U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

DRAFT REGULATORY GUIDE

April 1996
Division 5
Task DG-5007

Contact: P. Dwyer (301)415-8110
E. Suarez (301)415-8094

DRAFT REGULATORY GUIDE DG-5007
(Proposed Revision 3 to Regulatory Guide 5.44)

PERIMETER INTRUSION ALARM SYSTEMS

A. INTRODUCTION

Part 73, "Physical Protection of Plants and Materials," of Title 10 of the Code of Federal Regulations specifies performance requirements for the physical protection of nuclear power reactors, fuel facilities, and special nuclear materials. The general performance objectives and requirements that must be met through the establishment of a physical protection system are described in 10 CFR 73.55(a) and 73.20(a). Performance capabilities necessary to meet these requirements are described in 10 CFR 73.55(b) through (h) and in 10 CFR 73.45. For power reactors, 10 CFR 73.55(c)(4) requires detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier to ensure that adequate response by the security organization can be initiated. Adversaries are presumed to be determined and knowledgeable. For certain fuel cycle facilities, the use of an intrusion detection subsystem with the capability to detect penetration through the isolation zones is specifically set forth in 10 CFR 73.46(e)(1).

This guide describes the functions of perimeter intrusion detection sensors and detection methods that are acceptable to the Nuclear Regulatory Commission (NRC) staff for meeting those specified portions of the Commission's regulations described above. It provides guidance on sensors and methods that can be integrated to form an effective perimeter intrusion detection system. This guide was prepared to furnish

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received complete staff review and does not represent an official NRC staff position.

Public comments are being solicited on the draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rules Review and Directives Branch, DFIPS, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Copies of comments received may be examined at the NRC Public Document Room, 2120 L Street NW., Washington, DC. Comments will be most helpful if received by **June 25, 1996.**

Requests for single copies of final and draft guides (which may be reproduced) should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Office of Administration, Distribution and Mail Services Section, or faxed to (301) 415-2260. Requests for placement on an automatic distribution list for single copies of future draft guides in specific divisions should be made in writing to the same address..

nuclear power reactors and strategic special nuclear material processing facilities.

Regulatory guides are issued to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the Commission's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and guidance to applicants. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required. Regulatory guides are issued in draft form for public comment to involve the public in the early stages of developing the regulatory positions. Draft regulatory guides have not received complete staff review and do not represent official NRC staff positions.

Any information collection activities mentioned in this draft regulatory guide are contained as requirements in 10 CFR Part 73, which provides the regulatory basis for this guide. The information collection requirements in 10 CFR Part 73 have been cleared under OMB Clearance No. 3150-0002.

B. DISCUSSION

GENERAL

The effective use of a perimeter intrusion detection system is influenced by a number of factors. These factors include the environment; the selection, application, and installation of equipment; testing and maintenance of the particular sensor types used; the ability of the security organization to assess incoming alarm data in a timely manner; and the overall integration of the system. A perimeter intrusion detection system generally consists of one or more sensors, electronic processing equipment, a power supply, signal transmission media, an alarm monitor with display, and a means for maintaining and providing an alarm history.

Sensor systems can be classified, from an applications viewpoint, as either line-of-sight or terrain-following, and from a functional viewpoint, as either volumetric or planar. For line-of-sight systems to be effective, the terrain surface must be relatively flat with no significant contour depressions or elevations. In terrain-following systems, the sensor's detection pattern can adapt to some changes in the terrain's contour. The terms volumetric and planar refer to the general shape of the sensor's detection zone; the primary

difference between these terms concerns their depth dimension, or the distance an intruder must travel to pass through the sensor's detection zone. The depth dimension for a planar sensor is minimal to near zero (much like a plate of glass). A taut wire system is an example; the intruder must contact the wire to cause an alarm. In contrast, a microwave sensor creates a volumetric beam pattern having a depth of up to several feet.

An intruder's ability to determine a sensor's detection zone boundary can compromise the sensor. Microwave detectors have invisible detection patterns. At best, an intruder can only estimate points where detection will occur. In contrast, the detection zone of a taut wire system can easily and accurately be determined. The wires constitute the detection zone.

In selecting a sensor capable of detecting an intruder, it is crucial to select and integrate sensors that will minimize false and nuisance alarm rates. (See Appendix A, Glossary, for definitions.) Selecting the best sensor for a perimeter section will minimize the false and nuisance alarm rates. In selecting the best sensor for a perimeter location, the following factors are considered.

- Fence, barrier, and isolation zone conditions
- Soil types and conditions, including blowing sand
- Drainage
- Suitability of the perimeter for segmenting into detection zones
- Nearby roads, airports, waterways, railroads, and the type of traffic they carry
- Perimeter penetrations (above and below ground) such as culverts, pipes, buried wires, and utilities
- Temperature extremes
- Precipitation (e.g., rain or snow) amounts and rates, including ice accumulation and blowing snow
- Thunder and lightning frequency and severity
- Natural foliage
- Wildlife types, population densities, and activity at or near the perimeter
- Electromagnetic interference potential, including radio frequency interference potential.

Some typical commercially available sensor systems are described below.

SENSOR SYSTEMS

Microwave Systems

Microwave systems are line-of-sight and volumetric, and they are found in two basic configurations: (1) bistatic, consisting of a transmitter and receiver remote from each other at either end of a microwave link, and (2) monostatic, with receiver and transmitter located in the same unit.

Each link of a bistatic microwave perimeter detection system is composed of a transmitter, receiver, power supply, signal processing unit, signal transmission system, and an output for connection to an annunciation device. The transmitter radiates a low-power, three-dimensional, typically modulated microwave signal toward the receiver. The receiver detects, amplifies, and processes the signal. A reference rate of microwave energy transfer is established while the transmitter is unobstructed. When an intruder enters the space defined by a conical beam, the total amount of microwave signal energy entering the receiver is reduced from the established reference level. This causes the receiver to generate an alarm. The microwave beam is typically modulated to reduce interference from spurious sources of radio frequency energy, to increase sensitivity, and to decrease the vulnerability to defeat by the receiver capturing a false microwave source.

A monostatic microwave unit consists of a transmitter and receiver in the same unit along with a power supply, signal processing unit, signal transmission system, and an output for connection to an annunciation device. There are two different kinds of monostatic microwave, amplitude modulated (AM) and frequency modulated (FM). AM monostatic microwave systems detect changes in the net vector summation (direct and reflected components) of the received signal, similar to a bistatic system. FM monostatic systems operate on a pulsed doppler principle and thus can provide range information in addition to detection. In general, the useful range of a monostatic microwave is considerably less than that of a bistatic system. For this reason, its exterior use is generally limited to short links or volumes covering portals or gaps in coverage between bistatic microwave transmitters and receivers.

Electric Field Systems

An electric field perimeter intrusion detection system is considered terrain-following if there is uniform grade between mounting supports. First generation systems are considered planar, while second generation systems are more volumetric in nature. A typical system consists of field wires, a field generator, sensing wires, a sensing filter, an amplifier, a discrimination unit, and an output for connection to an annunciation device. The field generator excites the field wires, creating an omnidirectional electrical field primarily between the field wires and the sensing wires (a field is also created between the field wires and the earth ground). Electric field systems range from 4 to 7 wire systems, i.e., from 2 sensing and 2 field wires up to 3 sensing and 4 field wires. A person approaching the system changes the pattern of the electric field. Sensing wires installed at different locations within the transmitted pattern detect changes occurring in the pattern. If the changes are within the frequency bandpass of objects comparable to an individual's movement, a detection signal is generated. Some systems have additional signal processing to discriminate between people and what would otherwise be nuisance alarms.

Ported Coaxial Cable Systems

A ported coaxial cable system, considered to be terrain-following and volumetric, consists of two buried shielded coaxial cables, transmitters, detectors, power supply, processing unit, and an output for connection to an annunciation device. Radio frequency (RF) energy is transmitted along the transmission line and is radiated through ports in the shield strands. This RF energy can be either pulsed or continuous wave. The pulsed system operates in principle as a guided radar, and thus an intruder is both detected and located. The continuous wave system detects the intruder but does not localize the intruder's presence along the cable length. The transmit-receive antenna pattern that is set up between the two cables produces a zone of detection around and between the transmitting and receiving lines. Changes in this electromagnetic field that exceed threshold levels cause an alarm. The system detects moving targets in the zone of detection, and the signal is digitally processed to provide enhanced signal characteristic identification. The

received signal is generally processed to reduce interference from nearby RF emitters.

Active Infrared Multibeam Systems

Active infrared multibeam systems are considered line-of-sight and planar. Each link of an infrared system is composed of a transmitter, receiver, power supply, signal processor, signal lines, and an output for connection to an annunciation device. The transmitter directs a narrow infrared beam to a receiver. If the infrared beam between the transmitter and receiver is interrupted, an alarm is generated. The infrared beam is usually modulated. Since the infrared beam does not diverge significantly, multiple infrared beams between transmitters and receivers can be used to define a "wall." If this "wall" is then penetrated, an alarm will result. (**Note**: The term "active infrared" is used to distinguish these systems from "passive infrared" systems. Passive infrared systems do not emit infrared energy, but instead, simply "look" at their field of view and detect changes in the ambient infrared patterns or intensity levels.)

Taut Wire Systems

A taut wire system is a terrain-following (with ground leveling) planar system. The system consists of a series of steel wires, typically barbed, securely anchored on posts and stretched parallel to the ground. The wires are closely spaced to prohibit climbing between the wires without causing an alarm and are typically tensioned to 36 kg (80 lb). Deflection of or cutting one or more of the tensioned wires activates a sensing device connecting each wire to either a sensing post or anchor post. The sensing device may be a simple switch, strain gauge device, or other passive transducer. Slider posts are generally used to further support the wires, typically at 3-meter (10-foot) intervals.

Fiber Optic Systems

Fiber optics refers to light transmission through specially constructed optical fibers for communications, sensing, or imaging. Optical fiber consists

of a light-guiding core and a surrounding optical "insulator" called the cladding. The core has a higher index of refraction than the cladding, which permits total internal reflection if the angle of incidence is greater than the critical angle. Light can thus be confined in the core and transmitted along the length of the fiber.

A number of different techniques are being used in the developing technology of fiber optic intrusion detection. Speckle pattern and interferometry are two common techniques. In the speckle pattern technique, when light is sent through the optical sensing cable of the system, it appears at the end of the cable as a speckled pattern of light and dark spots. The patterns of light and dark are caused by the many different modes or paths through which light can travel in a multi-mode fiber optic cable. When the cable is stationary, the pattern is stationary. However, when pressure is applied to the cable, the light distribution through the cable is changed. This change redistributes the speckle pattern of light and dark. These speckle patterns are converted to usable electrical signals through the use of a photo-diode. An alarm processing unit uses this information to determine whether an alarm has occurred.

Interferometry can also be used to determine changes in the optical sensing cable. This technique uses wavelength-division multiplexing, which is a method capable of sending multiple signals at different wavelengths through the same fiber. The detection method involves monitoring mode interference changes of the light that are caused by pressure, vibration, or motion. To optimize detection capability and minimize nuisance alarms for a particular installation, the system allows the user to select appropriate processing parameters to qualify a disturbance as an alarm. The parameters include the frequency band, energy level and duration of the disturbance, and the number of disturbances within a specified time. Fiber optic systems using these techniques for detection are considered terrain-following and either volumetric or planar, depending on the specific installation and use.

Vibration or Strain Detection Systems

A variety of devices that detect strain or vibration are available for use as fence-mounted intrusion detection systems. Typically, such systems are considered terrain-following and planar. Although the devices vary greatly in

design, each basically detects strain or vibration of the fence on which it is mounted, such as that produced by an intruder climbing or cutting the fence. In the simplest devices, the vibration or strain makes or breaks electrical continuity and thereby generates an alarm. In more complex systems, vibration or strain changes light transmission characteristics through fiber optics.

C. REGULATORY POSITION

1. DESIGN OBJECTIVES AND INTEGRATION

1.1 Layout

In designing an effective perimeter intrusion detection system, dividing the site perimeter into segments that are independently alarmed and uniquely monitored assists the security organization in assessing and responding to an alarm by localizing the area in which the alarm is initiated. The perimeter segment lengths should be selected with consideration of such factors as range; limitations of the sensor system; and the location, alignment, and viewing areas for closed circuit television (CCTV) cameras, when CCTV is used for alarm assessment. Segmenting the perimeter alarm system also allows testing and maintenance of a portion of the system without affecting the remainder of the perimeter. The individual segments should generally be limited to a length that allows observation of the entire segment by an individual standing at one end of the segment. This typically means that segments should not exceed 100 meters (328 feet), but shorter segments may be needed to achieve the desired performance.

The ground surface of the detection zone should be prepared by stabilizing the soil to prevent the growth of vegetation along the length of the zone. Depending on the system type, this may help to minimize nuisance alarms caused by the movement of high grasses, etc. Measures for accomplishing stabilization include surfacing or soil sterilization. Isolation zones on either side of the detection zone also help to provide a clear zone for assessment. For all systems, the distance between the bottom of the detection zone and the ground plane should not be large enough for an individual to pass undetected under the detection zone and thereby circumvent the system.

Perimeter intrusion detection systems should be placed to maximize detection and assessment capabilities and minimize nuisance and false alarm rates. The following factors should be considered in locating the detection system.

1.1.1 The system should be located so that items such as existing (or planned) barriers, sensor mounts,[1] light poles, or natural terrain objects (e.g., trees) cannot be used as aids for bridging the sensor's detection pattern, blocking assessment, or providing cover and concealment.

1.1.2 There should be sufficient distance between the zone of detection and any areas of concealment to ensure assessment of the alarm prior to the intruder's concealment. [This distance is related to the time needed to circumvent barriers, time needed to reach a concealment location, and specific assessment capabilities at the site.] Digital video frame storage systems are one means of addressing site-unique assessment problems by capturing video frames before, during, and after an actual intrusion.

1.1.3 Pedestrian and vehicular traffic should be located away from the zone of detection to reduce nuisance alarms.

1.1.4 Sources of strong, fluctuating electromagnetic fields (such as large transformers and electrical power distribution subsystems) should be considered when selecting sensors susceptible to such disturbances (e.g., the electric field sensor and the ported coaxial cable system).

1.1.5 Site-specific environmental conditions should be considered in selecting the system. For example, sites where fog sometimes obscures visibility may not be suitable for beam-breaker type systems, such as the active infrared multibeam system, which may have its detection capability degraded by the fog's beam-scattering effect.

---

[1]After adjustments in sensor position are complete, it might be necessary to remove excessive lengths of mounting poles.

1.2 Detection and Alarm Capabilities

Optimum detection capabilities for any particular sensor system are achieved when the sensor selected has a detection volume suited to specific segment configuration and terrain. In general, volumetric systems are preferred because they are generally more difficult to defeat. However, for certain limited site configurations, planar systems may provide coverage with fewer false or nuisance alarm rates compared to a volumetric-type sensor.

Some systems that may alone be unacceptable for meeting detection performance requirements may, under certain circumstances, be enhanced and combined with other systems for a combined, improved performance. Such combination systems should employ dissimilar detection techniques. This combination of different sensing techniques requires an intruder to defeat two (or more) types of different sensing methods at the same time, which would significantly increase the difficulty of defeating the system.

The design goal of a perimeter intrusion detection system is to detect an individual weighing a minimum of 35 kg (77 pounds), whether the individual is running, walking, crawling, jumping, or rolling through the perimeter of a protected area. Further, the design goal of a perimeter intrusion detection system should be to limit false alarms and nuisance alarms to a total of not more than one false alarm per zone per day and one nuisance alarm per zone per day.

Because nuisance alarm rate data are extremely specific to location and detection technique, data should be gathered for the first year after a new system is installed to gain system experience and to allow for system alterations. After that period, the data should be examined to establish site-specific rates for both nuisance and false alarms. The findings should be reflected in adjustments to security plan commitments based on site-specific operational and environmental circumstances and actual performance at the site. Such revisions to security plans may be submitted under the provisions of 10 CFR 50.54(p) if the changes do not represent a decrease in effectiveness of the security plan. Settings of adjustable parameters should be recorded and future changes should be recorded with justifications.

Licensees should be able to observe, in a timely manner, the bridging of a detection zone or to justify to NRC that successful completion of a bridging attempt is not feasible.

The system should be designed to annunciate, audibly and visibly, under the following additional conditions:

- Placement of any portion of a perimeter intrusion detection system in the access mode,[2]
- A unique indication, other than a normal alarm, of a switchover to emergency or secondary sources of power,
- Any interruption or reduction of system power to the degree that any part of the system is not functioning properly,
- Any indication of tampering (e.g., opening, shorting, or grounding of the sensor circuitry) that renders the device incapable of normal operations;
- Any indication of tampering by activation of a tamper switch or other triggering mechanism.

1.3 System Electrical Specifications

If primary power is interrupted, the system should contain provisions for automatic switchover to emergency power (battery and generator) without causing false alarms and without causing a loss of system function or data. Emergency power should be capable of sustaining operation without external support for a minimum of four hours for Category I fuel cycle facilities, or for a site-specific period of time determined according to station blackout criteria for power reactor facilities. If emergency power is furnished by battery, all batteries (including stored batteries) should be maintained at full charge by automatic battery charging circuitry designed according to IEEE Standard 450, "Recommended Practice for Maintenance, Testing, and Replacement of Large Lead Storage Batteries for Generating Stations and Substations" (1987).[3]

---

[2]Access mode means the condition that maintains security over the signal lines between the detector and the annunciator and over the tamper switch in the detector but allows access into the protected area through the zone of detection without indicating an alarm condition.

[3]Copies may be obtained from the IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855.

1.4 Tamper-Indicating Systems

All enclosures containing controls that affect the operation and sensitivity of the detection system and all access point controls should be located within a tamper-indicating enclosure. The electronics should be designed so that tamper-indicating devices remain in operation even though the system may be placed in the access mode. At power reactor sites only, cable pull boxes and termination points need not be tamper-protected if line supervision is used, unless there are splices at the location. Also, at power reactor sites only, annunciator equipment located within the central and secondary alarm stations need not be as protected as facilities other than power reactors.

1.5 System Line Supervision

All signal lines connecting detection devices to alarm stations should be supervised.[4] If the processing electronics are separated from the sensor elements and are not located within the detection area of the sensor elements, the signal lines linking the sensors to the processing electronics should also be supervised. Line supervision on these communication paths should protect against simple electrical bridging of the system or compromise of the system by any of the following means.

- The substitution of resistance, voltage, or current,
- The substitution of equipment of the same design and manufacturer,
- Reintroduction by playback of signals previously recorded onto the communication path,
- Synthesizing signals externally and introducing these synthesized signals onto the path.

---

[4]Signal line supervision is discussed in NUREG/CR-5723, "Security System Signal Supervision" (September 1991). Copies may be purchased at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-1800); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161.

The tamper switch and transmission medium should be supervised to the same extent in the secure mode as when the sensor is conditioned for authorized access.

1.6 System Vulnerabilities

Licensees are cautioned that any sensor system may have one or more design vulnerabilities that may enable the system to be compromised by a knowledgeable intruder. For this reason, it is important that all equipment be installed per manufacturers' specifications and meet the performance criteria required by 10 CFR Part 73 as clarified in this regulatory guide. In some instances, the combination of different sensor types can yield improved performance with a reduction in vulnerabilities. (See Regulatory Position 1.2, "Detection and Alarm Capabilities," on combining sensors.) Licensees should consider requesting that a system manufacturer be present during final acceptance testing of a perimeter intrusion detection system to be sure that the system has been properly installed.

1.7 Assessment

A perimeter intrusion detection system is incomplete without some means to assess and resolve alarms. It is imperative that the assessment techniques identify the stimulus in a timely manner before the stimulus of the alarm disappears from view. The time an intruder takes to run through the isolation zones and disappear from the field of view of the assessment mechanism should be greater than the time required to visually acquire and evaluate the alarm information. If the required protected area barriers and isolation zones adjacent to the intrusion detection system do not provide sufficient delay to ensure assessment, additional means should be taken to increase delay or improve assessment (e.g., an additional fence, concertina rolls, razor tape, higher fence, video-capture monitoring techniques). Care should be taken that the means used to provide additional delay do not interfere with assessment capabilities. The following are acceptable methods of assessment.

1.7.1 CCTV systems that are fixed and properly positioned may be used to provide assessment information to the alarm station operators. It is

important to select and orient equipment to maximize fields of view and, thus, maximize assessment time for evaluating intruders passing through detection zones. These systems should be designed to display immediately, using the same signal that activates the annunciation. Video-image capture devices with the capability to record an adversary within the zone of assessment and immediately prior to detection are an acceptable alternative to alarm-activated display monitors. At Category I fuel cycle facilities, alarm-activated display monitors should continuously display and not "go blank" during quiet periods (periods of no alarm). Pan/tilt/and zoom (PTZ) cameras should also be used to augment fixed camera installations, as an adjunct to the fixed camera systems.[5]

1.7.2 Fixed guard posts can be effective if the posts are positioned so that there is a clear field of view of the assigned segment. These posts generally should be positioned at the end of the assessment area with the guard observing in one direction only. The intrusion detection system should annunciate in the local guard post as well as in both alarm stations. Consideration should be given to compensation for loss of guard observation capability during periods of reduced visibility such as darkness, rain, fog, and snow.

1.8 Maintenance

The regulations in 10 CFR Part 73 require that the perimeter intrusion detection system be maintained in an operable condition, thus a preventive maintenance program is necessary. Maintenance of the detection, alarm communication, annunciation, and assessment system is critical to successful operation. Licensees should establish an ongoing program for maintenance. In

---

[5]Video systems are discussed in NUREG/CR-5721, "Video Systems for Alarm Assessment" (D.A. Greenwoll and J.C. Matter (SAND91-0947), USNRC, September 1991). Copies may be purchased at current rates from the U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20402-9328 (telephone (202)512-1800); or from the National Technical Information Service by writing NTIS at 5285 Port Royal Road, Springfield, VA 22161. Copies are available for inspection or copying for a fee from the NRC Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington DC 20555; telephone (202)634-3273; fax (202)634-3343.

addition, maintenance may be initiated by the testing program, operational requirements, or from the routine periodic maintenance program.

The amount of time that equipment is out of service should be minimized to preclude the overuse of compensatory measures. The maintenance group should be effective and respond in a timely manner. The use of dedicated on-site maintenance technicians has proven effective to ensure perimeter intrusion detection system operability and proper performance.

2. PERIMETER INTRUSION DETECTION SYSTEMS -- MINIMUM QUALIFICATIONS

2.1 Microwave Systems

2.1.1 Installation Criteria

Bistatic transmitters and receivers should be installed on even terrain clear of trees, tall grass, standing or running water, and bushes. Typically, a bistatic microwave perimeter detection system should be installed to operate effectively in a range not more than 100 meters (approximately 328 feet) long. Some models are designed to operate over short ranges, e.g., across perimeter portals. Successive microwave links and corners should overlap to eliminate dead spots (areas where the microwave beam cannot detect) below and immediately in front of transmitters and receivers. The required amount of overlap of successive links is contingent on the antenna pattern and unit height. Each unit should be mounted rigidly on secure posts at a sufficient distance above the ground that incident and reflected signals combine positively, typically 60 cm (24 inches) for 100 meters (328 feet), or according to the manufacturer's installation criteria. Because of variances in the antenna patterns of different microwave systems, the height may have to be varied slightly to obtain coverage adequate to detect crawling intruders. Accordingly, the mounting mechanisms for a system should permit adjustment of antenna height and position to correct poor performance or alignment.

Receiver units for a microwave link may also need to be specially protected because of their susceptibility to tampering by a knowledgeable intruder or to "receiver capture" through electronic means. "Receiver capture" occurs when a receiver recognizes a false transmission signal as its own. Means available to minimize vulnerabilities include the use of monostatic microwave to protect the area where the receiver head is located or the use of additional

perimeter intrusion detection equipment, such as an electric field system, configured to require penetration of a detection zone in order to access a receiver head. As with bistatic receiver heads, monostatic transceiver heads may be vulnerable to certain tampering methods and must also be protected, possibly by placement inside another sensor's detection zone as described above.

Stacking of microwave sensors is one means of increasing the elevation-detection-zone height of the system to enhance its detection capabilities. The stacking technique, in effect, fills in the dead zones that can be inherent in simple bistatic systems. Additionally, the use of stacked units can help detect the bridging or jumping of a detection zone.

Since the bistatic transmitter/receiver link is a line-of-sight system, variations in ground level (e.g., ditches and valleys) may allow some intruders to crawl under the beam, and variable obstructions (e.g., snow drifts or accumulations) may interrupt the beam. To prevent passage under the microwave beam, variations in the ground should be leveled, ditches should be filled, and obstructions should be removed so that the area between the transmitter and receiver is clear of obstructions and free of rises or depressions. The distance between the bottom of the detection zone and the ground plane must be such that a person cannot crawl under the zone undetected. Typically, this means that penetrations greater than or equal to "man-sized" must be detected. That is, the distance between the bottom of the detection zone and the ground could not accommodate a "man-sized" penetration without detection. Man-sized is considered to be 648 square centimeters (96 square inches) with one dimension 15.4 centimeters (6 inches) or more. The clear area should be sufficiently wide to preclude the generation of alarms by legitimate movements near the microwave link (e.g., personnel walking or vehicular traffic) and to preclude system degradation caused by reflections from any structure, such as the perimeter fence. Approximate dimensions of the microwave pattern should be provided by the manufacturer.

Motion or disturbance of objects such as tumbleweed, paper, and bushes moving in the path of the beam can cause nuisance alarms. Since the beam is relatively wide, care must be taken to ensure that reflections from authorized activities do not create nuisance alarms. With the microwave link installed inside a perimeter barrier or between a double perimeter barrier, the transmitter and receiver should be positioned to detect anyone jumping over the microwave beam into the protected area from atop the perimeter fence or wall.

Typically, the distance between a chain link security fence with an overall height of 2.4 meters (8 feet) and the center of the microwave beam should be a minimum of 2.4 meters (8 feet). In addition, the microwave link should be positioned within the isolation zone to enhance assessment once detection is made. Neither a transmitter nor a receiver should be mounted on a fence unless prior approval is received from the NRC. Overlapping transmitter/receiver paths should also be designed to prevent bridging from transmitter or receiver posts and to prevent an intruder from moving undetected behind units. Similarly, care should be taken to be sure that mounting posts cannot be used as step-off points for jumping over the zone of detection.

2.1.2 Performance Criteria

A microwave perimeter detection system should be capable of detecting an intruder weighing a minimum of 35 kilograms (77 pounds) passing anywhere between the transmitter and receiver, including the area in front of both the transmitter and receiver, whether the individual is walking, running, jumping, crawling, or rolling. The beam should be modulated and the receiver should be limited to respond to selected frequencies to decrease susceptibility to "receiver capture."

2.2 Electric Field Systems

2.2.1 Installation Criteria

Electric field systems should be installed with zones that are limited to 100 meters (328 feet) or less in order to have effective detection sensitivity for assessment and response. The system can be mounted on metal, plastic, or wooden posts using specially designed electrical isolators that allow for small movements of the posts without disturbing the field and sensing wires. Both the field and sensing wires need to be under a high degree of spring tension to produce high-frequency vibrations when they are struck by small foreign objects or blown by the wind, both of which are out of the bandpass of the receiving circuitry.

For most applications, the electric field sensor should consist of a minimum of two field wires and two sensing wires. The wires should be spaced so that an individual moving between the wires cannot be detected. It is important that the lowest wire of any electric field system be consistently close enough

to the ground to detect crawling under the field. Accordingly, the bottom sensing wire should be located 15.4 centimeters (6 inches) or less above ground level. The field wires should be located between the sensing wires per the manufacturer's specifications. The electric field detector is not a line-of-sight system and therefore can be installed on uneven terrain and in an irregular line. However, the terrain between posts must be of uniform grade so that the sensing wires can be installed parallel to the ground.

Because of the characteristics of an electric field detection pattern, the system should not be mounted on or near a fence that an intruder could use to jump over the field. In addition, if the electric field system is mounted on the side of a wall, the stand-off from the supporting barrier should not permit crawling between the barrier and the system. The surrounding terrain within 3 meters (10 feet) of field wires should be free of all shrubs, trees, and undergrowth.

The system should be well grounded per the manufacturer's recommendations along its entire length with special care given to the sections that go over walls or buildings. The control unit should be well grounded using a 1-meter (39-inch) or longer grounding rod or equivalent electrical ground. Grounding may be difficult under dry earth conditions. The resistance between ground rods and earth should also meet manufacturer's recommendations.

Electric field systems should be tuned or overlapped if necessary to overcome any lack of sensitivity in the areas around tension springs and end insulators. Monostatic microwave could also be used to protect these areas. Each wire should be kept free of nicks, cuts, etc. and be properly tensioned per manufacturer's recommendations along its entire length. Systems mounted on chain-link fence are susceptible to wind-caused alarms and should be avoided. There may be some loss of sensitivity in the vicinity of metal posts used to support electric field fences. If site conditions necessitate installations over buildings, nonmetallic posts (e.g., wood or fiberglass-reinforced plastic) should be used to prevent gaps in the detection zone.

2.2.2 Performance Criteria

An electric field perimeter detection system should be able to detect an individual weighing a minimum of 35 kilograms (77 pounds) whether the individual is crawling or rolling under the lowest wire, stepping or jumping between the wires, or jumping over the wires. The field and sensing wires should be

supervised to prevent undetected cutting or bypassing of the system by electronic or clandestine means.

2.3 Ported Coaxial Cable Systems

2.3.1 Installation Criteria

Ported coaxial cable systems should be installed per the manufacturer's specifications. The maximum and minimum separation of the transmitter and receiver can vary. Generally, this type of system can operate in longer segments than other detection systems. However, it is recommended that detection zones be restricted to segments of 100 meters (328 feet) or less to facilitate assessment. The system is terrain-following and can be curved around corners. The lines are generally buried approximately 18 centimeters (7 inches) deep and 1 to 3 meters (3 to 10 feet) apart. Soil conductivity should be considered when installing this type of sensor. Soil found to have relatively high conductivity may cause the detection field to be reduced. Highly conductive soil includes soil that contains concentrations of iron or salt. Moving objects in the zone of detection such as foliage, rippling water, and grasses may create nuisance alarms. Rodents can chew through ported coaxial cable. Sensor locations should be selected carefully to prevent nuisance alarms from such sources as personnel and vehicular traffic. Similarly, the cleared area above the sensor should be defined and controlled to prevent the placement of objects within the area, even temporarily, which would degrade the detection zone. The transmitter and receiver transducer lines should be installed on well-drained terrain cleared of trees, tall grass, and bushes. System sensitivity may be affected by freezing or thawing of the surrounding terrain. Because local anomalies can cause variances in the antenna pattern, the separation between the lines may vary slightly in order to obtain proper ground coverage. Neither the transmitter nor the receiver lines should be mounted above ground. Approximate dimensions of the detection pattern should be provided by the manufacturer.

The system should be installed relative to perimeter fencing, so that the transmitter and receiver lines are positioned to prevent someone from avoiding detection by jumping over the electromagnetic field. Typically, the distance between chain-link security fencing with an overall height of 2.4 meters (8

feet) and the center of the detection zone should be a minimum of 2.4 meters (8 feet).

Manufacturer's instructions should be followed when installing cable across concrete or asphalt areas. Particular attention should be paid to the binding agent and applying epoxy over the cable groove after the cable is installed in the concrete or asphalt.

2.3.2 Performance Criteria

A ported coaxial cable perimeter detection system should be capable of detecting an individual weighing a minimum of 35 kilograms (77 pounds) passing over the transmitter and receiver wires, whether the individual is walking, running, jumping, crawling, or rolling. The electromagnetic field should be modulated, and the receiver should be frequency selective to decrease susceptibility to "receiver capture."

2.4 Active Infrared Multibeam System

2.4.1 Installation Criteria

When installing an active infrared multibeam system, the maximum distance between transmitter and receiver should permit proper operation during conditions of severe atmospheric attenuation that are typical for the site. The maximum distance between transmitter and receiver is generally 80 meters (260 feet). The infrared perimeter system should be installed so that, at any point, the lowest beam is 15.4 centimeters (6 inches) or less above grade and the highest beam is **at least** 2.6 meters (8.5 feet) above grade to prevent bridging. The beams should be sufficiently interlaced that an individual could not penetrate between the beams and remain undetected. The transmitters and receivers should be rigidly mounted (e.g., installed on a rigid post in a concrete pad extending below the frost line) to prevent nuisance alarms from vibrations or ground shifting. Systems with heights greater than 2.6 meters (8.5 feet) should be specially stabilized to prevent vibration-caused alarms, for example, by mounting on a building wall. Each post on which a transmitter and receiver is mounted should be provided with a pressure-sensitive cap to detect attempts at scaling or jumping over the post. Successive infrared links should overlap at corners to eliminate any dead spots, which precludes the use of common posts at corners.

Fog, rain, and snow can attenuate and disperse the infrared beam and can cause nuisance alarms. However, the system can be designed to compensate for severe atmospheric attenuation. Dust on the face plates will also attenuate the infrared beam, as will an accumulation of condensation, frost, or ice.

Condensation, frost, or ice may be eliminated by using heated face plates. Sunshine on the receiver may cause nuisance alarms. A misalignment of transmitter and receiver caused by frost heaves may also cause nuisance alarms. Like the microwave system, vegetation such as bushes, trees, or grass and accumulated snow will interfere with the infrared beam. The passage of an intruder may go undetected on irregular ground surfaces, ditches, or hills.

The transmitter and receiver units should be positioned a minimum of 3 meters (10 feet) from perimeter fencing. The infrared detection system should not be installed directly adjacent to a barrier, since the barrier may provide a solid base from which an intruder could jump over the beams into the protected area.

2.4.2 Performance Criteria

An infrared perimeter detection system should be a multibeam modulated type, consisting of a minimum of six beams per segment. The system should be capable of detecting an individual weighing a minimum of 35 kilograms (77 pounds) passing between the transmitters and receivers whether the individual is walking, running, jumping, crawling, or rolling. This means that the infrared beams should be placed and interlaced such that the infrared "wall" formed has no openings greater than or equal to "man-sized," i.e., any openings must be less than 648 square centimeters (96 square inches) with one dimension 15.4 centimeters (6 inches) or less. Furthermore, the systems should be able to operate as above with a factor of 20 (13dB) insertion loss from atmospheric attenuation (e.g., fog) at a maximum range of 80 meters (260 feet).

2.5 Taut Wire Systems

2.5.1 Installation Criteria

Manufacturer's specifications should be followed in the installation of the system. However, because of the basic operating principle of the system (i.e., tensioned wires), the length of the segments should be limited to 60 meters (200 feet) or less. The overall height of the system should be 3.7

meters (12 feet) or greater. Wires should be spaced so no intruder can pass between the wires without detection, normally a distance of 15.4 centimeters (6 inches) or less between wires. A sensing post should be placed approximately halfway between anchor posts. (Anchor posts may function as sensor posts in certain models.) To provide additional system support, slider posts should be spaced approximately every 3 meters (10 feet) between the anchor post and sensor post or between anchor posts. The system may be installed on chain link fencing or an existing wall with a standoff equal to or less than 15.4 centimeters (6 inches). When installed on chain-link fencing, the taut wire system should be installed on the interior or protected area side of the fence. The ground within 1 meter (39 inches) on either side of the taut wire system should be stabilized to prevent erosion and to maintain the bottom wire at 15.4 centimeters (6 inches) or less above the ground.

2.5.2 Performance Criteria

The system should be installed so that an alarm is received on deflection of any wire that causes a vertical opening greater than 15.4 centimeters (6 inches).

2.6 Fiber Optic Systems

2.6.1 Installation Criteria

Since the use of fiber optics in intrusion detection is a fairly new technology, licensees are encouraged to consult with the NRC on site-specific usage. Manufacturer's guidelines for installation should be followed. Segments should be limited in length to 100 meters (328 feet). Since such systems detect pressure, motion, or vibration, they are sensitive to many of the vulnerabilities found under vibration- or strain-sensitive systems or buried line technologies.

2.6.2 Performance Criteria

A fiber optic detection system should be capable of detecting an individual weighing a minimum of 35 kilograms (77 pounds) passing over the cable, whether the individual is walking, running, jumping, crawling, or rolling.

2.7 Vibration or Strain-Detection Systems

If used, a vibration or strain-detection system should be installed in accordance with the following criteria and used only as a secondary intrusion detection system to augment the detection capabilities of a primary system.

2.7.1 Installation Criteria

Depending on the variety of sensor, each sensor can monitor a length of fence ranging from about 1 meter (39 inches) to several hundred meters. Vibration or strain-detection devices for fence protection generally are susceptible to nuisance alarms caused by wind vibrating the fence, hail stones, or large pieces of trash blowing against the fence. The frequency of nuisance alarms caused by the wind can be reduced by rigidly mounting the fence and thereby lessening the propensity of the fence to vibrate in the wind. Electronic signal-processing equipment used in conjunction with signal-generating strain transducers can effectively reduce nuisance alarm rates without sacrificing sensitivity to climbing or cutting the fence. Increasing the fence height also appears to enhance sensor performance. However, most fence detection systems can be bypassed easily by a variety of methods.

2.7.2 Performance Criteria

Vibration or strain-detection systems used for fence protection should detect an intruder weighing a minimum of 35 kilograms (77 pounds) attempting to climb the fence. The system should also detect any attempt to cut the fence or lift the fence fabric 15.4 centimeters (6 inches) or more above grade. The system should not generate excessive nuisance alarms.

2.8 Other Intrusion Detection Systems

Some systems currently under development may be acceptable, when fully developed, for use at NRC-licensed facilities. Other systems that currently do not have an acceptable detection performance capability may at some future time be refined and be found suitable. In either case, these systems would have to be performance tested by the licensee and a qualified independent agent prior to consideration by the NRC.

3. RECOMMENDED TESTING PROCEDURES

In conducting any testing procedures, care should be taken to ensure the safety of the individuals performing the testing. The standard Occupational Safety and Health Administration procedures and practices should be followed.

Specification testing should take place at the initial installation of the equipment. If available, test procedures recommended by the manufacturer should be followed. As in all test situations, the area under test should be maintained under visual observation by a member of the security organization while the test is being conducted. For each perimeter segment, the test should (1) ensure that the system meets manufacturer's specifications and NRC-recommended detection probability, (2) verify that no dead spots exist in the zone of protection, and (3) verify that line supervision and tamper-protection in both the access and secure modes are functional. Records of initial testing capabilities, equipment sensitivity settings, or voltage outputs should be maintained by the licensee so that deterioration in equipment capability can be monitored.

Two acceptable options for testing, operational testing and performance testing, are described below. Other testing methods may be used if the methods are fully documented and are approved by the NRC.

3.1 Testing Option I -- Operational Testing

After the equipment has been installed and specification tested, the perimeter intrusion detection and alarm systems should be operationally tested in all segments at least once each seven days in the following manner. Testing may be conducted during routine patrols by members of the licensee's security force. The testing should be conducted by crossing the zone of detection or by disturbing the fence on which the system is attached to cause the system to alarm. Before the test, the individual making the test should notify the alarm stations that a test is about to be conducted. The detection system in all segments should be walk-tested in a different, preferably random, order every seven days, and the testing should be conducted throughout the week rather than conducting all tests on the same day. The testing should result in 100% detection on all segments every seven days. If the perimeter alarm system fails to detect an intrusion on one or more segments, corrective actions should be

taken and documented. Records should be maintained to document that all required testing has been accomplished.

At least semiannually, as well as after each inoperative state and after any repairs, the system should be performance tested. A 90% probability of detection with 95% confidence should be the design goal of the system. An acceptable performance testing method follows.

Model Performance Testing Program

Determine the most vulnerable area of each segment and determine the method of approach most likely to penetrate that segment, e.g., walking, running, jumping, crawling, rolling, or climbing. This determination will, in most cases, be sensor- and location-dependent. Note that vulnerability to penetration also varies with environmental conditions. Inclement weather may be a particularly good time for a realistic evaluation of perimeter vulnerabilities.

Test each segment using a combination of all the applicable penetration approaches at the most vulnerable area a total of 34 times. All 34 tests should result in successful detections.

If the minimum number of successful detections is not achieved, the system should be checked. If no problems with the system are discovered, 18 more tests should be made. If the minimum number of successful detections is achieved, in this case 51 out of 52 (see the following table), the testing for this segment can be ended. If no problems with the system can be discovered and not all intrusions are detected after 1 more test of 15 intrusions, the system must be upgraded to increase the detection probability to the required level. If problems with the system are discovered, the system should be repaired and 34 new tests performed. If there are 34 successful detections, testing can be ended.

Total No. of Tests	Minimum No. of Successful Detections	Maximum No. of Failures Detected
34	34	0
52	51	1
67	65	2

The penetration approach that is most difficult to detect should be attempted more frequently if an equal number of tests for each approach is not possible.

The segments should be tested in random order. This will protect against the possibility that environmental effects and other unknown factors that may affect the test results (detection or nondetection) always favor or handicap the same segment or method of approach. For example, if Segment 1 is always tested in the morning and Segment 2 is always tested in the afternoon and if the detection equipment is slightly more sensitive to intrusions in the morning, the conclusion might be drawn from the test results that Segment 2 is less protected than Segment 1. However, the difference noted between the two segments might only be due to the morning versus afternoon difference. Similarly, using random methods, no approach will be continually favored if the time sequence (ordering) affects the test results. This will protect against disturbances that may or may not occur and that may or may not be serious if they do occur. A random numbers table can be used to determine the order in which the segments will be tested.

Maintain records of the results of all tests performed. These records should include the segment number, date, time, and relevant environmental conditions when tests were performed. Records should be maintained consistent with 10 CFR 73.70.

3.2 Testing Option II -- Performance Testing

With this test option, one pass of a performance test is conducted in place of a weekly operational test. With proper system performance, semi-annual performance testing need not be conducted. Instead of a simple "go, no-go" operational test conducted by a member of the security force passing through the zone of a detector on a weekly basis as with the operational testing option, this performance type of test that is conducted weekly is identical to the performance test described in Section 3.1. The weekly performance test is conducted by determining the most vulnerable area of each segment and determining the method of approach most likely to penetrate that segment, e.g., walking, running, jumping, crawling, rolling, or climbing. This determination will, in most cases, be sensor- and location-dependent. Note that vulnerability

to penetration also varies with environmental conditions. Inclement weather may be a particularly good time for a realistic evaluation of perimeter vulnerabilities.

Each segment should be tested by using a combination of all the applicable penetration approaches at the most vulnerable area at least once a week. The penetration approach that is most difficult to detect should be attempted more frequently if an equal number of tests for each approach is not possible.

The segments should be tested in random order. This will protect against the possibility that environmental effects and other unknown factors that may affect the test results (detection or nondetection) always favor or handicap the same segment or method of approach. For example, if Segment 1 is always tested in the morning and Segment 2 is always tested in the afternoon and if the detection equipment is slightly more sensitive to intrusions in the morning, it might be concluded from the test results that Segment 2 is less protected than Segment 1. However, the difference noted between the two segments might only be due to the morning versus afternoon difference. Similarly, using random methods, no approach will be continually favored if the time sequence (ordering) affects the test results. This will protect against disturbances that may or may not occur and that may or may not be serious if they do occur. A random numbers table can be used to determine the order in which the segments will be tested.

Because this option for testing is conducted on a weekly basis, the performance of the system need only be determined annually, as opposed to semi-annually as with Test Option I. At the conclusion of a 12-month period, data accumulated from the weekly testing can be applied to totals used in determining performance levels.

In essence, improved weekly testing is conducted throughout the year, as opposed to Test Option I in which rudimentary weekly testing is conducted over 6-month periods along with extensive performance testing at the end of the period. The goal is improved testing over an annual period with reduced overall burden on the licensee.

Under Test Option II, if a sensor achieves 51 detections over a 52-week (annual) period through weekly testing of the segment, additional performance testing need not be conducted at the end of the year. (Traditional performance testing would still be required after each inoperative state or repair.)

Testing must never conclude on a nondetection. If two or more nondetections occur, accumulated data for the period may not be counted toward totals for performance testing and the accumulation of data must be restarted.

As described in the model performance testing program in Section 3.1, records of all tests performed should be maintained.

D. IMPLEMENTATION

The purpose of this section is to provide information to licensees and applicants regarding the NRC staff's plans for using this regulatory guide.

This draft guide has been released to encourage public participation in its development. Except in those cases in which an applicant proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the methods to be described in the active guide reflecting public comments will be used in the evaluation of applications for construction permits and operating licenses.

The active version of this guide may also be used to evaluate submittals from operating reactor licensees who propose modifications (i.e., changes initiated voluntarily by the licensee) to their current licensing basis if there is a clear nexus between the proposed modifications and this guidance. However, no backfitting is intended or has been approved in connection with issuance of this guide; any backfitting that may result from imposition of the new position in this context must be separately justified in accordance with the criteria of 10 CFR 50.109 and approved NRC backfitting procedures.

APPENDIX A

GLOSSARY

Access mode — The condition that maintains security over the signal lines between the detector and the annunciator and over the tamper switch in the detector but allows access into the protected area through the zone of detection without indicating an alarm condition.

Active system — A type of intrusion detection sensor that emits a signal from a transmitter and detects changes in the reception of that signal.

Bistatic system — As used with a microwave sensor, a sensor consisting of a transmitter and receiver remote from each other at either end of a microwave link.

Bridging — Circumvention of a perimeter detection system by traversing above the zone of detection.

Cladding — The reflective outer layer of an optical fiber that surrounds the light-carrying core. The cladding contains the light in the core and allows the fiber to guide light from one end to the other. The cladding has a lower index of refraction than the core.

Crawling — Crossing the detection zone lying prone on the ground with a low profile at an approximate velocity of 0.03 meter (1 inch) per second, body aligned perpendicular to the zone of detection.

Dead spot — An area in an intrusion detection zone where there is no detection capability.

Design stimulus — An individual weighing a minimum of 35 kilograms (77 pounds), running, walking, crawling, jumping, or rolling through the perimeter of a protected area.

False alarm — An alarm generated without an apparent cause.

False alarm rate — The frequency at which a particular alarm zone indicates a false alarm, the design goal for which is one per zone per day.

Index of refraction — A measure of a transparent material's ability to bend light, usually abbreviated as "n." The index of refraction is the ratio of the speed of light in a vacuum to the speed of light in the material.

Interferometry — Using the interference of light waves to precisely determine the wavelength of the light.

Isolation zone	An area adjacent to a physical barrier, clear of all objects that could conceal or shield an individual. For facilities required to have double protected area barriers, this zone should extend 20 feet on either side of the protected area barriers and include the area bounded by the barriers. For facilities required to have a single protected area barrier, the isolation zone should extend 20 feet on either side of the protected area barrier.
Jumping	Leaping over the zone of detection, including standing on a fence and attempting to leap across the zone of detection.
Line-of-sight system	As used with intrusion detection systems, a sensor that requires a terrain surface that is relatively flat, with no significant contour depressions or elevations.
Man-sized	An area of 648 square centimeters (96 square inches) with one dimension 15.4 centimeters (6 inches) or less.
Monostatic system	As used with a microwave sensor, a sensor that has the receiver and transmitter located in the same head or unit.
Multimode fiber	Optical fiber that permits more than one light mode to be propagated.
Nuisance alarm	An alarm generated by an identified input to a sensor or monitoring device that does not represent a safeguards threat.
Nuisance alarm rate	The frequency at which a particular alarm zone indicates a nuisance alarm, the design goal for which is one per zone per day.
Operational testing	Testing performed at the beginning and end of any period in which a system is used. If the period of continuous use is longer than seven days, under operational testing the system must be tested at least once every seven days.
Passive system	A type of intrusion detection sensor that produces no signal from a transmitter but simply detects energy emitted in its vicinity.
Performance testing	Testing conducted at least semi-annually, after each inoperative state, or after any repairs to ensure the design stimulus will be detected properly. An inoperative state for an alarm system or component exists, for example, when the power is disconnected to perform maintenance or when, for any other reason, both primary and backup power sources fail to provide power. Placing a properly operating alarm system in access would not constitute an inoperative state unless accompanied or followed by any of the conditions above.

Planar system	A system in which the distance an intruder must travel to pass through the detection zone is considered more two-dimensional, as a flat plane, than three-dimensional or volumetric.
Receiver capture	As used with a sensor system, the condition that occurs when a receiver recognizes a false transmission signal as its own.
Rolling	Crossing the detection zone on the ground with a low profile, body parallel to the zone of detection, and moving at an approximate velocity of 0.03 meter (1 inch) per second.
Running	Entering and leaving the zone of detection at an approximate velocity of 5 meters (16 feet) per second.
Secure mode	The condition that maintains security over the signal lines between the detector and the annunciator and over the tamper switch in the detector; the secure mode does not allow access into the protected area through the zone of detection without indicating an alarm condition.
Segment	One of several sections into which a perimeter intrusion zone might be subdivided to optimize sensor performance, compensate for unique terrain features or vulnerabilities, improve alarm assessment capabilities, or facilitate response force deployment.
Specification testing	Testing done after completion of the system's initial installation or replacement of any major component to verify that the system complies with (1) the manufacturer's specifications for design, installation, and adjustment, (2) performance criteria set by the NRC and the site, and (3) any other criteria on which the system's acceptability is based. Specification testing is more comprehensive than performance testing.
Speckle pattern	A light-interference pattern produced at the end of a multimode fiber that is being illuminated by a laser source.
Terrain-following system	As used with intrusion detection systems, a sensor with a detection pattern that can adapt to some changes in the terrain's contour.
Volumetric system	A system in which the distance an intruder must travel to pass through the detection zone is considered more three-dimensional than two-dimensional or planar.
Walking	Entering and leaving the zone of detection with a normal stride (2 30-inch steps per second).

APPENDIX B
CHECKLIST

This appendix contains checklists for each type of detection system. They may be used as reminders when planning, installing, or using the systems.

MICROWAVE

- Ensure that microwave sensors are set up so that they have a clear line of sight between transmitters and receivers.

- Ensure that microwave sensor systems are installed over flat ground to prevent shadowing (inadequate detection in depressions).

- Keep intersection angles of microwave beams as close as possible to 90 degrees, i.e., orthogonal.

- Never mount two microwave receivers on the same post.

- Remember that microwave sensors can be subject to constructive and destructive interference.

- Consider that the detection pattern is relative to the mounting position, and it is sometimes possible for an adversary to crawl under the detection beam when microwave sensor antennas, i.e., receivers and transmitters, are relatively high.

- Consider that it is sometimes possible to jump over the zone of detection when microwave sensor antennas, i.e., receivers and transmitters, are mounted low so the detection zone is close to the ground.

- When a boundary system is to be established using microwave sensors and multiple zones or sectors, the detection zones should overlap to achieve a continuous detection pattern with no areas of reduced detection capability at the ends of each sector.

- Be aware that reflections of microwave signals from nearby structures or surface discontinuities may cause nuisance alarms.

- Be aware that microwave sensor detection zones that parallel a road with vehicular traffic or long fence lines will produce nuisance alarms unless sufficient offset is established between the sensor axis and the interference source, e.g., traffic on the roads or swaying fence lines.

- Note that standing water, e.g., from heavy rain, under the microwave sensor detection zone can produce an increased nuisance alarm rate when the water is rippled by winds.

- Note that significant snow depths and drifts can produce voids in the detection zone.

- Consider that the dead spot in detection immediately below and in front of microwave units increases with mounting elevation.

- Consider that heavy rain exceeding 5.1 cm (2.2 inches) per hour is likely to cause microwave sensors to produce nuisance alarms.

- Consider that electro-magnetic interference, either reflected or direct, can strike the microwave receiver and cause nuisance alarms.

- Note that acoustic noises and vibrations, e.g., seismic activities or mechanical disturbances, can adversely affect some microwave sensors and not affect others, depending on their design, signal processing, and installation parameters.

- Remove food and water sources from the vicinity of the sensor system to prevent foraging animals from causing nuisance alarms.

- Limit grass heights to 10 cm (3.9 inches) to prevent nuisance alarms caused by the wind moving the grass.

ELECTRIC FIELD SYSTEMS

- Avoid installation in areas that are subject to drastic environmental changes, such as temperature extremes.

- Ensure that angles of corners are kept as close to 90 degrees as possible.

- Note that electric storms can cause electric field systems to malfunction and can cause false alarms.

- When electric field systems are installed on perimeter fencing, the perimeter fencing must be kept in good condition at all times.

- For electric field sensor zones located parallel to roads, provide sufficient offset from the road to prevent nuisance alarms.

- Note that significant snow drifts and depths can degrade detection capabilities.

- Ensure that wires are retensioned after extreme seasonal temperature changes.

PORTED COAXIAL CABLE SYSTEMS

- Ensure that the ground in which a ported coaxial cable system is buried is firm and is not subject to movement.

- Note that ground water can cause ported coaxial cable systems to generate false alarms.

- Note that rodents can chew through ported coaxial cable.

- Avoid intersecting irrigation pipes and power lines with the coaxial cable.

- Perform soil conductivity tests to ensure that high conductivity, such as is caused by high concentrations of iron or salt in the soil, does not "short out" the radio frequency field.

ACTIVE INFRARED MULTI-BEAM SYSTEMS

- Note that active infrared multibeam systems require a clear line of sight.

- Be aware that active infrared multibeam systems require flat ground to prevent shadowing.

- Be aware that the detection capability of active infrared multibeam systems can degrade in adverse environments such as heavy rain, dense fog, seismic activity, and vibration as from vehicle traffic.

- Install systems so that intruders can not crawl under or jump over the detection zone.

- Install systems so that the ends of adjacent zones overlap.

- Note that wildlife activity can cause nuisance alarms in active infrared multibeam systems.

TAUT WIRE

- Make sure that a constant tension is maintained on the wires through periodic checking and adjustments.

- Be aware that certain environmental conditions, such as icing or frozen ground heaves, can cause nuisance alarms.

- Ensure that, prior to installation, terrain under the system is leveled to a constant grade.

- Ensure that the path along the alignment of the sensor fence is cleared of all vegetation, tree branches, and other debris.

- Consider the installation of curbing under the fence system to prevent tunneling or trenching.

- Ensure that fence posts are securely anchored.

FIBER OPTICS SYSTEMS

- Install according to manufacturer's recommendations, since many new and different technologies are being used in fiber optic detection.

- For buried lines, be advised that nuisance alarms may be caused by tree-root movement in high winds and by nearby vehicular traffic.

- For installation on chain-link fencing, many of the same precautions apply as with vibration- or strain-sensitive systems.

VIBRATION- OR STRAIN-DETECTION SYSTEMS

- Foliage and debris touching or being blown against a fence can create nuisance alarms.

- Fence fabric must be securely fastened down.

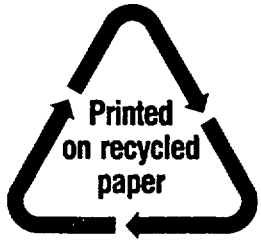
- All gates in the fencing system on which the sensors are mounted should be prevented from vibrating to prevent nuisance alarms.

- Ensure vibrations from nearby vehicles do not cause nuisance alarms.

- Wildlife activity can cause nuisance alarms.

VALUE/IMPACT STATEMENT

A separate value/impact statement has not been prepared for this proposed Revision 3 to Regulatory Guide 5.44. A value/impact statement was prepared for the upgraded physical protection amendments to the regulations that were published in the Federal Register on November 28, 1979. This analysis is also appropriate for this draft regulatory guide. A copy of the value/impact statement is available for inspection or copying for a fee in the Commission's Public Document Room at 2120 L Street NW., Washington, DC; the PDR's mailing address is Mail Stop LL-6, Washington, DC 20555; telephone (202)634-3273; fax (202)634-3343.



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001
