2
7-25-78

Conf-780917--2

SAND78-0644C
Unlimited Release

INTRUSION DETECTION SENSORS

MASTER

J. D. WILLIAMS
Intrusion Detection Systems Technology Division

SF 2900 Q(7-73)

INTRUSION DETECTION SENSORS*

James D. Williams, Supervisor
Intrusion Detection Systems Technology Division
Sandia Laboratories, Albuquerque, NM 87185

MASTER

ABSTRACT

Intrusion detection sensors are an integral part of most physical security systems. Under the sponsorship of the U.S. Department of Energy, Office of Safeguards and Security, Sandia Laboratories has conducted a survey of available intrusion detection sensors and has tested a number of different sensors. An overview of these sensors is provided. This overview includes (1) the operating principles of each type of sensor, (2) unique sensor characteristics, (3) desired sensor improvements which must be considered in planning an intrusion detection system, and (4) the site characteristics which affect the performance of both exterior and interior sensors. Techniques which have been developed to evaluate various intrusion detection sensors are also discussed.

INTRODUCTION

Since late 1974, the Department of Energy, Office of Safeguards and Security (DOE/OSS) and its predecessor organizations have provided funds for analysis, modeling, development, implementation, and demonstration of various safeguards system concepts which are appropriate for fixed-site facilities. Emphasis has been placed on DOE-type facilities; however, the results of these studies are also applicable to other government agencies and private industry, especially the nuclear power industry (both domestic and foreign).[1-11]

As a part of the DOE-sponsored nuclear safeguards effort, the Fixed Facilities Physical Protection Research and Development program at Sandia Laboratories provides (1) system analysis and assessment, (2) physical security equipment evaluation and development, and (3) system design and operational testing and evaluation.

This paper presents information on both exterior and interior sensors. These data were obtained as a result of a portion of the equipment evaluation and development effort.[11,12] The information presented has been obtained from evaluation programs conducted at various laboratories and sponsored by DOE/OSS, the Department of Energy, Office of Military Application (DOE/OMA), the Department of Defense (DOD), the Services, the Defense Nuclear Agency (DNA), the Nuclear Regulatory Commission (NRC), and other government agencies as well as from data provided by commercial security equipment suppliers.[13-17]

The selection of intrusion detection equipment involves identifying the equipment and installation methods which best meet the overall system objectives. The system objectives, which include the purpose of the intrusion detection equipment and define the types of assumed threats, should indicate the desired requirements of the intrusion detection system in three primary areas: (1) the probability of detecting the intruder (P_d), (2) the vulnerability to defeat of the equipment, and (3) the false/nuisance alarm rate (FAR/NAR) and causes of the alarms. However, these parameters cannot be represented by single-valued numbers; they are influenced by a large number of variables such as physical environment, weather, threat, maintenance, installation, regulations, procedures, and operating personnel. Therefore, when a high P_d and a low FAR/NAR are required over a wide range of operating conditions, it will be necessary to use combinations of sensors. Combinations of sensors also contribute to the safeguards concept known as "protection-in-depth," which is simply a number of protective measures in series, i.e., an intruder must successfully circumvent or defeat each of the protective measures in sequence before access to the protected material or facility can be achieved.

A major design goal is to obtain an intrusion detection system which exhibits a low FAR/NAR and an acceptable P_d and is not susceptible to defeat. This goal can be achieved by logically or hierarchically combining the outputs of different types of sensors. No single sensor presently exists that will reliably detect all intruders and still have an acceptably low FAR/NAR for all

*This work was supported by the U.S. Department of Energy under Doe Contract AT(2601)-789

expected natural and manmade environments. However, the number of sensor types in a system should not be increased and/or logically combined or implemented to change any of the above performance characteristics without consideration of how these changes affect the other performance characteristics. A common assumption is that the system should be adjusted to achieve a value of P_d which is very close to 1 and that any resultant increase in FAR/NAR will be tolerated. This assumption is acceptable only if the system FAR/NAR is equal to or less than that FAR/NAR which the security force will tolerate while at the same time continuing to treat each alarm as a credible alarm. When this FAR/NAR is exceeded and the system is turned off or ignored, the actual system P_d goes to zero.

Figure 1 shows a hypothetical site which employs both exterior and interior sensors. In order for unauthorized theft or sabotage of material (assumed to be stored on the metal shelving shown in the building cutaway) to occur, the following undetected actions by an intruder(s) must be taken:

1. The outer fence must be gone through, over, or under. If there are fence sensors, the job is more difficult.

2. The exterior volumetric sensors (assumed to be buried-line, microwave, and electric field sensors) must be gone over or under. This task becomes more difficult as the volume of the detection zone is increased.

3. The inner fence must be gone through, over, or under.

4. The distance from the inner perimeter fence to the building must be traveled.

5. The shell or boundary of the building must be penetrated. If a natural entry is used, door/window switches must be circumvented. If a new or unnatural opening is made/used, vibration sensors, ventilation duct sensors, etc., must be circumvented.

6. The motion or volumetric sensors in the building interior (ultrasonic, sonic, microwave, or infrared sensors) must be defeated.

7. The proximity sensors must be defeated.

8. Finally, the procedures must be repeated in reverse order if the intruder desires to also escape, undetected.

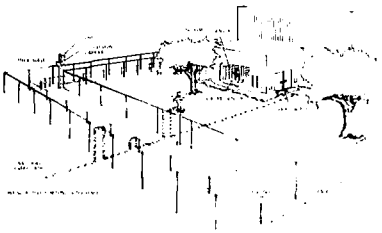


Figure 1. Hypothetical Site Showing a Possible Unauthorized Entry Path

Usually, the itemized actions must occur without the intruder being detected by a roving patrol or by closed-circuit television (CCTV) located on the perimeter of the area and in the building. The number of the various sensors shown in Figure 1 will vary with the degree of security required. The degree of security needed is influenced by the consequences of any theft or sabotage, available funds, regulations, etc. If buried-line sensors are used an intruder must dig deeper if he attempts to tunnel under the detection zone.

The remaining sections of this report describe the different technological types of sensors, provide a discussion on how to plan an operationally effective intrusion detection system using various sensors, and describe sensor evaluation techniques. A brief summary of the knowledge accumulated to date is also presented.

TECHNOLOGICAL TYPES OF SENSORS

Intrusion detection sensors can be categorized as either exterior or

interior sensors. Exterior sensors include fence sensors and free-standing line and buried-line sensors. Interior sensors include boundary penetration sensors, motion (volume) sensors, and proximity sensors. Figure 2 illustrates this breakdown.

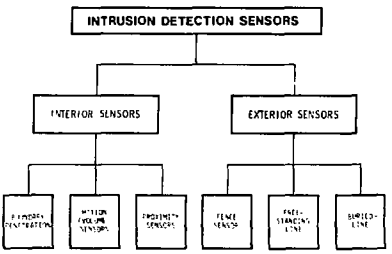


Figure 2. Types of Intrusion Sensors

General Exterior Sensors

Exterior sensors can be further divided into technological types as shown in Figure 3. Most of these categories are covered in the following discussion.

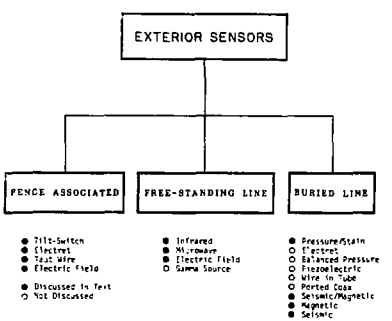


Figure 3. Types of Exterior Sensors

Fence-Associated Sensors--Since it is desirable to detect an intruder as soon as possible, the first type of sensor encountered by an intruder is usually located at the outer perimeter of a facility. Fences, no matter how tall or how elaborate, offer little resistance to a determined intruder. Therefore, fence sensors can only help to form a viable perimeter system. However, even if a good perimeter system is employed it is only part of an overall security system and cannot be considered as complete protection. Fence-associated systems offer no protection against the intruder who goes over or under the fence or who hides on the premises during a time when he has access to the facility.

Tilt-switch sensors consist of several series or parallel-connected switches coupled to a processor. Detection is based on the fact that any motion of the switch housing will result in the opening and closure of a contact switch. Switches are mounted on fence posts or chain-link fabric sections so that disturbance to the fence will cause switch action.

Tilt switches offer protection against intrusion by detecting abnormal motions, shocks, or vibrations which may occur during attempts to climb over the fence, to penetrate the fence by cutting or burning, or to push or pull the fence down. Several different types of transducers are currently in use: mercury switch, pedestal-mounted ball, piezoelectric element, and reed switch. Figure 4 shows a tilt-switch sensor installation.

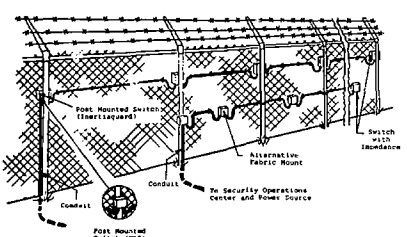


Figure 4. Tilt-Switch System

Electret Sensor cables are special cables which detect fence movement and sounds. These cables provide coverage along the entire length of the fence to be protected. An electret sensor consists of a coaxial sensing cable with a radially polarized dielectric and a

processor. Detection is based on the fact that a small stress applied to the dielectric will produce an electrical output. If the cable is attached to a chain-link fence, any disturbance of the fence will stress the cable and cause an output. The signal generated by the sensing cable is amplified and processed for frequency content, amplitude, and duration in order to allow differentiation between actual intrusions and environmental disturbances. Figure 5 shows an electret sensor installation.

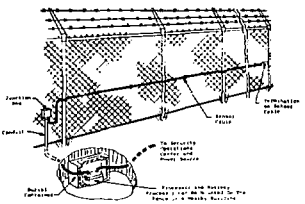


Figure 5. Electret Sensor

Both the tilt switch and the electret sensor can experience high false alarm rates caused by wind, blowing debris, animals, birds, moving vehicles, snow or ice, earthquakes, electrical storms, adjacent grass or bushes, or the motion of nearby trees. Many of the fence-mounted sensors are designed with variable time-constant adjustments which minimize false and nuisance alarm rates by ignoring a given number of instances (one or more) of fence vibration before producing an alarm. Also, some of the sensors are designed to primarily sense vertical fence motion and to be less sensitive to horizontal motion.

The best countermeasure for the intruder to take against a fence-mounted tilt-switch sensor is to avoid it completely by going over, under, or around the fence without coming in contact with it.

Environmental factors are a primary consideration in the design and installation of fence-associated sensors since these sensors are generally mounted outdoors and thus are exposed to all the inclemencies of the weather. High-quality installation is required; the sensors must be securely mounted and kept clean, dry, and rust-free. Regularly scheduled checks should be used to verify that all mechanical and electrical connections are tight. The fence should be rust-free, the posts set in stable footings, and the fence mesh and other accessories, tight and secure.

Most fence-associated sensors have provisions for line supervision, sensitivity adjustments, and multizone operation. Better rejection of wind-induced alarms and improved self-test features are desired improvements.

The taut-wire sensor or wire-tension sensor consists of a series of wires installed under tension and attached to switch sensors so that deflection of the wires produces an alarm. Various wire configurations are possible, including free-standing and chain-link fence-mounted configurations.

Commercial equipment built on the taut-wire principle uses barbed wire. The sensor consists of a twisted pair of wires that when stretched act as a spring distributed over the entire fence length. Adequate tension on the wire must be maintained during changes in environmental conditions. The sensor post (Figure 6) consists of a number of switches, one switch for each barbed wire, connected in parallel. Each sensor post is centered between anchor posts which can be up to 60 metres apart. Multiple sensor posts can then be wired in parallel to provide a detection zone of any desired length. A wire tension of 35 to 45 kg is necessary for proper operation of the system. Intermediate guide posts are used to guide the horizontal wires through holes to permit unobstructed lengthwise movement. These posts are usually spaced about 3 metres apart. The sensor switches are clamped to the barbed wire in such a manner that a sideways pull on the switch, which is induced by a man climbing the wires, pulling the wires apart, or cutting the wires causes the switches to close. A switch deflection of as little as 2 mm is sufficient to generate an alarm.

A unique feature of this switch is its self-adjusting property. This self-adjustment allows for gradual changes in post positions, while short-term changes create an alarm. The switch actuator is mounted inside a viscous silicone compound which acts as a low-frequency dampener. Slow changes cause

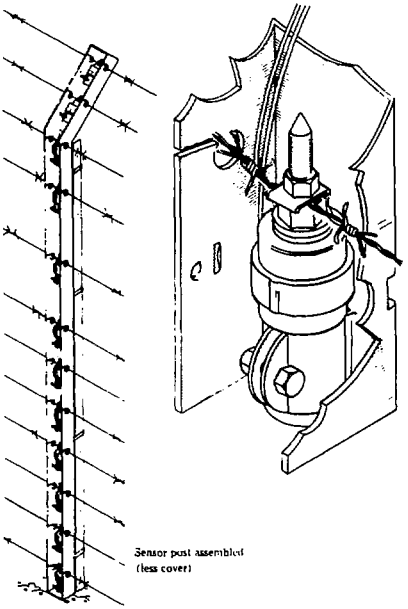


Figure 6. Taut-Wire Sensor and Sensor Post

the actuator to move through the compound, while faster changes make the compound appear rigid and result in switch closures.

This system exhibits a very low false alarm rate. Defeat may be possible by climbover at the anchor posts. Typical taut-wire sensor installations are shown in Figure 7.

An electric field fence sensor consists of an alternating-current field generator which excites a field wire, one or more sensing wires which couple into the resulting electric field, and an amplifier and signal processor which amplify and detect changes in the signal amplitude of the sensing wires. A signal is generated when a conductive body or a body with a high dielectric constant (such as a human body) distorts the coupling between the field wire and the sensing wires. Such an installation is shown in Figure 8. The electric field principle is also employed in free-standing sensors.

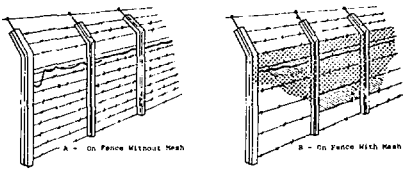


Figure 7. Typical Taut-Wire Sensor

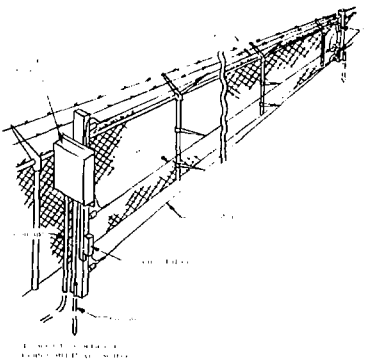


Figure 8. Three-Wire Electric Field Sensor Mounted on Chain-Link Fence

Free-Standing Sensors--Free-standing sensors used for exterior applications include infrared, microwave, and electric-field sensors.

Active exterior infrared sensors are free-standing line sensors which consist of infrared transmitters, photodetectors, and appropriate lenses. The effective size of the beam is determined by the size of the lenses.

Several transmitters and receivers are usually employed to provide a multiple beam system. The beams are usually configured into a vertical infrared fence. A pulsed synchronous technique is used to reduce interference from and/or defeat by other sources of light.

The significant characteristics of the infrared sensor used for perimeter

systems are

1. The sensor is strictly line-of-sight and requires very uniform terrain,

2. Alignment is critical and requires stable mounting to prevent movement,

3. The sensor is subject to high NAR/FAR or complete inactivation during heavy fog or snow or when wind blows snow lying on the ground into the beam, and

4. The narrow vertical plane does not provide much volume coverage; therefore, the sensor is vulnerable to defeat or bypass.

As a result of these characteristics, the infrared sensors are not well-suited to perform as long-range perimeter sensors. However, they have been used effectively in prisons since the apparatus required to defeat infrared sensors are not usually available to prisoners. These sensors also have short-range gap-filling applications, such as the protection of gates and portals. In general, the above discussion also applies to the use of lasers as perimeter sensors.

Microwave sensors used for exterior applications can either be monostatic (transmitter and receiver are located in the same housing) or bistatic (transmitter and receiver are located in two separate housings). Since the bistatic unit is most commonly used in exterior systems, it will be the only type discussed.

A bistatic microwave sensor uses a modulated transmitter and a receiver (usually operating at about 10 GHz) which are separated by a limited (≈100 metres) line-of-sight distance. Detection is based on the fact that an object moving through the beam will cause a signal change in the receiver. The volume of the detection zone corresponds to the cigar-shaped area between the transmitter and receiver, as shown in Figure 9.

Figure 10 shows the effective width and height of the detection zone as a function of distance from the transmitter for a typical bistatic system.

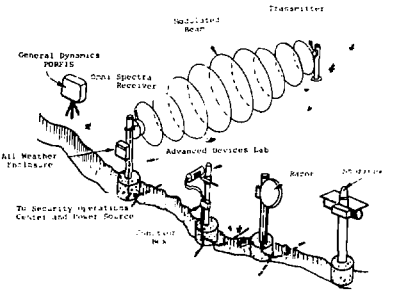


Figure 9. Various Microwave Sensors

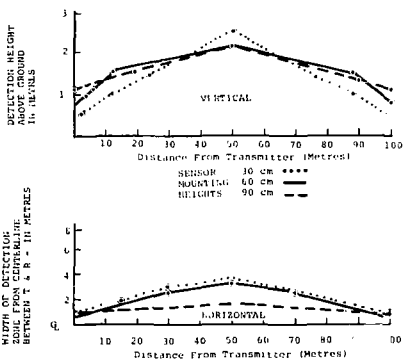


Figure 10. Detection Zone for a Bistatic Microwave Sensor

Electric field free-standing sensors are shown in two-wire and three-wire configurations in Figures 11 and 12, respectively. Not shown are some four-wire systems and other configurations which extend the effective protection volume. This type of sensor can also be mounted on a chain-link fence, as discussed earlier. Desired improvements include a provision for allowing small animals to pass under the sensor without detection and better lightning rejection.

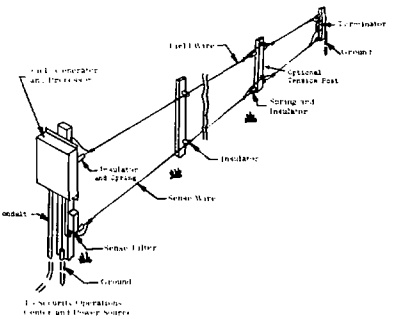


Figure 11. Two-Wire Electric Field Sensor

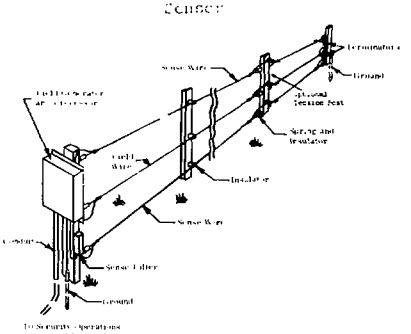


Figure 12. Three-Wire Electric Field Sensor

Buried-Line Volumetric Sensors--Buried-line sensors include extended length cable systems employing seismic, magnetic, or seismic-magnetic detection methods. This class of sensors also includes point sensors.

Seismic-magnetic buried-line sensors consist of a cable which is sensitive to both seismic and magnetic disturbances and a processor which evaluates signals generated in the cable. Detection is based on the fact that seismic disturbances will either move the cable in the earth's magnetic field or strain the flexible magnetic core and by magnetostriction change its permeability. Ferromagnetic material passing near the cable will vary the earth's magnetic field around the cable; this produces a voltage in the sensing coil.

Seismic buried-line sensors include two generic types of seismic buried-line sensors. One type consists of a pair of fluid-filled hoses. When one of the hoses receives more pressure than the other, a differential signal is produced. The second system consists of piezoelectric ceramic discs located at various intervals along a cable. Stressing the ceramic disc creates a signal.

Magnetic buried-line sensors consist of a wire loop which is coplanar to the earth's surface. As an intruder with ferromagnetic material crosses the loop, a detectable electrical signal is generated in the wire. This type of sensor will not detect a "magnetically clean" intruder.

Point Sensors are those sensors which provide a small zone of coverage and can be used as "gap fillers" and as tamper or "weak-link" protection devices. Point sensors can be geophones, electromagnetic point sensors, or Doppler radar sensors.

Interior Sensors

Sensors which monitor intrusions into buildings or enclosed structures have been available for a number of years. Recently, however, some significant improvements in the performance characteristics of these sensors, as well as test techniques and application understanding, have been realized.

Figure 13 shows a general breakdown of the technological types of interior sensors available.

Boundary Penetration Sensors--Boundary penetration sensors are designed to detect penetration of the boundary of a protected area. Included in this class of sensors are vibration sensors and door/window sensors. Vibration sensors are passive devices which are mounted on the wall and detect vibrations. They use a piezoelectric crystal or a moving-coil transducer. The transducer converts mechanical or acoustical signals into electrical signals. These transducers can be

mounted on or within walls, and the system can be adjusted to detect attempts to penetrate walls. Door/window sensors are usually balanced magnetic switches. Other boundary penetration sensors exist but are not discussed in this paper. These include passive ultrasonic detectors, wire grid sensors, and metal foil sensors.

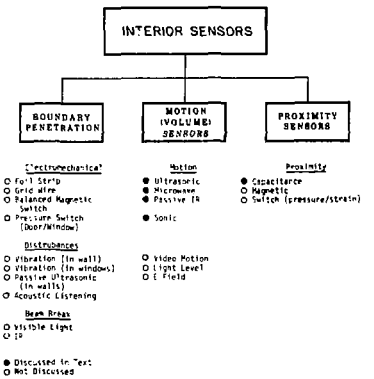


Figure 13. Types of Interior Sensors

Motion (or Volume) Sensors--These types of sensors are designed to detect the motion of an intruder within a confined interior protected area. Several different technological types of sensors fall into this category of motion sensors:

1. Ultrasonic sensors, which are active and operate in the frequency range of 19 to 40 kHz. Detection is provided by observing the Doppler frequency shift associated with motion.

2. Microwave sensors, which are active and operate at a frequency of approximately 10.5 GHz. Detection is provided by observing the Doppler frequency shift associated with motion.

3. Infrared sensors can be active or passive. They can be designed to detect heat and/or motion.

4. Audio (Sonic) sensors can also be active or passive. They operate at frequencies in the audio range and detect both Doppler frequency shift and phase shift associated with motion. In their simplest form, passive systems employ a microphone and amplifier to detect sound caused by an intruder.

Other motion sensors exist but are not discussed in this paper. The electric field sensor, designed for interior use, is an example of such a detector.

Ultrasonic sensors detect acoustic wave changes caused by target motion. When a target moves, the Doppler frequency shift causes the reflected energy to appear at a frequency which is different from that of the transmitted energy. Figure 14 illustrates how movement in a room produces a Doppler frequency shift. Examples of the types of data that are important for this sensor are presented in Figures 15, 16, and 17.

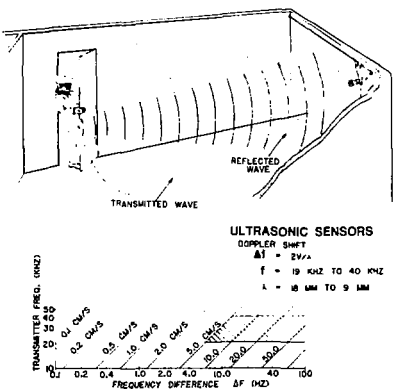


Figure 14. Operational Principle of an Ultrasonic Sensor

Microwave sensors for interior use are typically monostatic. Monostatic microwave sensors employ a single antenna for both the transmit and receive functions. Detection is based on the Doppler frequency shift; typical units operate at a frequency of about 10.5 GHz. The Doppler frequency shift is produced by movement in the room similar to that illustrated in Figure 14 for ultrasonic sensors.

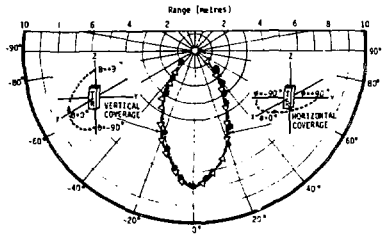


Figure 15. Detection Pattern for an Ultrasonic Sensor

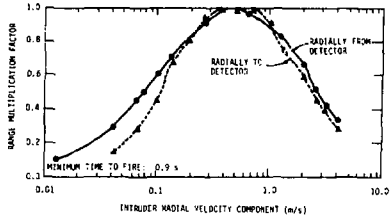


Figure 16. Intruder Velocity Range Multiplication Factor for an Ultrasonic Sensor

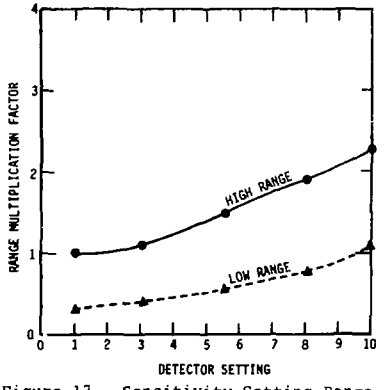


Figure 17. Sensitivity Setting Range Multiplication Factor for an Ultrasonic Sensor

An active infrared (IR) sensor system is basically a beam-breaking system. Passive systems, on the other hand, respond to the energy emitted from a moving intruder by employing special optical and electronic techniques. The detection pattern for a passive IR system is shown in Figure 18.

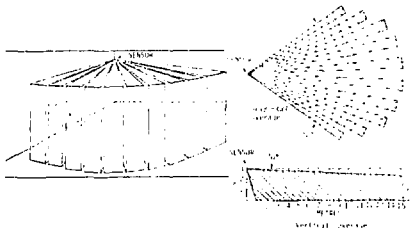


Figure 18. Detection Pattern for a Passive IR Sensor

Active sonic (audio) sensors are similar to ultrasonic and microwave sensors except that their operating frequency is about 1 kHz.

Proximity Sensors--Proximity sensors are designed to protect a metallic object and provide an indication if a person attempts to touch or actually does touch the object. Capacitance point sensors or capacitance proximity sensors are included in this category of interior sensors.

Interior capacitance proximity sensors can be used to detect unauthorized access to metal objects. They are sensitive to changes in capacitance between the protected object and ground caused by the approach of an intruder or another object. This change in capacitance is sensed by a tuned circuit located in the control unit.

PLANNING AN OPERATIONALLY EFFECTIVE INTRUSION DETECTION SYSTEM

The expression "operationally-effective" is used to describe systems which have achieved a reasonable balance between (1) optimization of system hardware, (2) comprehension, acceptance, and efficient utilization of the system by security personnel, and (3) a sufficient degree of detection capability at the facility.

It is essential that any new intrusion detection system or one that is to be improved be carefully planned and analyzed to ensure that it will perform its function reliably and that its strengths and weaknesses are identified and understood. Included in the planning and analysis is the development of (1) a system philosophy, (2) a preliminary system design, (3) on-site experiments and evaluation, (4) final system design, (5) construction and installation considerations, (6) a program schedule, (7) cost considerations, and (8) procurement.

Intrusion detection systems hardware comprises sensors, alarm assessment systems, and alarm reporting systems (including alarm communications and information display equipment). The performance of the sensing and assessment equipment is heavily influenced by the physical environment in which it must operate as well as by installation and maintenance. Since present-day knowledge of the correlation between sensor operation and the physical environment is limited, some on-site evaluation will be required before, during, and after installation. An operationally-effective intrusion detection system is also influenced by facility regulations, procedures, and personnel. All of these items, coupled with the type of facility or material to be protected and the most likely threat (including some intruder attributes), influence the final system selection.

Intrusion detection systems are generally used in association with a barrier system so that attempts to penetrate the barrier will result in an alarm. Intrusion detection systems can be used with entry-control systems to control authorized activity at a facility.

Considerations for Sensor Selection

Sensor selection consists of identifying the equipment and installation methods which best meet the intrusion detection system objective for a facility. A consideration of the interaction among equipment, environment, and intruder forces is integral to the selection of the proper technological type of equipment necessary to ensure the desired intrusion detection functions. These interrelationships and various technological types of both exterior and interior sensors are discussed in this section.

Exterior Detection--The physical and environmental conditions that can affect exterior detection systems include topography, vegetation, wildlife, background noise, meteorological conditions, and soil and pavement. It is important to recognize that there is no "typical" site since combinations of conditions are site specific. Topographical concerns include slopes and hills, gullies and ditches, lakes, rivers and streams, swamps and temporary surface water, perimeter access points, and manmade structures. Vegetation includes all plant life such as trees, weeds, grass, bushes, and crop foliage. The vibration of the root systems of this vegetation as well as the aboveground motion of foliage can affect sensor performance. Wildlife of concern includes large and small animals, burrowing animals, and birds and insects. Background noise such as traffic, wind, natural and manmade seismic sources, and electromagnetic interference all must be taken into account. The specific type of meteorological information which may prove useful in the design and operation of sensor systems includes wind, temperature, rain, snow, hail, visibility, airborne corrosives, and electrical storms. Soil and pavement conditions primarily affect buried sensors.

The major characteristics of several types of exterior sensors suitable for fixed-site applications are shown in Table I. The relative individual adversary detection coverage provided by these sensors is depicted in Figure 19.

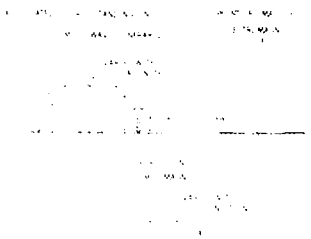
As mentioned earlier, no single sensor exists that will detect all types of intrusions and have an acceptably low FAR in normal outdoor environments. Single sensors can be employed to reliably detect the casual intruder who might simply climb a fence and walk through an area. However, in order to detect determined intruders while maintaining an acceptably low NAR/FAR, an appropriate combination of sensors is required.

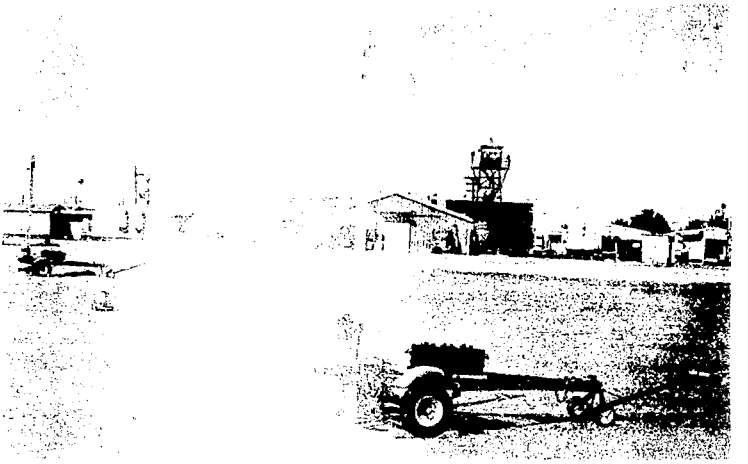
Interior Detection--In general, three classes of interior sensors are of interest: (1) boundary penetration sensors which are designed to detect penetration of the perimeter of the area

Table I

Exterior Sensors Suitable for
Fixed-Site Applications

Application	Operating Principle	Availability	Detection					Conditions for Unreliable Detection	Typical Defeat Methods	Major Causes of False Alarms									
			Nonmagnetic	Walk, Run, & Crawl	Tunnel	Climb Fence	Cut Fence			High Winds	Heavy Rain	Heavy Snow	Heavy Fog	Birds	Small Animals	Large Animals	Seismic Activity	Thunder and Lightning	Electrical Transients	RFI
Buried-Line	Seismic-Magnetic	Military Production	X	X					Bridge and carry no ferromagnetic material	X						X	X	X	X	X
	Seismic	Production	X	X				Frozen ground	Low bridge	X						X	X	X		
	Magnetic	Production		X	X				Carry no ferromagnetic material									X	X	X
Fence-Associated	Electret Cable	Production	X			X			Ladder or short tunnel	X						X		X	X	
	Tilt Switch	Production	X			X			Ladder or short tunnel	X						X				
	Taut-Wire	Production	X			X	X		Ladder or short tunnel							X				
Free-Standing-Line	E-Field (can be fence-associated)	Production	X	X		X	X		Tunnel High Bridge					X	X	X		X	X	X
	Microwave	Production	X	X				Irregular terrain, high grass	Tunnel High Bridge					X	X	?				
	Infrared	Production	X	X				Irregular terrain, high grass, or snow drifts	Ladder, short tunnel, or redirect low beam		X	X	X		X	X				
Point	Seismic or Electromagnetic	Development	X	X					Tunnel					X	X	X		X		X





of view. A knowledge of the azimuthal-motion response of ultrasonic sensors and the radial-motion response of infrared sensors is extremely beneficial to the system designer.

In addition to the patterns for radial intruder motion (such as these patterns shown in Figure 15), patterns have also been determined for movement normal and parallel to the centerline of the sensor field of view. Figure 21 is a composite for an ultrasonic sensor which shows the plus and minus radial directions on the left of the centerline and the plus 45° directions parallel to the line and the minus 135° directions parallel to the line on the right of the centerline. For this sensor, the patterns are symmetrical about the centerline; however, recent data have shown that this symmetry does not always exist. The arrows indicate intruder direction and the dots on the arrows indicate the position where detection occurred. The patterns in Figure 22 and Figure 23 are for the plus and minus directions parallel to the centerline and plus and minus directions parallel to the base line, respectively. Figure 24 shows a composite of all 10 movement directions. Movement by an intruder in any direction in this composite would generate an alarm. In all cases, the composite is smaller than the radial patterns and in a few cases it is many times smaller. These facts coupled with the basic differences in direction of movement for greatest sensitivity for different technological types of sensors must be considered when operational systems and performance tests for those systems are planned.

Another important aspect in the development of evaluation techniques involves the elimination, when possible, of the human factor from the test procedures. This is desirable for several reasons: (1) some test procedures are rather redundant and hence are better achieved electronically and/or mechanically, (2) if the simulation techniques are appropriately defined, then accurate repetition of experiments is possible, (3) error due to human judgment is minimized, and (4) greater flexibility in experimentation is achieved.

A floor plan of the Interior Sensor Evaluation Laboratory is shown in Figure 25. A picture of an aid developed to regulate the velocity of a human test target is shown in Figure 26; a picture

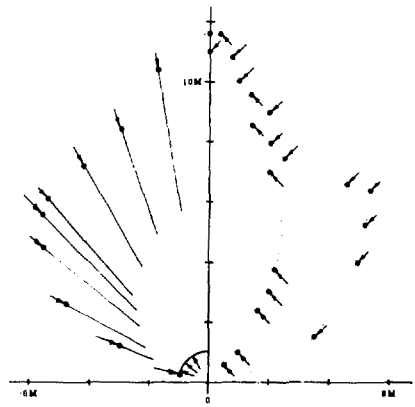


Figure 21. Detection Pattern Along Radial Directions

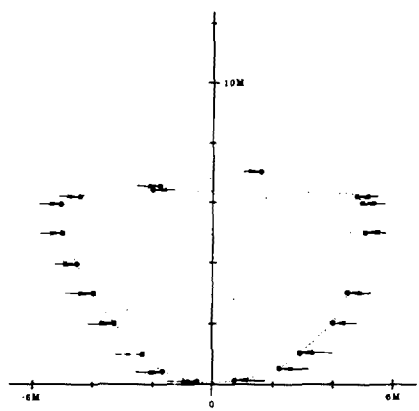


Figure 22. Detection Pattern for Movement Parallel to Centerline

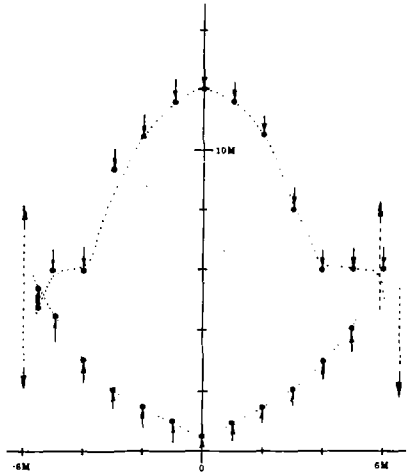


Figure 23. Detection Pattern for Movement Parallel to the Base Line

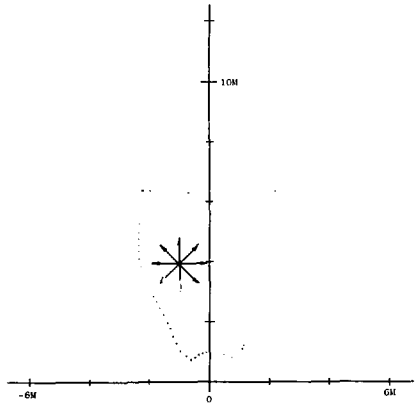


Figure 24. Composite of All 10 Movement Directions

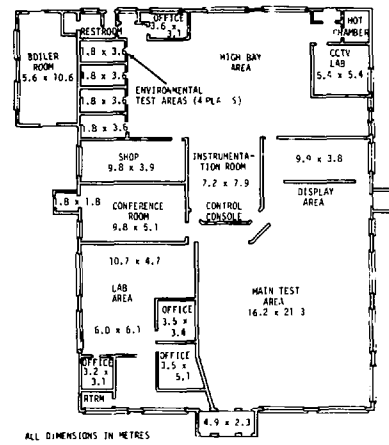


Figure 25. Interior Sensor Evaluation Laboratory

of a motor-driven mannequin used to replace human targets is shown in Figure 27.

Electronic simulators have also been developed to test ultrasonic and microwave sensors which operate on the Doppler principle. These electronic simulators can be used to determine detection pattern variations as a function of intruder velocity. They have also been programmed, in conjunction with temperature controls for the refrigerated rooms, for use in temperature testing of sensors. It now appears feasible to automatically achieve the time-consuming, cold-temperature testing totally within a refrigerated room without the necessity of opening the door or using a human target. Warm temperature testing can be conducted in a hot room in a similar manner. Some recent results indicate that the performance of some sensors vary by a factor of three over the temperature range of -18° to 49°C.

Figure 26. Human Test Target Holding Onto a Constant-Velocity String Controller

Figure 27. Motor-Driven Mannequin Used in Evaluation Programs

SUMMARY AND CONCLUSIONS

This paper has provided a brief review of some intrusion sensors which have been characterized by Sandia Laboratories through work sponsored by DOE/OSS. Other types of sensors exist. Some of them have been characterized by other laboratories and some are yet to be characterized. Sensor inclusion or noninclusion in this paper does not reflect on the usefulness of any type of sensor.

The key concepts which must be considered in planning an intrusion detection system and the site characteristics which affect the performance of both exterior and interior sensors were mentioned. Since each site is unique, a characterization will be required for each site. Performance characteristics (P_d, NAR/FAR, and vulnerability to defeat) of the total physical protection system, rather than of the individual sensor should be optimized. Weaknesses of individual sensor types can be compensated for by employment of combinations of more than one technological type of sensor. The outputs of these sensors can be combined with other pertinent system information (1) to produce an "operationally effective" physical protection system and (2) to achieve "protection-in-depth."

The ability to assess the cause of an alarm, even though it was not specifically discussed in this paper, is part of the other pertinent system information and must be included in the overall system planning.

Various sensor characterization and evaluation techniques were mentioned. Some of these are applicable for field use and others are limited to being useful in the laboratory. More complete information on the sensors discussed can be found in References 12 through 21.

ACKNOWLEDGMENTS

The author would like to express appreciation to the staff (both past and present) of the Intrusion Detection Systems Technology Division at Sandia Laboratories and to the staff of EG&G who have been assigned to the intrusion detection effort for their excellent technological assistance in sensor evaluation and reporting. It was from these efforts that the material in this paper

was drawn. I would also like to express appreciation to Tech. Reps., Inc. for their assistance in the preparation of the manuscript.

REFERENCES

1. H. E. Lyon, "The Role of Material Control and Development in ERDA's Safeguards Program," Journal of the Institute of Nuclear Materials Management, V, No. III (Fall 1976), 57-64.

2. Orval E. Jones, "Advanced Physical Protection Systems for Facilities and Transportation," Journal of the Institute of Nuclear Materials Management, V, No. III (Fall 1976), 211-225.

3. L. M. Brenner and S. C. T. McDowell, "ERDA's Integrated Safeguards System Program," Journal of the Institute of Nuclear Materials Management, V, No. III (Fall 1976), 292-301.

4. T. R. Canada, J. L. Parker, and J. W. Tape, "The U.S. ERDA Safeguards Technology Training Program," Journal of the Institute of Nuclear Materials Management, V, No. II (Summer 1977), 54-59.

5. Nuclear Proliferation and Safeguards, Congress of the United States, Office of Technology Assessment, Washington, D.C. (New York: Praeger Publishers).

   and also

   Appendix, Volume II, Part 2 to Nuclear Proliferation and Safeguards, Appendix VIII, Section 4.1, VIII-34 (OTA-E-50), June 1977.

6. H. E. Lyon, "The Many Faces of Safeguards," Journal of the Institute of Nuclear Materials Management, VI, No. III (Fall 1977), 37-43.

7. L. M. Brenner, "The Role of Containment and Surveillance in Integrated Safeguards Systems," Journal of the Institute of Nuclear Materials Management, VI, No. III (Fall 1977), 94-100.

8. Nuclear Safeguards Technology Handbook, HCP/D6540-01, U.S. Department of Energy, December 1977.

9. Measurement Reliability for Nuclear Material Assay, LA-6574, Los Alamos Scientific Laboratory of the University of California, January 1977.

10. Diversion Path Analysis Handbook, Vols. I and II, U.S. Department of Energy, Safeguards and Security, October 1976.

11. James D. Williams, "DOE/SS Handbooks--A Means of Disseminating Physical Security Equipment Information," Journal of the Institute of Nuclear Management, VII, No. 1 (Spring 1978) 65-76.

12. Intrusion Detection Systems Handbook, SAND76-0554, Sandia Laboratories, Albuquerque, New Mexico, November 1976 (Revised October 1977).

13. Sigmund Scala, "Generic Data Base for Modeling Safeguards Security Equipment Interim Report," Stanford Research Institute, prepared for Sandia Laboratories on Contract No. 05-8748, September 1977. [To be used in safeguards programs under the jurisdiction of the Nuclear Regulatory Commission (NRC)]

14. Catalog of Physical Protection Equipment (NUREG-0272) and Guide for the Evaluation of Physical Protection Equipment (NUREG-0273), U.S. Nuclear Regulatory Commission, January 1978.

15. R. A. Fite, Interim Report: Commercial Sensor Evaluation, MERADCOM, Ft. Belvoir, Virginia, August 7, 1975.

16. Siting Criteria for SAFE Programs, (SAFE-SIT-0001), Deputy for Command and Management Systems, Base and Installation Security System Program Office, July 1976 and Master Development Plan for the DOD Base and Installation Security Systems, April 1976.

17. Report on Sensor Technology for Battlefield and Physical Security Applications, MERADCOM, Ft. Belvoir, Virginia, July 1977.

18. "Selection and Application of Joint Services Interior Intrusion Detection System," Department of Army

Technical Bulletin TB 5-6350-262, Department of Air Force TO31S9-1-101, Department of Navy Navelex 0967,464-9010, February 1974.

19. Dennis L. Mangan, "DOE-Sponsored Evaluations of Interior Intrusion Detection Systems," 1978 Carnahan Conference on Crime Countermeasures Proceedings, May 15-19, 1978.

20. W. C. Garrett, Infrared Motion Sensor Evaluation, No. 2237, U.S. Army Mobility Equipment Research and Development Command, Ft. Belvoir, Virginia, March 1978.

21. Dennis L. Mangan, "The DOE Handbook on Intrusion Detection Systems," submitted for publication in Nuclear Safety.