it is focused will be detected. Since the amount of IR irradiation varies from wall to wall to floor to ceiling, it is almost impossible to build a shield at ambient temperature that could mask a moving intruder provided the detector heads are properly positioned. Painting the walls alternately with a dark and light color will reduce this possibility even further. Passive IR detectors, however, are line-of-sight devices and hence any equipment within their secured volume may cause IR shadow areas. In addition, positioning the sensor head such that it looks directly at intermittent sources of heat such as radiators, heating/cooling ducts, or ventilators can cause nuisance alarms.

Passive IR detectors will automatically adjust to any changes in their environment and therefore work well in environments that may change frequently (e.g., a warehouse that is full one day and empty the next day). Ultrasonic and microwave systems must be readjusted manually each time the environment changes significantly in order to provide constant sensitivity to intrusion. (However, since passive IR detectors are line-of-sight devices, changes to the

environment may require additional IR heads in order to obtain adequate coverage.) Most building materials, including glass, block out outside IR radiation because of the wavelength of IR, so that false alarms due to outside sources are effectively eliminated.

Passive IR detector units are not affected by fluorescent lamps, but incandescent lamps located within 0.6 meter (2 feet) of a detector head may cause false alarms.

Some basic do's and don'ts in using passive IR systems are (Ref. 1):

1. Do keep the lens on the heads clean of dust. Dusty environments may prohibit use of a passive IR system.

2. Don't use a passive IR system in an environment where insects swarm around lights or small rodents run around, since they may cause nuisance alarms.

3. Do place the IR sensor head so that the most likely path for an intruder will be across the field of coverage rather than into it or away from it.

4. Don't place the sensor over a portal (e.g., door, window, etc.) that would allow the intruder to approach the sensor head from the rear.

5. Don't place the sensor head near or aim it toward radiant heaters with exposed radiant elements.

6. Do try to place the passive IR detector units in areas containing backgrounds of various emissivities.

7. Don't place an IR sensor head in a location where direct sunlight might impact it and cause nuisance alarms to occur.

When properly positioned and in the proper environment, a good IR detector system will:

1. Detect a small individual moving at a rate of 0.3 meter (1 foot) per second or faster anywhere in the secured area.

2. Stabilize within 2 minutes after turn-on and be incapable of defeat by IR absorbent or reflective material placed between the intruder and IR heads.

3. Not false alarm if visible light strikes the IR head.

4. Not be susceptible to changes in temperature due to the heating or air-conditioning system being turned on or off.

An IR detector system can be easily bypassed while the system is in the access mode. For this reason it is recommended that the area be walk-tested prior to securing and that systems with self-test circuitry be purchased.

2.1.4 Closed-Circuit Television Motion Detector

2.1.4.1 Theory - The closed-circuit television (CCTV) motion detector couples a conventional CCTV system to an electronic processor that detects changes in gray contrast from one raster display to the next, such as would be caused by a moving intruder. Some systems allow the viewed scene to be divided into separately alarmed areas so that motion in one portion of the scene viewed by the camera will not trigger an alarm, but motion in another portion will. The area and depth of the volume protected is dependent on the lenses attached to the camera and therefore can be varied over a wide range.

In some CCTV motion detection systems, the electronic processor is incorporated into a TV monitor and requires one monitor per zone. In other systems the electronic processor is a separate unit that can monitor several zones at one time. In the event of an alarm, the zone that goes into alarm is switched automatically to a TV monitor. This system also allows the monitor operators to manually, automatically, or permanently switch the different zones onto TV monitors.

2.1.4.2 Operational Considerations - Changes in light contrast either in the viewed area or reflected into the viewed area can generate nuisance alarms in CCTV systems. Therefore, careful positioning of the CCTV camera or shielding of reflective surfaces may be necessary so that the camera's field of view does not encompass any reflective surface that would reflect movement occurring elsewhere.

A second source of nuisance alarms occurs when electromagnetic energy is coupled into the coaxial cables between the camera and video processor. When installing a CCTV alarm detector in an area with high electromagnetic interference, all coaxial signal lines may need to be run in electrically grounded conduit.

A common problem encountered when assembling a CCTV system is impedance mismatch between equipment and signal lines, which causes ghosts at the monitor. The industry standard for input and output equipment is 75 ohms, to which the user should closely adhere when ordering equipment.

Sensitivity to motion can be increased if objects and walls viewed by the camera are painted in contrasting colors. Sensitivity to motion decreases if the CCTV camera being used has an antimony trisulfide vidicon and is left in a fixed position for long periods of time. The viewed scene eventually burns its image onto the vidicon's faceplate, which reduces the camera's sensitivity to light changes. (Further information on CCTV systems is provided in Reference 5.)

A CCTV alarm system provides the capability of instantaneous assessment by the security force in the event of an alarm. Because of the instantaneous assessment capability, CCTV alarm

systems can have a higher false alarm rate than other intrusion alarm systems and still be effective. CCTV alarm systems also afford the security force the opportunity to randomly survey the secured area in either the secure or access mode in order to detect the unauthorized presence of individuals or violations of security procedures. Incidents occurring within the camera's field of view can be tape recorded for later use as evidence or information.

CCTV motion detectors that will detect motion when the images between frames vary by less than 1% are commercially available. This high degree of sensitivity may prevent the user from obtaining reliable operation. Other commercially available systems require a 12% change in gray contrast between frames before alarming. For most interior alarm uses, a 6-8% change in gray before alarming will provide high sensitivity with a low nuisance alarm rate. CCTV detectors can be bypassed while in the access mode either by repositioning the camera so that a portion of the secured area is not in the camera's field of view or by capping the lens of the TV camera. Periodic monitoring of the area at the central alarm station to determine whether the camera's field of view encompasses the sensitive area will verify the TV system's operability. However, only periodic walk-testing of the secured area or remote testing will verify the operability of the detection circuit.

Because the cameras of a CCTV motion detector will probably be mounted in a fixed position (motion of the camera will cause alarms), they can be protected against surreptitious repositioning with tamper switches.

2.2 SURFACE PROTECTION

Surface protection devices detect penetration of the boundary of a secured volume rather than the presence or motion of an intruder within the secured volume. Surface protection devices are commonly used to detect the opening of doors and security cabinet drawers (portal-type detectors) or the attempted penetration of walls. Surface protection devices generally do not offer as high a degree of security as do volume protection detectors and therefore are often used to complement volume protection detectors.

2.2.1 Balanced Magnetic Switch

2.2.1.1 Theory - The balanced magnetic switch is a device commonly used to protect against illegal openings of doors, windows, or other types of portals. The Justice Department (Ref. 6) has defined a balanced magnetic switch as follows: "A magnetic switch that will go to the alarm state on sensing a magnetic field larger or smaller than that which maintains the switch in its secure state." It consists of two units: a magnetic reed switch, a bias magnet, and a tamper switch in a nonferrous housing and a permanent bar magnet also in a nonferrous housing. Because it requires no input wiring, the magnet is mounted to the movable part of the opening and the magnetic switch to the frame. Separation of the reed switch from the magnet causes the reed to relax and shift from one set of contacts to another, thereby initiating an alarm. In addition, the reed is balanced against the magnet so that attempts to capture the reed by use of extraneous magnets causes the reed to shift contacts, again generating an alarm. The balanced magnetic switch has proven to be one of the most reliable and inexpensive of all sensors.

2.2.1.2 Operational Considerations - Balanced magnetic switches are designed to detect portal openings or closings, but will not detect someone penetrating the secured area through a hole in the wall or portal. To provide adequate security for a room, it may therefore be necessary to use other appropriate volume and surface detectors along with balanced magnetic switches. To secure an area that offers a high degree of resistance to penetration attempts, such as vaults, the use of a balanced magnetic switch on the doors and windows may prove adequate.

When installing the balanced magnetic switch on a door, the switch and magnet need to be mounted approximately 5 cm (2 inches) from the door edge opposite the hinge. The magnet is mounted to the door with the switch mechanism mounted to the frame. The switch and magnet must be mounted with the proper space gap between them as recommended by the manufacturer (usually between 1.27 and 3.8 cm (0.5 and 1.5 inches)). Balanced magnetic switches may cause nuisance alarms if attached to portals that are not securely fastened and vibrate or move with the wind. Mounting balanced magnetic switches on large metal doors may require that non-ferrous standoffs be used for mounting the magnet and switch to the door to prevent the metal door from capturing the magnetic field and thus preventing the switch from setting up properly.

The contacts of the reed switch of a balanced magnetic switch may be welded together by high current surges caused by voltage surges or lightning. Over a long period of time, the permanent bar magnet's field strength may deteriorate, making the switch more susceptible to nuisance alarms. The balanced magnetic switch can be bypassed easily by:

1. Immobilizing the reed switch in some manner,

2. Electrically shorting, opening, or placing a resistance across the signal lines to the switch, depending on the line supervision method used, or

3. Circumventing the switch itself by cutting a hole through the portal, moving the portal and frame together, or moving the pivot point of the portal so that the switch does not travel far enough to generate an alarm.

These bypass techniques can be countered easily by periodic testing of the switch, using a sensitive line supervisory system on the signal lines, routing all signal lines in conduit, requiring and monitoring a tamper switch in the reed switch housing, installing portals that provide high resistance to penetration, and hinging all portals inside the secured area. A good and properly installed balanced magnetic switch will initiate an alarm upon increase or decrease in the size of the magnetic field that maintains the switch in its secure state, attempted substitution of an external magnetic field, or sudden current surge when the switch is in the normally secured mode. A balanced magnetic switch is rated for a minimum of 500,000 activations without malfunction.

2.2.2 Infrared Beam

2.2.2.1 Theory - An infrared (IR) beam detector system usually consists of two main units: an IR transmitter and receiver. The IR transmitter emits a beam of IR light, invisible to the

human eye, to the receiver. This beam of light may be either coherent, as a laser beam, or noncoherent, as a flashlight beam, and has a cylindrical shape that is usually not much larger in diameter than the diameter of the lens. In either coherency type, direct line of sight is required between the transmitter and receiver. Interruption of the beam for more than 75 milliseconds should cause an alarm signal to be generated at the receiver.

The basic system can be configured in several ways to extend the area of coverage. The beam can be bent around a corner through the use of a mirror or a transceiver. A mirror is not recommended in most instances since between 40 and 60% of the energy is lost in reflecting the beam. Also, the system is subject to false alarms if the mirror becomes fogged or dusty. A transceiver, however, can receive the transmitted beam, amplify the signal, and retransmit and refocus the beam toward the end receiver.

Multiple transmitting and receiving IR units that can be used to define a wall of IR protection are also available.

2.2.2.2 Operational Considerations - IR beam systems can be defeated by capturing the transmitted IR beam with a clandestine IR transmitter and then walking through the captured beam undetected or by determining the location of the beam(s) and then crawling under or stepping over it. IR systems that pulse modulate the transmitted IR beam generally offer a high degree of resistance to capture, consume less power, increase the system's lifetime, and decrease the system's susceptibility to nuisance alarms caused by extraneous light such as sunlight impacting the receiver's lens. Defeat of the system by bypassing the IR beam can be greatly reduced by using multiple beams camouflaging the location of the IR transmitter and receiver, and, for interior uses, placing it close to the barrier it is protecting.

As an interior alarm system, IR systems are most advantageously used to provide surface protection at the perimeter of the area, i.e., for walls, doors, and windows. Reliability and security can be enhanced by rigidly mounting the system as close to the barrier as possible and camouflaging its location. In addition, if the perimeter of a secured area is to be protected by an IR system, IR beams should overlap at the corners.

There are several disadvantages to using an IR detector indoors. These include:

1. A small isolation zone, free of obstruction, has to be maintained to allow the system line-of-sight operation and thus reduce nuisance alarms.

2. Multiple IR beams need to be used to form an IR barrier to protect against an intruder crawling under or jumping over a single beam.

3. Although the IR system generally is not affected by interior environmental conditions, accumulation of dust or dirt on the lenses, faceplates, and mirrors of the system will decrease sensitivity.

2.2.3 Capacitance Detector

2.2.3.1 Theory - The capacitance detector consists of a control unit containing circuitry designed to detect the change in capacitive coupling that exists between one or more antennas (safes, filing cabinets, etc.) and electrical ground. These antennas are energized by an electromagnetic field, the frequency of which is controlled by the capacitance between the antenna and ground. An intruder's dielectric increases the capacitance between the antenna and ground which in turn reduces the frequency of the field. This change in frequency is what is detected and used to generate an alarm signal.

Most good capacitance detector systems are designed to reject the very slow changes in the antenna-to-ground capacitance caused by changes in temperature and humidity.

2.2.3.2 Operational Considerations - Although usually employed to protect individual objects such as safes and filing cabinets, capacitive detectors can be used for protection of all conductive surfaces that are electrically insulated from earth ground. A room can be protected by covering the walls and ceiling with a coarse wire mesh (insulated) which acts as an antenna for the device. Windows, vents and other openings can also be protected by means of a capacitance detector attached to an insulated conductive grill or screen that covers the opening.

The capacitance detector requires good insulation of the antenna from earth ground and a good earth ground of the control unit (e.g., a cold-water pipe) for effective operation. A capacitive detector is not recommended for use in those parts of the country where the earth ground varies during the year because of fluctuations in the level of ground conductivity caused by changes in ground moisture. Because the principle of detection is based upon the change in capacitive coupling between the antenna and ground when approached by an intruder, an electrically grounded mat or foil that is electrically isolated from the antenna may have to be placed on a nonconductive floor around the antenna in order to provide a good ground reference plane. Nuisance alarms can be generated by electromagnetic disturbances in nearby environments and by failing to establish or maintain good isolation between the antennas and ground. In relation to the latter, cleaning personnel need to be careful when mopping floors. Water that may collect under safes and security cabinets can short the antennas to ground and cause nuisance alarms. Good antenna isolation from electrical ground can be obtained by placing the antennas 7.5 to 10 cm (3 to 4 inches) off the floor on nonabsorbing materials such as phenolic glass, hockey pucks, or plastic.

When properly installed and adjusted, a capacitive detector should be able to detect an intruder moving within 15 cm (6 inches) of the antenna or an intruder touching an antenna while wearing a heavy insulated glove.

2.2.4 Electric-Field Sensor

Although an electric-field (E-field) sensor is basically an exterior alarm system, it does have limited application as an interior alarm system.

2.2.4.1 Theory - An E-field sensor consists basically of a field generator that excites a field wire with an alternating current, one or more sensing wires, a sensing filter, an amplifier, and a discriminator and annunciator unit. The field wire transmits essentially on omnidirectional E-field to ground. A large body approaching the system changes the pattern of this E-field. Sensing wires placed at different locations within the transmitted E-field pattern pick up any changes occurring in that pattern when an intruder enters the field. If the changes are within the bandpass of human movement, an alarm signal is generated.

2.2.4.2 Operational Considerations - An E-field sensor is readily adaptable for providing protection to a series of windows in a large building such as a warehouse. By placing the field wire and two sensing wires on standoffs on the side of the building so that the sensing wires are at the top and bottom of the windows with the field wire running between, complete protection can be provided for up to 91 meters (300 feet) of windows. When used for this purpose the field and sensing wires should be placed a minimum of 46 cm (18 inches) from the wall's surface.

Since the field and sensing wires can act as antennas, the system may be subject to false alarm when placed in an environment subject to external electrical interference (e.g., lightning). Also, both the field and sensing wires need to be under a high degree of spring tension so that high-frequency vibrations will be produced when they are struck by small foreign objects or blown by the wind, such vibrations being out of the alarm passband of the receiving circuitry. In addition, in order to keep the sensitivity of the system from varying, the E-field detector needs to be well grounded. Isolators used for supporting the wires and preventing electrical loading of them to the support posts should have large holes drilled through them to allow the wires freedom of movement during high winds.

The following performance specifications are appropriate for E-field sensors :

1. The system alarms when approached to within 1 meter (3 feet) by a test person approaching at a normal rate. When slowly approached, the system should alarm within 25 cm (10 inches) of the wires.

2. The system should be equipped with a remote self-test feature. This can be accomplished by connecting each sensing wire to ground through a 100-pF capacitor and a remotely activated relay.

3. For safety considerations, all field and sensing wires should be installed with lightning arrestors.

2.2.5 Breakwire

2.2.5.1 Theory - A breakwire detection system consists of a thin copper wire with electric current flowing through it and a simple current-sensing control unit attached on it. The sensing current can be the same as the line supervisory current used between the central alarm station and the secured area. The thin wire is placed inside a barrier (e.g., door, wall, screen) in

such a configuration that any type of forcible penetration through the barrier will break the wire and generate an alarm signal.

2.2.5.2 Operational Considerations - A breakwire detection system is intended to be used in screens and grids, open wiring, wooden dowels, doors, walls, and grooved stripping in various arrays and configurations. Its purpose is to detect surreptitious and forcible penetrations through movable openings, floors, walls, ceilings, and skylights.

These sensors can be easily bypassed, without detection, by short circuiting large portions of the protected barrier out of the system. However, once installed, the system rarely suffers from false or nuisance alarms, is an economical and highly reliable system to maintain, and does provide a certain level of protection against forcible entry.

The wire used in a breakwire system should not be larger than 24 AWG, should not exceed 4 pounds in tensile strength, and should be capable of carrying a current of 60 milliamperes with a temperature rise of not more than 1°C.

3. LINE SUPERVISORY UNITS

In order for the detector units to be of value to the security force, a means of transmitting their security status back to the central alarm station and secondary alarm station needs to be provided. If this transmission link is compromised either intentionally or accidentally without alerting the alarm stations, the detection capability of the detector unit is of little value. Transmission links used for transmitting the detector's security status can be categorized as either supervisory or nonsupervisory.

Nonsupervisory links transmit a signal back to the central alarm station only when an alarm occurs. Therefore, unless the system is frequently tested, the alarm stations can never be assured that the transmission link has not been compromised and is still operating properly. Nonsupervisory systems may use either hard wire or free space (microwave) to transmit data to the alarm stations. Microwave nonsupervisory units are often used by facilities when the secured area is far away from the alarm stations and when there are insufficient telephone lines available for transmitting alarm signals. When used in these environments, it is recommended that the transmitter be physically protected and hidden and that a means of remotely testing the system from the central alarm station be provided.

For most nuclear industry applications, a supervisory transmission link is required. Supervisory links continually transmit a signal back to the alarm stations, and are therefore readily able to detect breaks in the transmission link. Since distances between the central alarm station and the most remote secured area at a nuclear facility are relatively small, hard wire transmission links are usually used. This section will address primarily the various types of line supervisory transmission links.

3.1 A.C. AND D.C. SYSTEMS

D.C. line supervisory systems represent the oldest type of line supervision. The system operates by maintaining a constant d.c. current on the signal lines at all times. The level of current on the lines is determined by adjusting the current-limiting resistor in the line supervisory unit and the end-of-line resistor at the detector unit. An alarm signal is generated if the signal line is short-circuited or opened or if the current level on the line varies beyond a certain tolerance.

This current tolerance is a percentage of current change from the normal current and varies (depending on manufacturer) between 5 and 50%. The more sensitive units (5 to 10%) are called high line supervisory units.

D.C. line supervisory units are limited as to the length of signal line, which is directly proportional to line resistance, that they can monitor. D.C. systems may suffer from nuisance alarms caused by electromagnetic interference and such environmental effects as changes in

temperature and humidity that can vary the normal current beyond the chosen tolerance level. In addition, d.c. systems are relatively easy to bypass.

A.C. systems are a natural extension of d.c. systems with the end-of-line resistor replaced with a complex impedance and an a.c. signal maintained on the signal lines. Again, an alarm signal is generated if the signal lines are short-circuited or opened or if the a.c. signal's amplitude or phase varies beyond a predetermined tolerance.

A.C. systems suffer from the same drawbacks as d.c. systems, but it generally requires more sophisticated electronics to compromise them.

For most security operations it is recommended that a.c. or d.c. line supervisory units provide an alarm response at the annunciator in no more than 1 second as a result of (Ref. 7):

1. 5% or greater change in normal line current when it consists of direct current from 0.5 milliamperes to 30 milliamperes,

2. 10% or greater change in normal line current when it consists of direct current from 10 microamperes to 0.5 milliamperes,

3. 5% or greater change of any component(s) (a.c. or d.c. voltage or current, a.c. phase, or frequency duration) in a complex signal upon which the security integrity of the system is dependent (for frequencies up to 100 Hz), or

4. 15% or greater change of any component(s) (a.c. or d.c. voltage or current, a.c. phase, or frequency duration) in a complex signal upon which the security integrity of the system is dependent (for frequencies above 100 Hz).

3.2 DIGITAL SYSTEMS

More recent developments in line supervision use digital techniques for transmitting security data. Most digital systems code and modulate the information before transmitting it. This technique makes it very difficult for an untrained observer to determine the status of the detector units.

In the basic layout of a digital system, the alarm output from the detector unit is connected via a d.c. or a.c. line supervisory technique to a remote data gathering unit that converts the security status of the detector unit into a digital format. This digital signal is then transmitted over telephone lines to the central alarm station, where it is detected. Many digital systems gather data from several sensors at remote sites and transmit the data via a single telephone line using time division multiplexing techniques. With this technique, data from each remote site are transmitted during a particular time slot in each block of data. This technique makes it more difficult for an intruder to determine the status of a particular sensor unit unless he is familiar with the exact multiplexing format used. A more sophisticated intruder can record the signals on the line, no matter what type of coding, modulation, or multiplexing

scheme is used, during periods he believes all detectors are in the nonalarm status and then play them back later during an intrusion attempt.

Some digital systems have countered this playback threat by varying the nonalarm system with time. This also makes it more difficult for the intruder to determine the format of the nonalarm signal and then to generate and substitute bogus signals. Further information on the various digital coding techniques being used is included in Reference 1.

Some advantages of a digital line supervisory system over an a.c.or d.c. system include:

1. The system is not as susceptible to nuisance alarms caused by electromagnetic interference.

2. Most digital systems are capable of supervising long lengths of signal lines.

3. Temperature and humidity do not have as adverse an effect on digital systems as they do on a.c. or d.c. systems.

4. Digital systems are much less susceptible to clandestine attack.

5. For large installations, digital systems are much more cost-effective, in that fewer signal lines are needed between the secured area and the central alarm station and less space is required in the central alarm station for housing the equipment.

It is recommended that the following criteria be applied when specifying a digital line supervisory system:

1. The system should operate in an interrogate/response mode or a constant transmission mode from the secured area in order to provide constant assurance that the transmission path is intact.

2. For an interrogation/response mode of transmission, the signal technique used in the interrogation mode should be different from the signal technique of the response mode.

3. An alarm signal at the detector should cause a lock-in condition that is transmitted to the annunciator in approximately 1 second.

4. The circuits used in the system should be highly resistant to transmission line noise, such as crosstalk, hum, and voltage transients.

3.3 FIBER OPTICS SYSTEMS

One of the newest techniques for securing transmitted data uses digitally encoded light imposed on a fiber optic transmission line. The security advantages of using fiber optics are:

1. It cannot be easily tapped in order to monitor the signal stream because of the small diameter of the fiber optic line.

2. False alarms due to electrical interference, crosstalk, and lightning do not occur.

3. Processors are available for detecting any breaks in the fiber optic line.

4. Fiber optic lines, usually being very small in diameter, are in bundles, making identification of a particular line difficult.

5. Because fiber optic lines are very small in diameter, more transmission lines can be run in a given space than can a corresponding number of copper transmission lines.

The main disadvantage in using fiber optics is that the signal has to be reamplified after relatively short distances. These amplifiers are vulnerable to surreptitious attack when installed outdoors .

3.4 LASER SYSTEMS

Infrared (IR) laser communication links similar to IR detectors readily lend themselves for use as security transmission links over short distances. Surreptitiously extracting information from the beam itself requires a somewhat sophisticated intruder. However, the transmission lines to the IR transmitter and receiver are vulnerable to attack unless protected by another type of line supervisory system. Also, the system can be prone to false alarms caused by light hitting the receiver or by inclement weather such as fog, heavy rain, or snow.

3.5 OPERATIONAL CONSIDERATIONS

A successful attack on a supervised link requires that an adversary:

1. Learn the characteristics of the signal for a no-alarm or all-clear condition (by obtaining the documentation for the system or actually observing the data on the line),

2. Construct hardware that will generate the no-alarm signal,

3. Gain access to the link for a sufficient amount of time to complete the desired attack, and

4. Successfully substitute the bogus no-alarm signal during the time that the sensor is alarming.

In order to protect the communication link, one or more of these steps must be detected or prevented (Ref. 1).

Some of the line supervisory protective techniques previously discussed offer a high degree of security against surreptitious attack. Unfortunately, as the complexity of signal transmission increases, so does the cost of its protection. In addition, some of the cheaper and less sophisticated line supervisory techniques are also more susceptible to environmental constraints. For example, a.c. and d.c. line supervisory systems experience a high false alarm rate when the lines are exposed to large temperature fluctuations that vary line impedance or to high electromagnetic interference such as that caused by thunderstorms, power line fluctuations, or generators.

No matter what type of line supervisory technique is used, the system may still be susceptible to attack at junction boxes and data-collecting units unless these devices are protected by tamper switches or point sensors and are located within the protected area.

At most facilities, the location of the telephone lines dictates the different security levels of line supervision required. As shown in Figure 3, there are three basic facility locations where telephone lines carrying security information might be run, each requiring different levels of line supervision.

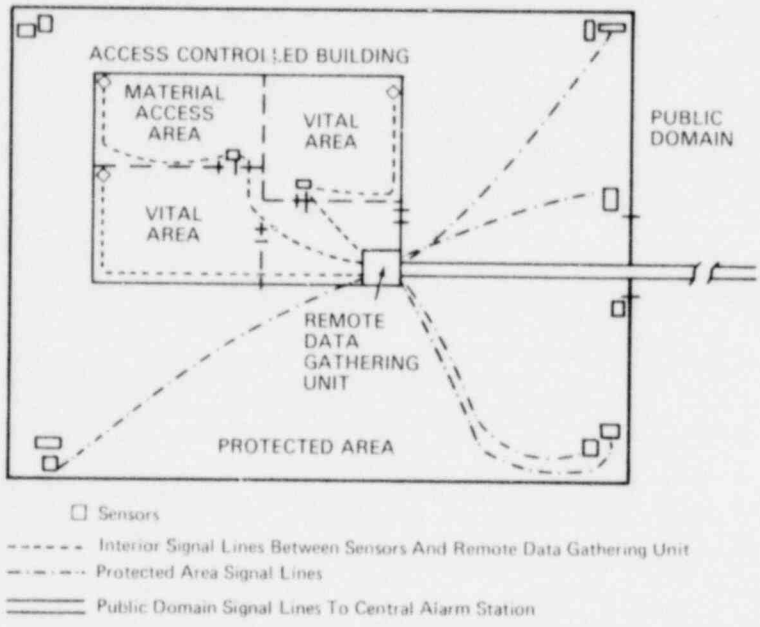

FIGURE 3. GENERIC LICENSEE ALARM SIGNAL LINE LAYOUT

3.5.1 Lines Within Controlled Access Building

Lines that are located within a building into which personnel access is controlled have a certain degree of physical protection afforded them by the building itself and any intrusion alarms located in the building and are least vulnerable to attack from outsiders. Access even by authorized personnel, however, still represents a threat to the security link and, for that reason, the lines still require a certain degree of supervision. If the line will not be exposed to high electromagnetic fields, a.c. or d.c. line supervision usually offers sufficient security.

When a.c. or d.c. line supervision is used on lines in the building, these lines can be placed in conduit to offer some physical protection against covert attack.

3.5.2 Lines Within Protected Area

Lines from perimeter alarm sensors that are located within protected areas are more vulnerable to attack than are lines within controlled access buildings. However, the threat is still primarily from access by authorized individuals. If the environment is conducive, a.c. or d.c. line supervision offers sufficient security for these lines provided they are properly installed and the detection system is tested after work or activity in the area has ceased. It is recommended that these lines be located well within the protected area whenever possible. If there is normally a large amount of activity within the protected area or if the area is subject to high electromagnetic energy fields, the use of a digital type of alarm system will keep the false alarm rate low and increase security.

The use of lasers or fiber optics as a security transmission link within protected areas may in some instances be very effective both financially and operationally. A laser beam between adjacent buildings at the second story level or above will provide a high degree of transmission security without overburdening inadequate cable runs. Fiber optic cable runs between buildings in a protected area allow for a large number of transmission links at reduced cost and volume.

3.5.3 Lines Through Public Domain

Security lines that travel through public domain are most vulnerable to attack by an intruder. Oftentimes these lines go long distances through areas that are not protected and over which the licensee has little or no control. In such areas the intruder may have easy access and ample time to locate, analyze, and defeat the system. In addition, the lines are more likely to be exposed to alarm-producing environments caused by crosstalk, electromagnetic interferences, and temperature fluctuation. Therefore, security lines traveling through public domain need to be protected by a sophisticated type of digital line supervisory system. The digital system allows a high degree of supervision sensitivity over long distances that is not possible with a.c. and d.c. systems and is more immune to false alarms caused by electromagnetic interference.

4. ANNUNCIATOR UNITS

Annunciator units, when connected with their ancillaries in an intrusion alarm system, provide the means to monitor the security status of detectors, alarm lines, and tamper switches. Their purpose is to allow the central alarm station to monitor and control the security status of all alarmed areas in an efficient and timely manner. Reference 1 lists some features that can be considered in the selection of an annunciator system as follows:

1. Clarity of Presentation: The status of individual alarms and of the general facility should be readily perceptible. This characteristic is especially important if multiple alarm situations occur.

2. Ease of Operation: The display system should be engineered so that controls are clearly labeled and conveniently located.

3. Reliability: In the event of malfunctions or failure, various elements of display capability may be lost. Some display system designs segment the task or provide backup to limit the loss. The expected time for repair and operational procedures to be invoked during an alarm-system failure should be considered.

4. Flexibility: It should be a straightforward task to make moderate system alterations such as adding or deleting alarms. Changes in work schedules and startup times should also be easily accommodated. Sophisticated systems may even permit the mode or format of the information display to be altered.

5. Adequate Capacity: The capacity of a system includes physical capacity (how many alarms) and human limitations (how many sensors can be effectively monitored). Adequate resources should be available for any reasonable expansion, but the potential capacity should be consistent with the complexity of the system being considered.

6. System Cost: In addition to initial purchase costs, indirect or hidden expenses should also be considered, i.e., maintenance costs, training costs, cost of system modification, and salaries of security personnel. If a sophisticated system can be operated with fewer personnel, it may prove to be less expensive than a less sophisticated system requiring more personnel for operation.

4.1 CATEGORIES OF ANNUNCIATOR SYSTEMS

Commercially available annunciator systems differ considerably according to such factors as the type of display, the ease and cost of installation and maintenance, expandability, and ease of operation. Some systems use a unique display for each zone they monitor, while others integrate

all monitored zones into one display. For purposes of this report, annunciator systems will be categorized and identified as stand-alone displays or integrated display.

The systems discussed below are all visual in nature. These systems need to be combined with an audible signal that sounds whenever a change of status occurs at the annunciator and that requires manual resetting by the central alarm station operator to restore silence. The silencing control should be so connected that the audible alarm signal will be reactivated upon receipt of an alarm from another zone. When a detection circuit is conditioned for authorized entry into the secured area (access mode), the annunciator should continue to indicate alarms if line supervisory limits are exceeded or if any tamper switches are disturbed.

For increased security, the annunciator system should be so designed that, after an alarm occurs, it requires manual resetting at the secured area before the zone can be reset at the central alarm station.

4.1.1 Stand-Alone Display Systems

The manufacturer of a sensor may also offer a companion display system to display the status of that sensor. Typically, stand-alone systems are physically compact desk-top units that are not intended to handle large numbers of alarms. A single unit may be able to accommodate a number of sensors of the same model. A basic stand-alone unit could indicate the current state of the sensor as "normal," "alarm," "reset," or "tampering" (Ref. 1).

Advantages of the stand-alone display are guaranteed compatibility with the sensor, simple installation procedures, and relatively low cost. The manufacturer's display equipment may also perform some processing on the output from the sensor as an integral part of the system. Using stand-alone units, it is possible to display the status of all currently active sensors, with breakdown of a specific stand-alone unit affecting only the associated sensors (Ref. 1).

If the security system consists of several types of sensors supplied by different manufacturers, the use of stand-alone systems becomes less desirable. Different types of sensors may result in different types of displays, each with its own method of indicating alarm and discrete maintenance and operational procedures. The presentation of sensor status would be affected because the units would physically group together by similar sensor types, rather than a more desirable grouping criterion such as physical location (Ref. 1).

4.1.2 Integrated Display Systems

Integrated display systems are systems that accept inputs from a variety of sensors and use one uniform technique for displaying alarms and operating the system. Such systems have the best potential for making meaningful information presentations, but this advantage may be offset by increased costs or the need for more extensive in-house capability for designing interfaces and maintaining the equipment (Ref. 1). The integrated systems discussed in this section are annunciator panels, numeric readouts, computer-driven cathode ray tube (CRT) displays, and computer-driven teleprinters.

4.1.2.1 Annunciator Panels - An annunciator panel or alarm board consists of a collection of individual indicators with each indicator dedicated to one specific alarm circuit. Normally, duplicate colored lights are used to indicate the security status of each secured zone. Green lights are used to indicate that the detectors and signal lines are in the secure mode, yellow lights are used to indicate that the detectors are in the access mode, and red lights are used to indicate an alarm condition in either the secure or access mode. It is recommended that these lights have a life expectancy of not less than 50,000 hours.

The principal advantage of an annunciator panel display is that the complete status of the entire security system can be perceived simultaneously since the status of each sensor is always visible. Similarly, an alarm can be acknowledged and reset easily since controls are provided for each alarm circuit (e.g., pushing one button identifies both the circuit that is to be affected and the action that is to be taken on that circuit). Another advantage of annunciator panel systems is that separate components (e.g., lights and relays) are used for each alarm circuit so that a component failure affects only one alarm circuit. When the alarm system is modified, indicators can be added to the display up to the panel's capacity (Ref. 1).

A more effective display of information can sometimes be provided by a modification of the basic annunciator panel approach. A geographic display in which indicator lights are arranged on a map or floor plan of the premises can be used. This type of display simplifies identification of the location of alarms and recognition of related alarms, such as a sequence of alarms occurring when an intruder passes through adjacent detector zones (Ref. 1).

There are potentially several disadvantages in the use of an annunciator panel in large systems. The use of individual components for each alarm circuit may cause increased board size to the point that, while physical capacity of the system is not exceeded, the human capacity is. In such a case it may not be possible to see the entire display easily or to reach the various controls. Also, it may be difficult to perceive and evaluate the information contained in the simultaneous display of a large number of alarms. Another disadvantage of a large geographic display is that it is more difficult to associate easily accessible controls with their alarm indicators. In order to increase the number and capacity of sensors to be handled, it may be necessary to have an in-house capability for building interfaces or to install new panels. The costs of these system expansions may exceed the costs of alternative integrated display systems (Ref. 1).

4.1.2.2 Numeric Readouts - Numeric readout systems are a more recent development in alarm display systems. These systems employ an electronic readout device (such as a nixie tube, light emitting diode display, or liquid crystal display) to display a number that identifies the alarm. The main advantage of this type of display is that any number of alarm circuits can be monitored with only one readout device, thus providing an economic solution for large security systems. But since there is only one readout device, only one alarm can be displayed at any one time, so that concurrent alarms can be recognized and processed only on a serial basis. Some numeric readout systems provide two or more displays so that several alarms can be presented simultaneously, but the general problem remains that it is not possible to simultaneously display

the status of the full alarm circuit system. This limitation makes it difficult to rapidly assess the severity of the situation (e.g., multiple alarms or alarm patterns) (Ref. 1).

Acknowledging but not resetting an alarm in a numeric readout system may present problems since the alarm may be reindicated to the operator on every scan or the alarm may be forgotten. Selecting a specific alarm circuit for display on a random basis may not be possible. It is impossible to alter the mode of output of a numeric readout system into a clearer form. But the most serious disadvantage of the numeric readout approach is that, if all alarms are displayed via one common set of electronics and that portion of the system fails, the entire system fails. The inherent reliability of the individual annunciator panel is defeated by the use of common display numeric readout (Ref. 1).

4.1.2.3 Computer-Driven Cathode Ray Tube Displays - The most recent development in alarm display systems is the use of computer-driven CRT displays (Ref. 1). The advantage of computer-CRT systems over other types of displays is the greater flexibility in the type of information that can be displayed and the format (or organization) of the presentation. Both descriptive text and graphic layouts can be used in a computer-CRT display system to indicate the exact location and status of each sensor, with specific procedural instructions associated with each alarm stored and automatically displayed when needed. Another advantage of these systems is that the computer can be programmed to perform other security functions, including (Ref. 1):

1. Remembering individual opening/closing schedules for each zone,
2. Distinguishing among "set-up" alarms, true alarms, and other alarm circuit states,
3. Displaying concurrent alarms in accordance with installation-defined priority,
4. Monitoring performance of the guard force,
5. Aiding in recognition of patterns of alarms that may result from a single intrusion,
6. Aiding in recognition of false alarms,
7. Reducing the number of points to be displayed by providing a hierarchical alarm structure (e.g., protected area, vital area, material access area),
8. Automatically scheduling/checking guard tours,
9. Automated self-testing, and
10. Providing complex combinations of alarms (meta-alarms) (e.g., alarm A coincident with alarm B for t seconds during interval T).

One major disadvantage of a computer-CRT system is its cost, but the cost can be distributed by using the system to perform additional security functions such as primary and secondary

power monitoring, personnel accountability, logging, and report generation. As an example, since CRT displays allow different functions controlled by a single computer to be displayed separately, it would be possible to share fire and security functions on a single computer by programming one CRT to display only those events pertaining to fire and another CRT to display only security events.

CRT displays are also limited in the number of alarms that can be simultaneously presented, although that number is usually greater than that available from numeric readout displays. An alphanumeric terminal (incapable of graphics) can only display a maximum number of characters, while a graphics terminal can only display a certain amount of information without flicker. Flicker or other display perturbations can make continuous monitoring of CRT displays extremely fatiguing (Ref. 1).

Because it is computer-based, the control logic of the computer-CRT display is embodied in the operating system software. Such software is not always easily modifiable, thus limiting the flexibility of such a system. While some software systems are designed to be modified, others are not. At one extreme, installation parameters specified in a high-level alarm-display language could yield a flexible system, but at the other extreme, all logic (including the installation-specific parameters) may be embedded in machine language code, yielding a highly inflexible system. The quality of documentation provided may vary considerably among systems. If such a system is being contemplated, the costs of obtaining services for modification of the software should be considered. The costs may include training in-house personnel in software development or purchasing these services from the vendor. If the decision is made to implement in-house software development, expensive support equipment must be available, including text editing programs, listing devices, or even alternative computer systems for testing (Ref. 1).

The reliability problem resulting from use of common equipment is magnified in the computer-CRT approach by the extensive and complex equipment employed. A single component breakdown could disrupt the entire system, but this problem can be minimized through the use of redundant configurations (Ref. 1). Redundancy of key elements in a security-controlled computer system is necessary if the user wants assurance that the system will be available when most needed. A CRT display in conjunction with a computer-driven logging unit complement each other to provide this assurance of reliability.

Two parameters of a CRT display that are of utmost importance to a security officer are the legibility of the display and the environment in which the CRT will be installed. The legibility of the CRT display depends on factors such as character size and spacing, contrast between the CRT background and the characters, the amount of character or screen jitter, CRT blemishes or noise, and the brightness of the display. The environmental effects are the amount of illumination in the central alarm station, the angle of the viewer to the CRT, the size of the CRT, and the number and size of characters displayed. Most CRT displays come equipped with a specially designed keyboard for providing editing, erasing, and inserting controls to the display. Before purchasing a CRT display system, the potential user should view the proposed displays to see if they present the type of information in the format and clarity desired. (Further information on CRT displays can be found in Reference 5.)

4.1.2.4 Computer-Driven Logging Units - Logging units can be used as an ancillary piece of equipment to the annunciator unit, providing a permanent record of all alarm status changes. The logging unit presents the current status of all alarmed points and the exact time, date, location, and status of all secured points, and it frees the operator from time-consuming and often error-creating paper work. An automatic logging unit is almost a necessity for installations having many security points.

Most logging units are computer controlled. Some units print out the information in coded form and others in plain language. For most security applications it is recommended that logging units use plain language printouts to minimize guard response time. Like computer-driven CRT displays, computer-driven logging units can offer great flexibility in the type of information which can be displayed. The units can be programmed to log (1) all personnel entrances to and exits from secured areas, (2) all concurrent alarms in accordance with a priority list, (3) all guard tours, and (4) all changes in status of alarmed points. Logging units also tend to have some of the same restrictions as numeric readouts and CRT displays, e.g., (1) concurrent alarms can only be logged on a serial basis, (2) the computer software program may not be easily modified, and (3) a component breakdown in the logging unit can disrupt the entire system. In relation to reliability, since logging units are electromechanical devices, they do not tend to have as high a mean time between failure rate as do all-electronic devices. Combining a logging unit with another type of display provides the user with an instant understandable readout that is permanently logged.

In the selection of a logging unit, criteria such as the need for copies, acceptable noise levels, graphics, and maintainability need consideration along with such traditional criteria as speed and cost.

Logging units can be classified according to three characteristics (Refs. 8 and 9):

1. Impact and nonimpact units - Impact units use various forms of hammer-type mechanisms for transmitting alphanumeric characters to the paper. All impact units can produce multiple copies since the impact pressure is transmitted through the carbons. However, impact units can be noisy, especially those types that print a whole line of information at one time versus the type that print only one character at a time. Nonimpact logging units produce only an original copy and usually require special paper, but they are quieter to operate and are as fast as the impact units.

2. Character or line - The difference between character or line logging units is whether the printer prints a whole line of information at a time or just a character at a time. Line units are faster, but generally cost more and may be noisier. Impact and nonimpact units that use either the character or line type of format are available.

3. Shaped or dot-matrix characters - Dot-matrix characters form the alphanumeric characters through the use of either a 5 x 7 dot matrix or a 7 x 9 dot matrix. Shaped characters are preformed characters. Again, either type of characters can be used on both impact and nonimpact logging units.

The most commonly used logging units are the low-cost, 10-to-30-characters-per-second character units used for interactive operator-oriented terminals. Medium- to high-speed units (300 to 1,200 lines per minute) represent the major output devices for small- to large-scale computers. Logging unit performance is measured by print quality, speed, flexibility, and reliability. The principal factors that determine print quality are horizontal and vertical character registration, character smear, character tilt, character clipping, ghosting, character voids, and variations in print intensity. Depending on the type of machine chosen, one or more of these character flaws can be a problem. Before buying a printer it is recommended that the purchaser carefully look at a demonstration unit to determine its print quality. Many new types of logging units are designed to improve reliability and maintainability by incorporating such features as integrated circuits, modularity, and replaceable components so that the printer can be maintained in the field.

Some basic operator questions concerning printers that need to be considered are (Ref. 8):

1. Is the paper easily loaded?

2. Are the tractors easily adjusted to accommodate various forms?

3. Is the paper path straight or does it have sharp bends?

4. How is paper motion accomplished?

5. Is the ribbon easily loaded?

6. How long does the ribbon last?

7. What kind of ribbon reversal system is used? Is it subject to failure? If so, what happens?

8. Is the printer rigid?

9. Can it withstand vibration caused during operation over long periods?

5. PREMISES CONTROL UNITS

The purpose of a premises control unit is to allow the detector unit to be switched between the secure and access mode at the secured area. The premises control unit is so designed that, when both it and the corresponding point at the central alarm station are in the access mode, it permits entrances into and movement within a security area without activating an alarm signal. The unit consists of circuitry installed in a metal tamper-proof enclosure, the cover of which contains a two-or-more-position key-operated switch. The positions are labeled "access," "secure," and other labels required to denote functions designed into the unit. Turning the switch from secure to access alters the signal(s) to the annunciator and bypasses the output of the detector's alarm contacts. However, all tamper switches in detector units and junction boxes continue to be monitored. Turning the switch from access to secure alters the signal(s) to the annunciator and activates the detection device enabling monitoring of both alarm and tamper signals. Switching from secure to access or from access to secure should cause an alarm signal to be generated at the central alarm station annunciator unit until it is set to the corresponding mode of the premises control unit. The premises control unit is usually located just inside the entrance door to the alarmed area. In some instances it may be located on the outside wall of the alarmed area, but then the signal lines between it and the detector units usually enter in a conduit directly from the premises control unit, through the wall, and into the alarmed area. This is done to protect these lines from compromise since they usually do not have as high a degree of signal supervision as those between the annunciator and premises control unit.

6. POWER SOURCES

Primary power for interior alarm systems can be provided from a public utility, batteries, or local generators. Interior alarm systems can be wired so that, in the event primary power fails, an emergency power source will automatically take over and operate the interior alarm systems without causing a security systems alarm at the annunciator. However, a separate alarm point should be annunciated at the central alarm station upon switchover from primary to emergency power. Emergency power sources can be provided from either battery supplies alone or a combination of battery and local generators. Switchover to emergency power should be instantaneous and automatic upon failure of the primary power source and should not cause an alarm signal of the intrusion alarm system.

Consideration should be given to the fact that most computer systems require an alternating current power source in order to operate. For this reason, it is recommended that an active inverter be placed between the emergency power source and the computer and be used to operate the computer at all times.

Batteries can be either dry cell or rechargeable. Rechargeable batteries should be kept fully charged or be recharged automatically whenever the voltage drops 10% below normal under load. Dry cells should be replaced with fresh ones whenever the voltage drops 20% below the rated voltage under load. A signal can be activated in a power annunciator monitor to indicate when recharging or replacement is required. Except for nickel-cadmium batteries, which need to be charged by constant current and never fully discharged, batteries are usually float charged and so arranged that they are fully charged at all times when primary power is available. Chargers need to be of ample capacity to recharge the batteries from a fully discharged state to not less than 85% of capacity within 24 hours.

Emergency power sources should be capable of maintaining full operation of the alarm system for not less than 24 hours. Such power sources can contain a switching capability to facilitate operational testing designed to determine the adequacy of the emergency power sources.

Batteries should be sufficiently vented to preclude explosions caused by the buildup of hydrogen gas.

7. TESTING AND MAINTENANCE

Periodic testing and maintenance of interior intrusion alarm system components is needed to ensure that they are performing to specifications and will perform properly when needed. Testing of the sensors and monitor systems can be done each time a secured area changes from access to secure or vice versa. Maintenance of the interior alarm systems can be done on a continuing rotational basis by technicians whose primary responsibility is ensuring their proper operation and continued availability.

It is advisable that the maintenance crew have a complete and current set of schematics and specifications for each of the components for which they are responsible. In addition, the downtime due to maintenance and troubleshooting can be greatly shortened by having sufficient spare parts. The manufacturer of the units can offer insight on the type and quantity of spare parts most frequently required.

Tests of sensors that look for dead zones and proper sensitivity to intrusion can be done monthly. Line supervisory units can be tested every three to six months for proper current and voltage levels. Annunciator panels can be tested daily to ensure that no lights are burned out, that the audible alarms work properly, and that all logging units and readout devices function correctly. Emergency power supplies for all units can be checked monthly to ensure that they are fully charged and are in good working order. Tamper switches on alarm sensors, premises control units, junction boxes, and line supervisory units can be checked every 3 months to ensure that they are operating properly and that tampering has not occurred. Results of all tests, checks, and maintenance performed on the alarm system can be documented for later reference when troubleshooting or installing new systems. All tests, maintenance, and troubleshooting need to be coordinated with the security force to ensure that security will be adequate while work is going on. After all work has been completed, a member of the security force can test the system to verify its proper operability.

7.1 DAILY TESTS

When daily tests are recommended for alarm systems (e.g., those detector systems that do not incorporate circuit supervision), tests can be performed by actual intrusion into the alarmed area, except as noted below. Alarms caused by the opening and closing of doors by operating personnel in the normal performance of their activities would be acceptable as daily tests.

When daily tests are not feasible (e.g., alarm systems in vaults that are seldom opened), a test can be scheduled at least weekly.

When a number of electromechanical devices are used, such as door and window switches in a single series circuit, only one door or one window switch needs to be tested each day. Testing of these switches can be on a random rotational sequence basis so as to provide a complete test of the circuit on a periodic basis.

When volumetric devices (both active and passive types) are used, sensitivity tests can be conducted on a monthly basis to ensure that the required degree of sensitivity is maintained.

7.2 PERFORMANCE TESTING

Volumetric (active and passive type) and door protection interior intrusion alarm systems can be tested by actual intrusion into the volume protected before and after each period during which the system is protecting the volume. Except for breakwire detectors, surface protection systems on walls, ceilings, and floors can be tested by simulated breaching of the surface on a weekly schedule. Barriers that use breakwire systems can be visually inspected to verify that no physical tampering has occurred.

7.3 SPECIFICATION TESTING

In order to be assured that the system is operating as specified and installed, interior intrusion alarm systems and transmission supervisory systems can be tested against the manufacturer's performance specifications at least quarterly. Test procedures developed by the manufacturer can be used. Keeping a detailed record of equipment and circuits tested and results of their inspection can provide information useful in determining long-term changes in sensitivity.

REFERENCES

1. Sandia Laboratories, "Intrusion Detection Systems Handbook," November 1976, SAND 76-0554, Albuquerque, NM 87115.

2. Underwriters Laboratories, Inc., "Intrusion-Detection Units," Standard UL-639, September 1976 (draft).

3. Underwriters Laboratories, Inc., "Thermal Plastic-Insulated Wires," Standard UL-83, 1975 (revised June 1976).

4. Insulated Power Cable Engineer Association/National Electrical Manufacturers Association, "Rubber Insulated Wire and Cable for the Transmission and Distribution of Electrical Energy," IPCEA S-19-81/NEMA WC 3-69, June 1, 1976, as revised.

5. J. A. Prell, "Basic Considerations For Assembling A Closed Circuit Television System," U.S. Nuclear Regulatory Commission Technical Report NUREG-0178, May 1977, Washington, DC 20555.

6. "Magnetic Switches For Burglar Alarm Systems," U.S. Department of Justice - Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice Standard, NILECJ-STD 0301.00, March 1974.

7. "Interim Federal Specification Alarm Systems, Interior, Security, Components For" W-A-00450B (GSA-FSS), February 16, 1973, Federal Supply Service, General Services Administration, Washington, DC 20406.

8. Ken Freund, "Make No Mistakes When You Buy Your Next Printer," Electronic Products Magazine, April 28, 1975.

9. I. L. Wieselmen, "Printers - The Major Output Devices For Computers," Electronic Products Magazine, July 16, 1973.

10. The Mitre Corporation, "Guide For The Evaluation Of Physical Protection Equipment," U.S. Nuclear Regulatory Commission Technical Report NUREG-0273, June 1977, Washington, DC 20555.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
UNITED STATES NUCLEAR
REGULATORY COMMISSION

1806 150