U.S. NUCLEAR REGULATORY COMMISSION

DRAFT REGULATORY GUIDE DG-5065

Proposed Revision 4 to Regulatory Guide 5.44

Issue Date: February 2023
Technical Lead: A. Tardif

PERIMETER INTRUSION ALARM SYSTEMS

A. INTRODUCTION

Purpose

This regulatory guide (RG) describes an approach that is acceptable to the staff of the U.S. Nuclear Regulatory Commission (NRC) to meet regulatory requirements for perimeter intrusion alarm systems used to identify unauthorized or attempted unauthorized access to:

- Category I, II, or III quantities of special nuclear material possessed by NRC licensees at fixed sites. [1]
- Source or byproduct material that NRC licensees receive, possess, use, transfer, and/or deliver.

The guide is being revised to describe the appropriate citations in Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage" (Ref. 1), which has been updated since Revision 3 was issued. Specifically, this revision will clarify the expected actions for an intrusion detection system's operability and performance tests.

Applicability

This RG applies to the following NRC licensees: power reactors; independent spent fuel storage installations; gaseous diffusion plants; certain uranium conversion, enrichment, and fuel fabrication facilities; and those facilities that possess or store a Category I, II, or III quantity of special nuclear material.

This RG does not apply to transportation security requirements for special nuclear material.

This RG applies to non-reactor and reactor applicants and licensees subject to the following regulations:

- 10 CFR Part 20, "Standards for Protection Against Radiation" (Ref. 2);

[1] Category I refers to a formula quantity of strategic special nuclear material, Category II refers to special nuclear material of moderate strategic significance, and Category III refers to special nuclear material of low strategic significance, as defined in 10 CFR 73.2

- 10 CFR Part 40, "Domestic Licensing of Source Material" (Ref. 3);
- 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities" (Ref. 4);
- 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" (Ref. 5);
- 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material" (Ref. 6);
- 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste" (Ref. 7);
- 10 CFR Part 73, "Physical Protection of Plants and Materials."

Applicable Orders and Regulations

- Security Order, EA 02-025, "Order for Compensatory Safeguards Measures," issued March 25, 2002 (Ref. 8).

- 10 CFR Part 20, "Standards for Protection Against Radiation," provides applicable regulations to control the receipt, possession, use, transfer, and disposal of licensed material by any licensee so that the total dose to an individual does not exceed the standards for protection against radiation, specifically

    - 10 CFR 20.1801, "Security of stored material," requires that "[t]he licensee shall secure from unauthorized removal or access licensed materials that are stored in controlled or unrestricted areas."

    - 10 CFR 20.1802, "Control of material not in storage," requires that "[t]he licensee shall control and maintain constant surveillance of licensed material that is in a controlled or unrestricted area and that is not in storage."

- 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," provides regulations for licensing production and utilization facilities, specifically

    - 10 CFR 50.34(c)(1) requires that "[e]ach applicant for an operating license for a production or utilization facility that will be subject to 10 CFR 73.50 and 10 CFR 73.60 of this chapter must include a physical security plan," and 10 CFR 50.34(c)(2) requires that "[e]ach applicant for an operating license for a utilization facility that will be subject to the requirements of 10 CFR 73.55 of this chapter must include a physical security plan."

- 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," governs the issuance of early site permits, standard design certifications, combined licenses, standard design approvals, and manufacturing licenses for nuclear power facilities, specifically

    - 10 CFR 52.79(a)(35)(i) requires the applicant to submit to the NRC a physical security plan that describes how the requirements of 10 CFR Part 73 will be met.

- 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," provides regulations for licensing special nuclear material, specifically

- 10 CFR 70.22(h)(1) requires that licensees controlling a formula quantity of special nuclear material (except those licensed to operate a nuclear power reactor under 10 CFR Part 50) submit a physical security plan for NRC approval.

- 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste," establishes requirements, procedures, and criteria for the issuance of licenses to receive, transfer, and possess power reactor spent fuel, power reactor-related Greater than Class C (GTCC) waste, and other radioactive materials associated with spent fuel storage in an independent spent fuel storage installation (ISFSI), specifically

  - 10 CFR 72.180, "Physical protection plan," requires that "[t]he licensee shall establish, maintain, and follow a detailed plan for physical protection as described in 10 CFR73.51 of this chapter."

- 10 CFR Part 73, "Physical Protection of Plants and Materials," prescribes requirements for the establishment and maintenance of a physical protection system for the protection of special nuclear material at fixed sites and in-transit, specifically

  - 10 CFR 73.20, "General performance objectives and requirements," provides general performance requirements and objectives for the physical protection of plants and materials, specifically 10 CFR 73.20(a), 10 CFR 73.20(b).

  - 10 CFR 73.40, "Physical protection: General requirements at fixed sites," requires that "[e]ach licensee shall provide physical protection at a fixed site, or contiguous sites where licensed activities are conducted, against radiological sabotage, or against theft of special nuclear material, or against both, in accordance with the applicable sections of this Part for each specific class of facility or material license. If applicable, the licensee shall establish and maintain physical security in accordance with security plans approved by the Nuclear Regulatory Commission."

  - 10 CFR 73.45, "Performance capabilities for fixed site physical protection systems," provides performance capability requirements for fixed site physical protection systems, specifically 10 CFR 73.45(c), 10 CFR 73.45(f).

  - 10 CFR 73.46, "Fixed site physical protection systems, subsystems, components, and procedures," provides requirements for fixed site physical protection systems, subsystems, components, and procedures for Category I facilities, specifically 10 CFR 73.46(c), 10 CFR 73.46(e)(1), 10 CFR 73.46(e)(3), 10 CFR 73.46(e)(4), 10 CFR 73.46(e)(5), 10 CFR 73.46(e)(7), 10 CFR 73.46(e)(8), 10 CFR 73.46(g), 10 CFR 73.46(h)(4), 10 CFR 73.46(h)(6).

  - 10 CFR 73.50, "Requirements for physical protection of licensed activities," requires, in part, that "[e]ach licensee who is not subject to 10 CFR 73.51, but who possesses, uses, or stores formula quantities of strategic special nuclear material that are not readily separable from other radioactive material and which have a total external radiation level in excess of 1 gray (100 rad) per hour at a distance of 1 meter (3.3 feet) from any accessible surfaces without intervening shielding other than at nuclear reactor facility licensed under Parts 50 or 52 of this chapter, shall comply with the following," specifically 10 CFR 73.50(b), 10 CFR 73.50(c)(4), 10 CFR 73.50(d), 10 CFR 73.50(f), 10 CFR 73.50(g)(3).

- 10 CFR 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste," requires, in part, the following physical protections for stored spent nuclear fuel and high-level radioactive waste, specifically 10 CFR 73.51(b), 10 CFR 73.51(d), 10 CFR 73.51(d)(11), 10 CFR 73.51(d)(13).

- 10 CFR 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," specifically 10 CFR 73.55(a), 10 CFR 73.55(b), 10 CFR 73.55(c), 10 CFR 73.55(d), 10 CFR 73.55(e)(7), 10 CFR 73.55(e)(8), 10 CFR 73.55(g), 10 CFR 73.55(i), 10 CFR 73.55(i)(4), 10 CFR 73.55(i)(5), 10 CFR 73.55(i)(6), 10 CFR 73.55(n), 10 CFR 73.55(o).

- 10 CFR 73.67, "Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance," provides the following requirements for Category II/III licensees, specifically 10 CFR 73.67(a)(2)(i)-(ii), 73.67(d)(3) and 10 CFR 73.67(f)(2).

Related Guidance

- NUREG-1959, "Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees," issued September 2017 (Ref. 9).

- Regulatory Guide (RG) 1.128, "Installation Design and Installation of Vented Lead-Acid Storage Batteries for Nuclear Power Plants," describes a method acceptable for the installation design and installation of vented lead-acid storage batteries in nuclear power plants (Ref. 10).

- RG 1.129, "Maintenance, Testing, and Replacement of Vented Lead-Acid Storage Batteries for Nuclear Power Plants," describes methods and procedures acceptable regarding the maintenance, testing, and replacement of vented lead-acid storage batteries in nuclear power plants (Ref. 11).

- RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," describes methods and procedures acceptable for demonstrating compliance with the NRC's regulations on design, installation, and testing to address the effects of electromagnetic and radio-frequency interference (EMI/RFI), power surges, and electrostatic discharge on safety-related instrumentation and control (I&C) systems (Ref. 12).

- RG 1.9, "Application and Testing of Safety-Related Diesel Generators in Nuclear Power Plants," provides guidance for onsite emergency alternating current (AC) power sources using emergency diesel generators (EDGs) (Ref. 13).

- RG 5.59, "Standard Format and Content for a Licensee Physical Security Plan for the Protection of Special Nuclear Material of Moderate or Low Strategic Significance," (Ref. 14).

- RG 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements," (not publicly available) (Ref. 15).

- RG 5.70, "Guidance for the Application of the Theft and Diversion Design-Basis Treat in the Design Development, and Implementation of a Physical Security Program that Meets CFR 73.45 and 73.46," (not publicly available) (Ref. 16).

Purpose of Regulatory Guides

The NRC issues RGs to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated events, and to provide guidance to applicants. RGs are not NRC regulations and compliance with them is not required. Methods and solutions that differ from those set forth in RGs will be deemed acceptable if they provide a basis for the regulatory findings required for the issuance or continuance of a permit or license by the Commission.

Paperwork Reduction Act

This RG provides voluntary guidance for implementing the mandatory requirements in 10 CFR Parts 20,40, 50, 52, 70, 72, and 73, that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et. seq.). These information collections were approved by the Office of Management and Budget (OMB), under control numbers 3150-0014, 3150-0020, 3150-0011, 3150-0151, 3150-0009, 3150-0132, and 3150-0002, respectively.

Send comments regarding this information collection to the FOIA, Library and Information Collections Branch (T6-A10M), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by e-mail to Infocollects.Resource@nrc.gov, and to the OMB reviewer at: OMB Office of Information and Regulatory Affairs (3150-0014, 3150-0020, 3150-0011, 3150-0151, 3150-0009, 3150-0132, and 3150-0002), Attn: Desk Officer for the Nuclear Regulatory Commission, 725 17th Street, NW Washington, DC20503; e-mail: oira_submission@omb.eop.gov.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the document requesting or requiring the collection displays a currently valid OMB control number.

Table of Contents

B. DISCUSSION

Reason for Revision

The guide is being revised to provide guidance on updates to Title 10 of the *Code of Federal Regulations* (10 CFR) 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage." This revision gives a comprehensive description of an approach the NRC staff considers acceptable to meet particular requirements for perimeter intrusion alarm systems in 10 CFR 73.20, 10 CFR 73.40, 10 CFR 73.45, 10 CFR 73.46, 10 CFR 73.50, 10 CFR 73.51, 10 CFR 73.55, and 10 CFR 73.67. Specifically, this revision clarifies the expected actions for an intrusion detection system's operability and performance tests.

Background

RG 5.44 provides guidance on regulatory requirements for perimeter intrusion alarm systems, including the operability and performance tests required in 10 CFR 73.55. This guide describes the functions of perimeter intrusion detection sensors and detection methods that are acceptable to the NRC staff for meeting the portions of the NRC's regulations specified above. It provides guidance on (1) sensors and methods that can be integrated to form an effective perimeter intrusion detection system and (2) selecting perimeter intrusion detection systems.

In Sandia National Laboratory literature titled, "The Design and Evaluation of Physical Protection Systems," (Ref. 17) physical protection consists of three elements: detection, delay, and response. Perimeter intrusion alarm systems are one aspect of detection that can be a means for an NRC licensee to meet certain protection objectives to address a threat.

A physical protection program that includes a perimeter intrusion alarm system is a requirement for NRC-licensed nuclear power reactors; Category I, II, III special nuclear material facilities; spent fuel storage facilities; and certain special nuclear material processing facilities. Licensees could use a perimeter intrusion alarm system to meet the intrusion detection requirements for facilities with a Category II or III quantity of special nuclear material in 10 CFR 73.67(d)(3) and 10 CFR 73.67(f)(2), respectively.

The effective use of a perimeter intrusion detection system is influenced by various factors. These factors include:

- the environment (such as terrain, snow, rain, temperature, lightning),
- the selection, application, and installation (including proper electrical grounding) 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,
- the overall integration of the system.

A perimeter intrusion detection alarm system generally consists of:

- security personnel: one or more sensors,
- electronic processing equipment,
- an offsite power supply,
- an onsite power supply that typically consists of an uninterruptible power supply and a fossil-fueled combustion generator,
- signal transmission media,
- an alarm monitor with display,

- an assessment system, and
- a means for maintaining and providing an alarm history.

From an applications viewpoint, sensor systems can be classified as either line of sight or terrain following. From a functional viewpoint, they can be 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. 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,
- 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, and the optimal environments in which to deploy them, are described in NUREG-1959. In addition, several sensor systems and considerations for installation are presented below.

SENSOR SYSTEMS

Microwave Systems

Microwave systems are line of sight and volumetric. 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 increased or 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 the system 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. The two different kinds of monostatic microwave are 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 the grade is uniform 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 four to seven wire systems (i.e., from two sensing and two field wires up to three sensing and four 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 is considered to be terrain following and volumetric. It consists of two buried shielded coaxial cables, transmitters, detectors, a power supply, a processing unit, and an output for connection to an annunciation device. Radio frequency energy is transmitted along the transmission line and is radiated through ports in the shield strands. This radio frequency 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 radio frequency 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 kilograms (kg) (80 pounds). 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.

Institute of Electrical and Electronics Engineers (IEEE) has established standards for installation and maintenance of fiber optic cables, connections, and optical fiber splices. **The NRC staff has reviewed the following available IEEE standards and found they contain additional technical information and criteria regarding fiber optic cables that licensees and applicants may find useful. However, the NRC staff has not endorsed the following IEEE standards in this revision of RG 5.44:**

- IEEE Standard (Std.)1682-2011, "IEEE Standard for Qualifying Fiber Optic Cables, Connections, and Optical Fiber Splices for Use in Safety Systems in Nuclear Power Generating Stations," provides general requirements, directions, and methods for qualifying fiber optic cables, connections, and optical fiber splices for use in safety systems of nuclear power generating stations, including fuel reprocessing stations and other related installations (Ref. 18).

- IEEE Std. 1428-2004, "IEEE Guide for Installation Methods for Fiber Optic Cables in Electric Power Generating Stations and in Industrial Facilities," (Ref. 19), provides guidance

for cables designed for use in power generating stations and industrial facilities, in both the outside plant environment and indoor applications.

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 photodiode. 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.

Alarm Communication and Display Systems

A perimeter intrusion alarm system depends upon an alarm communication and display (AC&D) system in order to function as intended. Therefore, evaluating the AC&D capabilities is an important activity. Several industry standards have been issued that can be utilized to evaluate an AC&D. For example:

- American National Standards Institute (ANSI) (/International Association of Automation (ISA) 18.2, “Management of alarm Systems for the Process Industries,” (Ref. 20).

- National Institute of Standards and Technology (NIST), SP 880-53, “Security and Privacy Controls for Information Systems and Organizations,” (Ref. 21).

Consideration of International Standards

(U) The International Atomic Energy Agency (IAEA) works with member states and other partners to promote the safe, secure, and peaceful use of nuclear technologies. The IAEA has established a series of security guides to address nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities. IAEA security guides

present international good practices and increasingly reflect best practices to help users striving to achieve high levels of security. To inform its development of this RG, the NRC considered IAEA Safety Requirements and Safety Guides pursuant to the Commission's International Policy Statement, "Nuclear Regulatory Commission International Policy Statement," (Ref. 22) and Management Directive and Handbook 6.6, "Regulatory Guides" (Ref. 23).

The following IAEA Nuclear Security Guide was considered in the update of the RG:

- IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," INFCIRC/225," (Ref. 24), contains guidance for incorporating perimeter intrusion detection as a fundamental part of the overall security plan for nuclear material/facilities.

Documents Discussed in Staff Regulatory Guidance

This RG refers to one or more codes or standards developed by external organizations and other third-party guidance documents. These codes, standards, and third-party guidance documents may contain references to other codes, standards, or third-party guidance documents ("secondary references"). If a secondary reference has itself been incorporated by reference into NRC regulations as a requirement, then licensees and applicants must comply with that standard as set forth in the regulation. If the secondary reference has been endorsed in an RG as an acceptable approach for meeting an NRC requirement, then the standard constitutes a method acceptable to the NRC staff for meeting that regulatory requirement as described in the specific RG. If the secondary reference has neither been incorporated by reference into NRC regulations nor endorsed in an RG, then the secondary reference is neither a legally binding requirement nor a "generic" NRC-approved acceptable approach for meeting an NRC requirement. However, licensees and applicants may consider and use the information in the secondary reference, if appropriately justified, consistent with current regulatory practice, and consistent with applicable NRC requirements.

C. STAFF REGULATORY GUIDANCE

1 DESIGN OBJECTIVES AND INTEGRATION

1.1 Layout

1.1.1 In designing an effective perimeter intrusion detection system, dividing the site perimeter into segments that are independently alarmed and uniquely monitored helps the security organization to assess and respond to an alarm by localizing the area in which the alarm is initiated.

1.1.2 The perimeter segment lengths should be selected with consideration of such factors as range; limitations of the sensor system; terrain conditions; and the location, alignment, and viewing areas for video assessment systems (e.g., closed-circuit television (CCTV) cameras), when video technology is used for alarm assessment.

1.1.3 Segmenting the perimeter alarm system also allows testing and maintenance of a portion of the system without affecting the remainder of the perimeter.

1.1.4 In general, the individual segments should be limited to a length that allows observation of the entire segment by an individual standing at one end of the segment.

1.1.5 This typically means that segments should not exceed 100 meters (328 feet), but shorter segments may be needed to achieve the desired performance.

1.1.6 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.

1.1.7 Depending on the system type, this may help to minimize nuisance alarms caused by the movement of high grasses, etc.

1.1.8 Measures for accomplishing stabilization include surfacing or soil sterilization.

1.1.9 Isolation zones on either side of the detection zone also help to provide a clear zone for assessment.

1.1.10 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.

1.1.11 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.

1.1.11.1 The system should be located so that items such as existing (or planned) barriers, sensor mounts,[2] 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.

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

1.1.11.2 In determining the distance between the zone of detection and any area in which an adversary may be concealed, the licensee should consider the time needed to circumvent the barriers, the time to reach a concealed location, and the specific intruder-assessment capabilities at that location. 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.

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

1.1.11.4 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).

1.1.12 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.

1.2 Detection and Alarm Capabilities

1.2.1. 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.

1.2.2. In general, volumetric systems are preferred because they are generally more difficult to defeat.

1.2.3. However, for certain limited site configurations, planar systems may provide coverage with fewer false or nuisance alarms compared to a volumetric-type sensor.

1.2.4. A single system that by itself does not meet detection performance requirements may, in conjunction with another system with a different sensing method, provide adequate detection performance.

1.2.4.1. Such combination systems (i.e., complementary sensor systems) should employ dissimilar detection techniques.

1.2.4.2. 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.

1.2.5. 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.

1.2.6. A further 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.

1.2.7. 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.

1.2.7.1. After that period, the data should be examined to establish site-specific rates for both nuisance and false alarms.

1.2.7.2. 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.

1.2.7.3. Such revisions to security plans may be submitted for nuclear power plants under the provisions of 10 CFR 50.54(p)(2), and for certain special nuclear material processing sites under the provisions of 10 CFR 70.32(e), if the changes do not represent a decrease in the physical protection system effectiveness of the security plan.

1.2.8. Settings of adjustable parameters should be recorded, and future changes should be recorded with justifications.

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

1.2.9.1. Testing of bridging attempts should include the physical use of a ladder and the electronic bridging techniques described in Regulatory Position 1.5.3.

1.2.9.2. For each perimeter intrusion detection system described in Regulatory Position 2; bridging tests should also include those as described for each system.

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

1.2.10.1 placement of any portion of a perimeter intrusion detection system in the access mode.[3]

1.2.10.2 a unique indication, other than a normal alarm, of a switch over to emergency or secondary sources of power.

1.2.10.3 any interruption or reduction of system power to the degree that any part of the system is not functioning properly.

1.2.10.4 any indication of tampering (e.g., opening, shorting, or grounding of the sensor circuitry) that renders the device incapable of normal operations.

1.2.10.5 any indication of tampering by activation of a tamper switch or other triggering mechanism.

3 "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.

1.3 System Electrical Specifications

1.3.1 For interruptions to primary power, the security system should contain provisions for automatic switchover to emergency power (battery or electrical generator) without causing false alarms and without causing a loss of system function or data.

- RG 1.9 provides NRC guidance for onsite emergency AC power sources using EDGs.

- RG 1.128 provides NRC guidance for the installation design and installation of vented lead-acid storage batteries in nuclear power plants.

- RG 1.129 provides NRC guidance regarding the maintenance, testing, and replacement of vented lead-acid storage batteries in nuclear power plants.

In addition, the IEEE has standards for installation and maintenance of onsite power sources, including direct current systems and generators. **The NRC staff has reviewed the following available IEEE standards and found they contain additional technical information and criteria for onsite power sources that licensees and applicants may find useful. However, the NRC staff has not endorsed the following IEEE standards in this revision of RG 5.44:**

- IEEE Std. 946-2020, "IEEE Recommended Practice for the Design of DC Power Systems for Stationary Applications," provides guidance on lead-acid and nickel-cadmium storage batteries, static battery chargers, and distribution equipment (Ref. 25).

- IEEE Std. 1106-2015, "IEEE Recommended Practice for Installation, Maintenance, Testing, and Replacement of Vented Nickel-Cadmium Batteries for Stationary Applications" provides guidance for installation design and for installation, maintenance, and testing procedures that can be used to optimize the life and performance of vented nickel-cadmium batteries, including partially recombinant types, used in stationary applications (Ref. 26).

- IEEE Std. 1187-2013, "IEEE Recommended Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Batteries for Stationary Applications," provides guidance for the installation and installation design of valve-regulated lead acid (VRLA) batteries (Ref. 27).

- IEEE Std. 1188-2005, "IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications," provides guidance limited to maintenance, test schedules and testing procedures that can be used to optimize the life and performance of VRLA batteries for stationary applications (Ref. 28).

- IEEE Std. 2420-2019, "IEEE Standard Criteria for Combustion Turbine-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations," provides guidance for the application and testing of combustion turbine-generator units as Class 1E standby power supplies in nuclear power generating stations (Ref. 29).

1.3.2 Emergency power should be capable of sustaining operation without external support for a minimum of 4 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. Other NRC-licensed facilities that implement emergency power may follow the 4-hour criteria stated immediately above.

1.3.3 If emergency power is furnished by battery, all batteries (including stored batteries) should be maintained at full charge by automatic battery charging circuitry.

- IEEE Std. 946-2020, "IEEE Recommended Practice for the Design of DC Power Systems for Stationary Applications" provides guidance on lead-acid and nickel-cadmium storage batteries, static battery chargers, and distribution equipment. **The NRC staff has reviewed the IEEE Std. 946-2020 and found it contains additional information and criteria for emergency power furnished by batteries that licensees and applicants may find useful. However, the NRC staff has not endorsed IEEE Std. 946-2020 in this revision of RG 5.44.**

- National Electrical Manufacturers Association (NEMA) PE5, "Utility Battery Chargers," (Ref. 30) provides guidance on battery chargers. **The NRC staff has reviewed NEMA PE5 and found it contains additional information and criteria for emergency power furnished by batteries that licensees and applicants may find useful. However, the NRC staff has not endorsed NEMA PE5 in this revision of RG 5.44.**

1.4 Tamper Protection

1.4.1 All enclosures containing controls that affect the operation and sensitivity of the detection system and all access point controls should be located within an enclosure protected by a tamper switch.

1.4.2 The electronics should be designed so that tamper switches remain in operation even though the system may be placed in the access mode.

1.4.3 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.

1.5 System Line Supervision

1.5.1 All signal lines connecting detection devices to alarm stations should be supervised. Facilities that possess Category I quantities of special nuclear material should provide line security using either of the following two methods:

1.5.1.1 Provide central station line security in accordance with Underwriter Laboratories (UL) Standard 1076, "Standard for Proprietary Burglar Alarm Units and Systems" (Ref. 31); UL Standard 1610, "Standard for Central-Station Burglar-Alarm Units" (Ref. 32); and UL Standard 1635, "Standard for Digital Alarm Communicator System Units" (Ref. 33), as appropriate.

1.5.1.2 Provide encrypted line security by a means employing a data encryption standard. The encryption must be at least 128-bit that meets NIST, Federal

Information Processing Standards (FIPS) 197, "Advanced Encryption Standard (AES)" (Ref. 34), or equivalent.

1.5.2 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.

1.5.3 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:

1.5.3.1 substitution of resistance, voltage, or current.

1.5.3.2 Substitution of equipment of the same design and manufacturer.

1.5.3.3 reintroduction by playback of signals previously recorded onto the communication path.

1.5.3.4 introduction of signals onto the path that were synthesized externally.

1.5.4 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

1.6.1 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.

1.6.2 For this reason, it is important that all equipment be installed in accordance with the manufacturers' specifications, meet the performance criteria required by 10 CFR Part 73 as clarified in this RG, and be thoroughly tested in accordance with the manufacturers' recommendations and any applicable design basis threat capabilities.

1.6.3 In some instances, the combination of different sensor types (i.e., complementary sensor systems) can yield improved performance with a reduction in vulnerabilities. (See Regulatory Position 1.2, "Detection and Alarm Capabilities," on combining sensors.)

1.6.4 Licensees should consider requesting that a system manufacturer, a qualified engineer, or both 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

1.7.1 A perimeter intrusion detection system is incomplete without some means to assess and resolve alarms.

1.7.2 It is imperative that the assessment techniques identify the stimulus in a timely manner before the stimulus of the alarm disappears from view.

1.7.3 The detection of an intruder in the isolation zone should allow enough time for an adequate security response (i.e., the scenario results in a satisfactory probability of physical protection system effectiveness) (Ref. 35).

1.7.4 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-image capture monitoring techniques).

1.7.5 Care should be taken that the means used to provide additional delay do not interfere with assessment capabilities.

1.7.6 The following are acceptable methods of assessment:

1.7.6.1 Video assessment equipment, such as CCTV systems that are fixed and properly aimed parallel to the barrier or perpendicular to the intruder's path may be used to provide assessment information to the alarm station operators.

1.7.6.1.1 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.

1.7.6.1.2 These systems should be designed to display immediately, using the same signal that activates the detection alarm annunciation.

1.7.6.1.3 Video-image capture devices with the capability to record an adversary within the zone of assessment and immediately prior to, during and after detection are an acceptable alternative to alarm-activated display monitors. Video-image capture assembles the before, during and after video frames of a sensor detection event. Captured video frames are then viewed by alarm station security personnel by utilizing playback on a digital video recorder (DVR) or network video recorder (NVR) to determine the potential cause of the event. Details of video playback are described in NUREG-1959.

1.7.6.1.4 At Category I fuel cycle facilities, alarm-activated display monitors should continuously display and not "go blank" during quiet periods (periods of no alarm). Consideration should be given to the use of pan/tilt/zoom cameras to augment fixed camera installations, as an adjunct to the fixed camera systems. An acceptable means for installation of video systems can be found in NUREG-1959.

1.7.6.2 Fixed guard posts can be effective if the posts are positioned so that there is a clear field of view of the assigned segment.

1.7.6.2.1 These posts generally should be positioned at the end of the assessment area with the guard observing in one direction only.

1.7.6.2.2 The intrusion detection system should annunciate in the local guard post as well as in both alarm stations.

1.7.6.2.3 Consideration should be given to compensation for loss of guard observation (i.e., detection and assessment) capability during periods of reduced visibility such as darkness, rain, fog, and snow, as well as for durations of greater than 20 minutes.

1.8 Maintenance

1.8.1 The regulations in 10 CFR Part 73 require that the perimeter intrusion detection system be maintained in an operable condition; therefore, a preventive maintenance program is necessary.

1.8.2 Maintenance of the detection, alarm communication, annunciation, and assessment system are critical to successful operation.

1.8.3 Licensees should establish an ongoing program for maintenance.

1.8.4 In addition, maintenance may be initiated by the testing program, operational requirements, the routine periodic maintenance program, or a trending program or analysis.

1.8.5 The amount of time that equipment is out of service should be minimized to preclude the overuse of compensatory measures.

1.8.6 The maintenance group should be effective and respond in a timely manner.

1.8.7 The use of dedicated onsite maintenance technicians has proven effective to ensure the operability and proper performance of the perimeter intrusion detection system.

2 PERIMETER INTRUSION DETECTION SYSTEMS—MINIMUM SPECIFICATIONS

2.1 Microwave Systems

2.1.1 Installation Criteria

2.1.1.1 Bistatic transmitters and receivers should be installed on even terrain clear of trees, tall grass, standing or running water, and bushes.

2.1.1.2 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.

2.1.1.3 Some models are designed to operate over short ranges (e.g., across perimeter portals).

2.1.1.4 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.

2.1.1.5 The required amount of overlap of successive links is contingent on the antenna pattern and unit height.

2.1.1.6 In zone overlap areas, the equipment for the overlapped zones should either both be transmitters, or both be receivers; this is to minimize interference between the successive links that could otherwise result in decreased sensitivity and greater false alarm rates within the zones.

2.1.1.7 Each unit should be mounted rigidly on secure posts at a sufficient distance above the ground so that incident and reflected signals combine positively, typically 60 centimeters (24 inches) for 100 meters (328 feet), or according to the manufacturer's installation criteria.

2.1.1.8 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.

2.1.1.9 Accordingly, the mounting mechanisms for a system should permit adjustment of antenna height and position to correct poor performance or alignment.

2.1.1.10 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.

2.1.1.11 Receiver capture occurs when a receiver recognizes a false transmission signal as its own.

2.1.1.12 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 to access a receiver head.

2.1.1.13 As with bistatic receiver heads, monostatic transceiver heads may be vulnerable to certain tampering methods and should also be protected, possibly by placement inside another sensor's detection zone.

2.1.1.14 Both bistatic and monostatic receiver heads could be deployed in a protected manner by situating them within a fenced perimeter, where for example, a ported coaxial and/or taut wire detection system(s), coupled with assessment capabilities, were deployed between the outer fence and the receiver heads.

2.1.1.15 Stacking of microwave sensors is one means of increasing the elevation-detection-zone height of the system to enhance its detection capabilities.

2.1.1.15.1 The stacking technique, in effect, fills in the dead zones that can be inherent in simple bistatic systems.

2.1.1.15.2 Additionally, the use of stacked units can help detect the bridging or jumping of a detection zone.

2.1.1.16 Multichannel microwave units should be used in an alternating pattern around the perimeter.

2.1.1.17 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.

2.1.1.18 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.

2.1.1.18.1 The distance between the bottom of the detection zone and the ground plane should be such that a person cannot crawl under the zone undetected.

2.1.1.18.2 Typically, the distance between the bottom of the detection zone and the ground should be 15.24 centimeters (6 inches) or less.

2.1.1.18.3 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.

2.1.1.18.4 Approximate dimensions of the microwave pattern should be provided by the manufacturer.

2.1.1.19 Motion or disturbance of objects such as tumbleweed, paper, and bushes moving in the path of the beam can cause nuisance alarms.

2.1.1.20 Since the beam is relatively wide, care should be taken to ensure that reflections from authorized activities do not create nuisance alarms.

2.1.1.21 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.

2.1.1.22 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).

2.1.1.23 In addition, the microwave link should be positioned within the isolation zone to enhance assessment once detection is made.

2.1.1.24 Neither a transmitter nor a receiver should be mounted on a fence unless prior approval is received from the NRC.

2.1.1.25 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.

2.1.1.26 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*

2.1.2.1 A microwave perimeter detection system should be capable of detecting an intruder weighing a minimum of 35 kilograms (77 pounds) passing through the zone of detection 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.

2.1.2.2 Provision should be made to ensure detection in spite of the dead spots in front of transmitters and receivers.

2.1.2.3 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

2.2.1.1 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.

2.2.1.2 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 wires.

2.2.1.3 The 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.

2.2.1.3.1 The electric field sensor's wires should be spaced so that an individual moving between the wires can be detected.

2.2.1.3.2 It is important that the lowest wire of any electric field system be consistently close enough to the ground to detect crawling under the wire.

2.2.1.3.3 Accordingly, the bottom wire should be located 15.24 centimeters (6 inches) or less above ground level.

2.2.1.3.4 The field wires and sensing wires should be located and spaced in accordance with the manufacturer's specifications.

2.2.1.3.5 The electric field detector is not a line-of-sight system and therefore can be installed on uneven terrain and in an irregular line.

2.2.1.3.6 However, the terrain between posts must be of uniform grade so that the field and sensing wires can be installed parallel to the ground.

2.2.1.4 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.

2.2.1.5 Consideration may also need to be given to the ability of intruders to set up, without observation, such hand-carried equipment as small ladders for jumping over the electric field without detection.

2.2.1.6 In general, evasion of detection by jumping over a planar system need not be considered if the overall height of the system is about 3.7 meters (12 feet) or greater, because of the impact of jumping from those heights.

2.2.1.7 For electric field systems, wires that are not connected to either field generators or field change sensors may prove useful for altering the field contours to fill in gaps or to extend the effective height of the field.

2.2.1.8 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 passage between the barrier and the system.

2.2.1.9 The surrounding terrain within 3 meters (10 feet) of field wires should be free of all shrubs, trees, and undergrowth.

2.2.1.10 The system should be well grounded in accordance with the manufacturer's recommendations along its entire length, with special care given to the sections that go over walls or buildings.

- IEEE Std. 142-1991, "IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems," (Ref. 36) provides additional information on grounding. **The NRC staff has reviewed the IEEE Std. 142-1991 standard and found it contains additional technical information and criteria for grounding that licensees and applicants may find useful. However, the NRC staff does not endorse IEEE Std. 142-1991 in this revision of RG 5.44.**

2.2.1.10.1 The control unit should be well grounded using a 1-meter (39-inch) or longer grounding rod or equivalent electrical ground.

2.2.1.10.2 Grounding may be difficult under dry earth conditions.

2.2.1.10.3 The resistance between ground rods and earth should also meet manufacturer's recommendations.

2.2.1.11 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.

2.2.1.11.1 Monostatic microwave could also be used to protect these areas.

2.2.1.11.2 Another alternative is to install barriers in these areas to either channel an intruder into the higher sensitivity envelope or require

increased activity to penetrate the barrier sufficient to be detected even in the reduced sensitivity region.

2.2.1.11.3 Each wire should be kept free of nicks, cuts, etc. and be properly tensioned in accordance with the manufacturer's recommendations along its entire length.

2.2.1.12 Systems mounted on chain link fence are susceptible to wind-caused alarms and should be avoided.

2.2.1.13 There may be some loss of sensitivity in the vicinity of metal posts used to support electric field fences.

2.2.1.14 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

2.2.2.1 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.

2.2.2.2 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

2.3.1.1 Ported coaxial cable systems should be installed in accordance with the manufacturer's specifications.

2.3.1.2 The maximum and minimum separation of the transmitter and receiver can vary.

2.3.1.3 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.

2.3.1.4 The system is terrain following and can be curved around corners.

2.3.1.5 The lines are generally buried approximately 18 centimeters (7 inches) deep and 1 to 3 meters (3 to 10 feet) apart.

2.3.1.6 The installation of ported coaxial cable perpendicular to buried metal conduit for electrical cables or metal pipes used for water or storm drains may degrade detection or cause nuisance alarms.

2.3.1.7 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.

2.3.1.8 Highly conductive soil includes soil that contains concentrations of iron or salt.

2.3.1.9 Moving objects in the zone of detection such as foliage, rippling water, and grasses may create nuisance alarms.

2.3.1.10 Rodents can chew through ported coaxial cable.

2.3.1.11 Sensor locations should be selected carefully to prevent nuisance alarms from such sources as personnel and vehicular traffic.

2.3.1.12 Similarly, the cleared area above the sensor should be controlled to prevent the placement of objects within the area, even temporarily, which would degrade the detection zone.

2.3.1.13 The transmitter and receiver transducer lines should be installed on well-drained terrain cleared of trees, tall grass, and bushes.

2.3.1.14 System sensitivity may be affected by freezing or thawing of the surrounding terrain.

2.3.1.15 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.

2.3.1.16 Neither the transmitter nor the receiver lines should be mounted above ground.

2.3.1.17 Approximate dimensions of the detection pattern should be provided by the manufacturer.

2.3.1.18 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.

2.3.1.18.1 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).

2.3.1.19 Manufacturer's instructions should be followed when installing cable across concrete or asphalt areas.

2.3.1.19.1 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

2.3.2.1 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.

2.3.2.2 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

2.4.1.1 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.

2.4.1.1.1 The maximum distance between transmitter and receiver is generally 80 meters (260 feet).

2.4.1.1.2 The infrared perimeter system should be installed so that, at any point, the lowest beam is 15.24 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.

2.4.1.2 Consideration should be given to the ability of intruders to set up, without observation, such hand-carried equipment as small ladders for jumping over the infrared beams without detection.

2.4.1.2.1 In general, evasion of detection by jumping over a planar system need not be considered if the overall height of the system is about 3.7 meters (12 feet) or greater, because of the impact of jumping from those heights.

2.4.1.2.2 The beams should be sufficiently interlaced that an individual could not penetrate between the beams and remain undetected.

2.4.1.2.3 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.

2.4.1.2.4 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.

2.4.1.2.5 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.

2.4.1.2.6 As an alternative, successive infrared links should overlap at angles, with sufficient overlap to preclude the use of the mounting

posts for jumping over the plane of detection; this installation precludes the use of common posts.

2.4.1.3 Fog, rain, and snow can attenuate and disperse the infrared beam and can cause nuisance alarms.

2.4.1.3.1 However, the system can be designed to compensate for severe atmospheric attenuation.

2.4.1.3.2 Dust on the face plates will also attenuate the infrared beam, as will an accumulation of condensation, frost, or ice.

2.4.1.4 Condensation, frost, or ice may be eliminated by using heated face plates.

2.4.1.4.1 Sunshine on the receiver may cause nuisance alarms.

2.4.1.4.2 A misalignment of transmitter and receiver caused by frost heaves may also cause nuisance alarms.

2.4.1.4.3 Like the microwave system, vegetation such as bushes, trees, or grass and accumulated snow will interfere with the infrared beam.

2.4.1.4.4 The passage of an intruder may go undetected on irregular ground surfaces, ditches, or hills.

2.4.1.5 The transmitter and receiver units should be positioned a minimum of 3 meters (10 feet) from perimeter fencing.

2.4.1.6 The infrared detection system should not be installed directly adjacent to a barrier, because 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

2.4.2.1 An infrared perimeter detection system should be a multibeam modulated type, consisting of a minimum of six beams per segment.

2.4.2.2 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.

2.4.2.3 This means that the infrared beams should be placed and interlaced to form an infrared “wall.”

2.4.2.4 Furthermore, the systems should be able to operate as above with a factor of 20 (13 decibels) 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

2.5.1.1 Manufacturer's specifications should be followed in the installation of the system.

2.5.1.2 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.

2.5.1.3 The overall height of the system should be 3.7 meters (12 feet) or greater.

2.5.1.4 Wires should be spaced so no intruder can pass between the wires without detection, normally a distance of 15.24 centimeters (6 inches) or less between wires.

2.5.1.5 A sensing post should be placed approximately halfway between anchor posts. (Anchor posts may function as sensor posts in certain models.)

2.5.1.6 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.

2.5.1.7 The system may be installed on chain-link fencing or an existing wall with a stand-off equal to or less than 15.24 centimeters (6 inches).

2.5.1.8 When installed on chain-link fencing, the taut wire system should be installed on the interior or protected area side of the fence.

2.5.1.9 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 15.24 centimeters (6 inches) or less above the ground.

2.5.2 Performance Criteria

2.5.2.1 The system should be installed so that an alarm is received on deflection of any wire that causes a vertical opening greater than 15.24 centimeters (6 inches).

2.6 Fiber Optic Systems

2.6.1 Installation Criteria

2.6.1.1 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.

2.6.1.2 Manufacturer's guidelines for installation should be followed.

2.6.1.3 Segments should be limited in length to 100 meters (328 feet).

2.6.1.4 Since such systems detect pressure, motion, or vibration, they are sensitive to many of same the vulnerabilities as vibration- or strain-sensitive systems or buried line technologies.

2.6.2 Performance Criteria

2.6.2.1 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

2.7.1 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.

2.7.2 Installation Criteria

2.7.2.1 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.

2.7.2.2 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.

2.7.2.3 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.

2.7.2.4 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.

2.7.2.5 Increasing the fence height also appears to enhance sensor performance. Consideration should be given to the ability of intruders to set up, without observation, such hand-carried equipment as small ladders for jumping over the infrared beams without detection.

2.7.2.6 In general, evasion of detection by jumping over a planar system need not be considered if the overall height of the system is about 3.7 meters (12 feet) or greater, because of the impact of jumping from those heights.

2.7.2.7 However, most fence-based detection systems can be bypassed easily by a variety of methods.

2.8 Performance Criteria

2.8.1 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.

2.8.2 The system should also detect any attempt to cut the fence or lift the fence fabric 15.24 centimeters (6 inches) or more above grade.

2.8.3 The system should not generate excessive nuisance alarms.

2.8.4 In addition to the testing described in Regulatory Position 3 of this guide, the vibration- or strain-detection systems should be tested for their ability to detect fence-cutting attacks or other means of defeating detection unique to these systems.

2.9 Other Intrusion Detection Systems

2.9.1 Some systems currently under development may be acceptable, when fully developed, for use at NRC-licensed facilities.

2.9.2 Other systems that currently do not have an acceptable detection performance capability may at some future time be refined and be found suitable.

2.9.3 In either case, these systems would have to be performance tested by the licensee and a qualified independent agent (such as a national laboratory) before consideration by the NRC.

3 RECOMMENDED TESTING PROCEDURES

3.1 General Testing Procedures Guidelines

3.1.1 In conducting any testing procedures, care should be taken to ensure the safety of the individuals performing the testing.

3.1.2 The standard Occupational Safety and Health Administration procedures and practices should be followed.

3.1.3 The "National Electric Safety Code" (NESC) (Ref. 37) provides additional information concerning practical safeguarding of persons against arc flash during the installation, operation, or maintenance of the following:

- electric supply stations,
- overhead supply and communications lines,
- underground or buried supply and communication cables.

The NRC staff has reviewed the NESC and found it contains additional information about safeguarding personnel against arc flash that licensees and applicants may find useful. However, the NRC staff does not endorse the NESC in this revision of RG 5.44.

3.1.4 Specification testing should take place at the initial installation of the equipment.

3.1.5 If available, test procedures recommended by the manufacturer should be followed.

3.1.6 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.

3.1.7 For each perimeter segment, the test should include the following:

3.1.7.1 ensure that the system meets the manufacturer's specifications and NRC-recommended detection probability,

3.1.7.2 verify that no dead spots exist in the zone of protection, and

3.1.7.3 verify that line supervision and tamper protection in both the access and secure modes are functional.

3.1.7.4 Verify that the zone being tested does not have any active alarms and is in normal status.

3.1.8 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.

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

3.2 Testing Option I

3.2.1 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 every 7 days in the following manner.

3.2.2 Testing may be conducted during routine patrols by members of the licensee's security force.

3.2.3 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.

3.2.4 Before the test, the individual making the test should notify the alarm stations that a test is about to be conducted.

3.2.5 The detection system in all segments should be walk-tested in a different, preferably random order every 7 days, and the testing should be conducted throughout the week rather than conducting all tests on the same day.

3.2.6 The testing should result in 100 percent detection on all segments every 7 days.

3.2.7 If the perimeter alarm system fails to detect an intrusion on one or more segments, corrective actions should be taken and documented.

3.2.8 Records should be maintained to document that all required testing has been accomplished.

3.2.9 In addition to operational testing, the system should be performance tested at least semi-annually, as well as after each inoperative state and after any repairs.

3.2.10 A 90 percent probability of detection with 95 percent confidence should be the design goal of the system.

3.2.11 An acceptable model performance testing program includes the following:

3.2.11.1 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).

3.2.11.2 This determination will, in most cases, be sensor and location dependent.

3.2.11.3 Note that vulnerability to penetration also varies with environmental conditions.

3.2.11.4 Inclement weather may be a particularly good time for a realistic evaluation of perimeter vulnerabilities.

3.2.11.5 Test each segment using a combination of all the applicable penetration approaches at the most vulnerable area a total of 30 times. All 30 tests should result in successful detections.

3.2.11.6 If the minimum number of successful detections is not achieved, the system should be checked.

3.2.11.6.1 If no problems with the system are discovered, 10 more tests should be made.

3.2.11.6.2 If the minimum number of successful detections is achieved, in this case 39 out of 40 (see the following table), the testing for this segment can be ended.

3.2.11.6.3 If no problems with the system can be discovered and less than 9 out of 10 additional intrusions are detected, the system should be upgraded to increase the detection probability to meet the design goal of the system.

3.2.11.6.4 If problems with the system are discovered, the system should be repaired, and 30 new tests performed.

3.2.11.6.5 If there are 30 successful detections, testing can be ended.

Total No. of Tests	Minimum No. of Successful Detections	Maximum No. of Failures Detected
30	30	0
40	39	1
50	48	2

3.2.11.7 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.

3.2.11.8 The segments should be tested in random order.

3.2.11.8.1 This will protect against the possibility that environmental effects and other unknown factors that may affect the test results (detection or non-detection) always favor or handicap the same segment or method of approach.

3.2.11.8.2 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.

3.2.11.8.3 However, the difference noted between the two segments might only be due to the difference between morning and afternoon.

3.2.11.8.4 Similarly, using random methods, no approach will be continually favored if the time sequence (ordering) affects the test results.

3.2.11.8.5 This will protect against disturbances that may or may not occur and that may or may not be serious if they do occur.

3.2.11.8.6 A random numbers table can be used to determine the order in which the segments will be tested.

3.2.11.9 Maintain records of the results of all tests performed.

3.2.11.9.1 These records should include the segment number, date, time, and relevant environmental conditions when tests were performed.

3.2.11.9.2 Records should be maintained consistent with 10 CFR 73.70, "Records.

3.3 Testing Option II

3.3.1 Under this option, one pass (i.e., one attempt to circumvent the zone of detection) of a performance test is conducted in place of an operational test, and the burden for semiannual performance testing is greatly reduced.

3.3.2 With proper system performance, semiannual 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 at least every 7 days as with operational testing, this performance type of test that is conducted at least every 7 days represents a challenge to the system.

3.3.3 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).

3.3.4 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.

3.3.5 Over time, each segment should be tested by using a combination of all the applicable penetration approaches at the most vulnerable area.

3.3.6 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.

3.3.7 The segments should be tested in random order.

3.3.7.1 This will protect against the possibility that environmental effects and other unknown factors that may affect the test results (detection or non-detection) always favor or handicap the same segment or method of approach.

3.3.7.2 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.

3.3.7.3 However, the difference noted between the two segments might only be due to the difference between morning and afternoon.

3.3.7.4 Similarly, using random methods, no approach will be continually favored if the time sequence (ordering) affects the test results.

3.3.7.5 This will protect against disturbances that may or may not occur and that may or may not be serious if they do occur.

3.3.7.6 A random numbers table can be used to determine the order in which the segments will be tested.

3.3.8 Because this option for testing is conducted weekly, 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.

3.3.9 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 a year with reduced overall burden on the licensee.

3.3.10 Under Test Option II, if a sensor achieves 50 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.)

3.3.11 Testing must never conclude on a non-detection. If three or more non-detections occur, accumulated data for the period may not be counted toward totals for performance testing, and the accumulation of data must be restarted.

3.3.12 As described in the model performance testing program in Regulatory Positions 3.2.8. and 3.2.11.9, records of all tests performed should be maintained for at least 3-years, consistent with 10 CFR 73.70.

4 GUIDANCE FOR PERIMETER INTRUSION ALARM SYSTEMS FOR PREVENTING UNAUTHORIZED REMOVAL OR ACCESS OF LICENSED CATEGORY I, II, AND III SPECIAL NUCLEAR MATERIAL REQUIRED BY 10 CFR 20.1801 and 20.1802

10 CFR 20.1801 requires that "[t]he licensee shall secure from unauthorized removal or access licensed materials that are stored in controlled or unrestricted areas."

10 CFR 20.1802 states: "The licensee shall control and maintain constant surveillance of licensed material that is in a controlled or unrestricted area and that is not in storage."

4.1 For Category I special nuclear material, licensees should follow the guidance on the provisions of perimeter intrusion detection systems to control and maintain constant surveillance of licensed material that is in a controlled area described in Regulatory Position 5 of this guide. A controlled area for Category I special nuclear material is within a material access area that is inside a protected area.

4.2 For Category II or III special nuclear material, licensees should follow the guidance described in Regulatory Position 9 of this guide.

4.3 Requirements for securing a Category I, II, or III quantity of special nuclear material in an unrestricted area pertains to transportation of the material; the NRC staff expectations for meeting those requirements are not described in this guide.

5 GUIDANCE FOR CATEGORY I LICENSEE PERIMETER INTRUSION ALARM SYSTEMS REQUIRED BY 10 CFR 73.46 AND 10 CFR 73.20

5.1 Protected area perimeter intrusion alarm system

10 CFR 73.46(c) requires that the perimeter of the protected area "must be provided with two separated physical barriers with an intrusion detection system placed between the two."

5.1.1 Protected area perimeter intrusion alarm systems should use sensor devices that provide detection. Applicable terrain exterior sensor detection devices include, but are not limited to, microwave sensors, electric field sensors, ported coaxial cable systems, active infrared sensors, taut wire sensors, and fence disturbance sensors. Each of these sensors are described in NUREG-1959.

5.1.2 A perimeter intrusion alarm system should also contain five elements: (1) electronic processing equipment (that includes a means for maintaining and providing an alarm history), (2) a power supply, (3) signal transmission media, (4) an alarm monitor with display, and (5) an assessment system. These elements are also described in NUREG-1959.

5.2 Material access area perimeter alarm systems

10 CFR 73.46(e)(3) requires, in part, material access areas to have intrusion detection as follows: "All unoccupied vital areas and material access areas shall be locked and protected by

an intrusion alarm subsystem which will alarm upon the entry of a person anywhere into the area, upon exit from the area, and upon movement of an individual within the area, except that for process material access areas only the location of the strategic special nuclear material within the area is required to be so alarmed."

5.2.1 For intrusion detection equipment at a material access area perimeter, a balanced magnetic switch should be used on each door or movable barrier to allow detection of attempted or actual unauthorized access. Balanced magnetic switches should do the following:

5.2.1.1 Meet the requirements of UL Standard 634, "Standard for Connectors and Switches for Use with Burglar-Alarm Systems" (Ref. 38), for a level 2 high-security switch, balanced magnetic switch.

5.2.1.2 Initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normal secured position.

5.2.1.3 Initiate an alarm when the door moves more than 2.5 centimeters (1 inch) from the fully closed position.

5.2.1.4 For process material access areas, the location of the special nuclear material should be sensed for detection by microwave and/or passive infrared volumetric sensors.

5.2.1.5 For process material access areas, the location of the special nuclear material containers themselves can be set upon sensing platforms that react to specific changes in weight and/or thermal energy, as appropriate.

5.2.1.6 For process material access areas, where special nuclear material is located, if outfitted with both volumetric sensors as described in Regulatory Position 5.2.1.4 and platform sensors as described in Regulatory Position 5.2.1.5, then a layered complimentary sensor scheme would be provided and it could result in a higher probability of detection, than if volumetric or platform sensors were implemented by themselves.

5.3 Alarm assessment system

10 CFR 73.46(h)(6) requires an alarm assessment to ascertain the cause of an alarm as follows: "To facilitate initial response to detection of penetration of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area shall be provided, preferably by means of closed-circuit television or by other suitable means which limit exposure of responding personnel to possible attack."

10 CFR 73.46(h)(4) requires an assessment, "[u]pon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, a material access area, or a vital area, or upon evidence or indication of intrusion into a protected area, a material access area, or a vital area, the licensee security organization shall: (i) Determine whether or not a threat exists, (ii) Assess the extent of the threat, if any."

5.3.1 A sensor detection generates an alarm. An assessment by the licensee security organization should be performed to ascertain the cause of the detection and corresponding alarm. There are three types of alarm:

1. false alarm,
2. nuisance alarm, and
3. actual alarm.

False and nuisance alarms are described in NUREG-1959.

5.3.2 The action of assessment may be conducted by security personnel through visual observation by line of sight or through the use of video assessment equipment (e.g., CCTV that has a video-image capture capability). Video-image capture assembles the before and after video frames of a sensor detection event. Captured video frames are then viewed by alarm station security personnel by utilizing playback on a digital video recorder (DVR) or network video recorder (NVR) to determine the potential cause of the event. Details of video playback are described in NUREG-1959.

5.4 Isolation zone

10 CFR 73.46(c)(3) requires an isolation zone with the following characteristics: "Isolation zones shall be maintained in outdoor areas adjacent to the physical barrier at the perimeter of the protected area and shall be large enough to permit observation of the activities of people on either side of that barrier in the event of its penetration. If parking facilities are provided for employees or visitors, they shall be located outside the isolation zone and exterior to the protected area."

10 CFR 73.46(e)(1) requires the isolation zone to have specific detection capabilities: "The licensee shall provide an intrusion alarm subsystem with a capability to detect penetration through the isolation zone and to permit response action."

5.4.1 An isolation zone is a key feature of a perimeter intrusion detection and assessment system (PIDAS). To meet these requirements, licensees should do the following:

5.4.1.1 The isolation zone should be established considering the zone of detection for the perimeter detection system and the assessment methods used (e.g., CCTV video-image capture, observation with optical devices such as binoculars, direct line of sight), so that accurate assessment may be made on either side of the perimeter barrier, either after receipt of an alarm or through proactive visual observation of the isolation zone by security force staff.

5.4.1.2 Positive assessment capabilities should be verified for all of the assessment methods used, during day, night, and various weather conditions, to ensure that the isolation zone provides for observation of persons on either side of the protected area barrier in the event of its penetration.

5.4.1.3 Intrusion alarm detection subsystem capabilities (i.e., detection, assessment, response) should be verified in the isolation zone to ensure persons passing through the zone are detected. Response actions associated with detection and assessment of a potential adversary incursion into the isolation zone should be adequate to provide a satisfactory probability of physical protection system effectiveness (Ref SAND2007-5591).

5.4.1.4 If adversary tunneling is determined to be a threat for the facility, a tunnel detection system should be installed in the isolation zone. And the system, or components thereof, should be mathematically performance tested for the probability-of-detection design goal of 90 percent probability of detection with a 95 percent confidence level, as described in Regulatory Position 3 of this RG.

5.5 Isolation zone illumination.

10 CFR 73.46(c)(4) states: "Isolation zones and all exterior areas within the protected area shall be provided with illumination sufficient for the monitoring and observation requirements of paragraphs (c)(3), (e)(8), (h)(4) and (h)(6) of this section, but not less than 0.2 footcandle measured horizontally at ground level."

10 CFR 73.46(e)(8) states: "All exterior areas within the protected area shall be monitored or periodically checked to detect the presence of unauthorized persons, vehicles, materials, or unauthorized activities."

10 CFR 73.46(h)(6) states: "To facilitate initial response to detection of penetration of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area shall be provided, preferably by means of closed-circuit television or by other suitable means which limit exposure of responding personnel to possible attack."

5.5.1 The established isolation zone is required to have certain illuminance (i.e., light level or luminous flux) that enables positive assessment during low-light conditions.

5.5.2 Regulatory Position 5.4.1discusses how to meet isolation zone features required per 10 CFR 73.46(c)(3).

5.5.3 Regulatory Position 5.10 discusses how to meet assessment aspects requirements per 10 CFR 73.46(h)(4) and (h)(6), respectively.

5.5.4 Regulatory Position 5.8 discusses how to meet monitoring/checking requirements for detection purposes for exterior areas within the protected area per 10 CFR 73.4(e)(8).

5.5.5 Light technologies, lighting design and the procedure for measuring light levels to ensure compliance with these illumination/detection/assessment requirements are discussed in NUREG-1959.

5.6 Duress alarms

10 CFR 73.46(e)(4) states: "All manned access control points in the protected area barrier, all security patrols and guard stations within the protected area, and both alarm stations shall be provided with duress alarms."

5.6.1 The typical perimeter of a facility that possesses special nuclear material consists of:

- a PIDAS,
- vehicle portals,
- personnel portals,
- buildings, and
- culverts.

5.6.2 "Manned access control points in the protected area barrier" refers to the vehicle and personnel portal locations.

5.6.3 So that intrusion detection may be alarmed by the protective force individuals manned in those locations, duress alarms should be installed with the following characteristics:

5.6.3.1 For ease of use by the individuals manning those locations, the duress alarm actuator should be in close proximity to where personnel are situated while conducting access portal operations.

5.6.3.2 The duress alarm actuator should be out of sight from persons, and persons in vehicles, while they are processing through the access control points.

5.7 Alarm annunciation

10 CFR 73.46(e)(5) states: "All alarms required pursuant to this section shall annunciate in a continuously manned central alarm station located within the protected area and in at least one other independent continuously manned onsite station not necessarily within the protected area."

10 CFR 73.46(e)(7) states: "All alarm devices including transmission lines to annunciators shall be tamper indicating and self-checking e.g., an automatic indication shall be provided when a failure of the alarm system or a component occurs, when there is an attempt to compromise the system or when the system is on standby power. The annunciation of an alarm at the alarm stations shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location. The status of all alarms and alarm zones shall be indicated in the alarm stations."

5.7.1 To meet 10 CFR 73.46(e)(5), all perimeter alarm detection signals should annunciate in parallel, in both the central and in the secondary alarm station (i.e., the other continuously manned station).

5.7.2 To meet the 10 CFR 73.46(e)(7) "…attempt to compromise…" requirement:

5.7.2.1 Line supervision should be established and maintained for transmission lines, and there must be the ability to display on the monitors in each alarm station the status of all alarms and alarm zones (e.g., perimeter alarm zones, balanced magnetic switches inside the protected area, tamper switches on data gathering panels).

5.7.2.2 Line supervision standards that should be complied with include UL Standards 1076, 1610, or 1635, or the lines may be encrypted in accordance with National Institute of Standards and Technology FIPS 197 or equivalent.

5.7.3 To meet 10 CFR 73.46(e)(7) requirements for: "…alarm devices \ transmission lines, tamper indication, self-checking, emergency exit alarm and indication of standby power:

5.7.3.1 For tamper-indicating requirement, the system should have the following characteristics:

5.7.3.1.1 Each sensor should have a tamper-indicating feature.

5.7.3.1.2 Each data gathering panel should have a tamper-indicating switch.

5.7.3.1.3 Each processor box for detection devices should have a tamper-indicating switch.

5.7.3.1.4 Tamper alarm testing procedures for intrusion alarm componentry (e.g., processor boxes, balanced magnetic switches, microwave sensors) are discussed in NUREG-1959.

5.7.3.2 For the self-checking requirement, each alarm system and component thereof should send an automatic indication when failure occurs to each alarm station, and that indication should describe the component, system, location, and type of failure.

5.7.3.3 For the indication of emergency exit alarm requirement, an annunciation should be conveyed to each alarm station when an emergency exit is detected as being utilized.

5.7.3.4 For the indication of standby power requirement, an annunciation of emergency power activation for the perimeter intrusion alarm system should be conveyed to each alarm station.

5.8 Surveillance within the protected area

10 CFR 73.46(e)(8) states: "All exterior areas within the protected area shall be monitored or periodically checked to detect the presence of unauthorized persons, vehicles, materials, or unauthorized activities."

5.8.1 This function provides a backup method of perimeter intrusion detection if the intrusion detection system located in the isolation zone is bypassed.

5.8.2 The following guidance applies to this requirement:

5.8.2.1 The monitoring and/or checking may be accomplished by the application of video assessment equipment (e.g., CCTV), direct visual observation, direct visual observation aided by the use of devices to enhance direct visual observation capabilities, random patrols, or a combination thereof.

5.8.2.2 Random patrols should be conducted rather than routine periodic ones. Random versus regularly scheduled patrols have a greater probability to detect/interrupt an adversary's planned conduct of a malevolent act.

5.8.2.3 The discovery of unauthorized persons, vehicles, materials, or unauthorized activities within an exterior area of the protected area should generate apprehension in the security force. This apprehension should then be resolved by an appropriate response by the licensee security organization that addresses the discovery. This monitoring/checking activity reduces an adversary's probability of success to exit or enter the protected area without being detected, consequently interrupted, and potentially neutralized.

5.9 Intrusion alarm system test and inspection during installation and construction

10 CFR 73.46(g) states: "The licensee shall have a test and maintenance program for intrusion alarms, emergency exit alarms, communications equipment, physical barriers, and other physical protection related devices and equipment used pursuant to this section that shall provide for the following; (1) Tests and inspections during the installation and construction of physical protection related subsystems and components to assure that they comply with their respective design criteria and performance specifications."

5.9.1 Before installation and construction of an alarm system or alarm system component, a licensee should: (1) make engineering drawings for the placement and location of the intrusion alarm system and alarm system components; and (2) develop a document that describes, as appropriate, the technical specifications for the alarm system as a whole and each individual alarm system component.

5.9.2 During installation and construction, the licensee should verify that the alarm system and its componentry are in alignment with both the engineering drawings and the technical specifications. In addition, as necessary, the engineering drawings and specification document should be adjusted to reflect field adjustments made to ensure that the installation and construction process produces an intrusion alarm system that functions as intended.

10 CFR 73.46(g)(2) requires the licensee's test and maintenance program for alarms provide "[p]reoperational tests and inspections of physical protection related subsystems and components to demonstrate their effectiveness and availability with respect to their respective design criteria and performance specifications."

5.9.3 To meet the NRC staff's expectation for this requirement, before operational activity following construction and installation of an intrusion detection system or components, the licensee should do the following:

5.9.3.1 Perform and document tests of the system.

5.9.3.2 These tests should include both operability and performance tests of both individual components and overall system infrastructure. The physical methods for performance and operability testing of intrusion detection systems and their components are described in NUREG-1959.

5.9.3.3 In addition, the system or components should be mathematically performance tested for the probability-of-detection design goal of 90 percent probability of detection with a 95 percent confidence level, as described in Regulatory Position 3 of this RG.

10 CFR 73.46(g)(3) requires the licensee's test and maintenance program for alarms provide "[o]perational tests and inspections of physical protection related subsystems and components to assure their maintenance in an operable and effective condition, including: (i) Testing of each intrusion alarm at the beginning and end of any period that it is used. If the period of continuous use is longer than seven days, the intrusion alarm shall also be tested at least once every seven days."

10 CFR 73.20(b)(4) requires that a Category I licensee establish and maintain, or arrange for, a physical protection system that "[i]ncludes a testing and maintenance program to assure control over all activities and devices affecting the effectiveness, reliability, and availability of the physical protection system, including a demonstration that any defects of such activities and devices will be promptly detected and corrected for the total period of time they are required as a part of the physical protection system."

5.9.4 To meet the NRC staff's expectation for these requirements, operability tests should be performed.

5.9.4.1 Operability tests include having an individual pass into the zone of detection of an intrusion detection sensor and verifying that an alarm is generated.

5.9.4.2 Operability tests are discussed in NUREG-1959.

5.9.4.3 In addition, performance tests should be conducted at least semi-annually.

5.9.4.4 Performance testing procedures which mathematically test for the probability of detection design goal of 90 percent probability of detection with a 95 percent confidence level, is described in Regulatory Position 3, "Recommended Testing Procedures."

10 CFR 73.46(g)(3)(ii) states that operational tests and inspections of physical protection-related subsystems and components shall include "[t]esting of communications equipment required for communications onsite, including duress alarms, for performance not less frequently than once at the beginning of each security personnel work shift. Communications equipment required for communications offsite shall be tested for performance not less than once a day."

5.9.5 To meet the NRC staff's expectation for this requirement for duress alarms, each duress alarm should be activated, and it should be verified that an alarm is generated and announced at the alarm stations at the beginning of each security personnel work shift.

10 CFR 73.46(g)(4) states: "Preventive maintenance programs shall be established for physical protection related subsystems and components to assure their continued maintenance in an operable and effective condition."

10 CFR 73.20(b)(4) requires that a Category I licensee establish and maintain, or arrange for, a physical protection system that"[i]ncludes a testing and maintenance program to assure control over all activities and devices affecting the effectiveness, reliability, and availability of the physical protection system, including a demonstration that any defects of such activities and devices will be promptly detected and corrected for the total period of time they are required as a part of the physical protection system."

5.9.6 To meet the NRC staff's expectation for these requirements, licensees should establish a documented preventive maintenance program for the intrusion detection alarm system through the development of procedures.

5.9.6.1 Procedures for preventive maintenance should include periodic observations of all components of an intrusion detection system to assess potential damage from environmental conditions, inadvertent employee actions, and potential tampering.

5.9.6.2 Proactive servicing of all intrusion detection alarm components should be conducted in accordance with manufacturer instructions.

5.9.6.3 Preventive maintenance procedures should include actions informed by the intrusion alarm technician's insights on the processes necessary to keep the intrusion detection system functioning as intended.

5.9.6.4 Preventive maintenance procedures should include actions to remedy either more than one false alarm per zone per day or more than one nuisance alarm per zone per day.

5.9.6.5 Preventive maintenance for an intrusion detection alarm system is discussed in NUREG-1959.

10 CFR 73.46(g)(5) states: "All physical protection related subsystems and components shall be maintained in operable condition. The licensee shall develop and employ corrective action procedures and compensatory measures to assure that the effectiveness of the physical protection system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures. Repairs and maintenance shall be performed by at least two individuals working as a team who have been trained in the operation and performance of the equipment. The security organization shall be notified before and after service is performed and shall conduct performance verification tests after the service has been completed."

5.9.7 To meet the NRC staff's expectation for this requirement, the licensee should establish both a corrective action and a compensatory measure program for the perimeter intrusion detection alarm system through the development and application of procedures for them.

5.9.7.1 Corrective actions and compensatory measures should be developed and implemented for observed failures.

5.9.7.2 As appropriate, corrective actions and compensatory measures should be proactively developed and established for anticipated probable failures that could be caused by events such as extreme weather conditions (e.g., hurricane), earthquakes, floods, fires, malevolent acts, and electrical power loss.

5.9.7.3 When corrective actions or compensatory measures require maintenance or repair of components of the intrusion detection system, the work shall be performed by at least two individuals who have been trained in the operation of the equipment and should have sufficient on-the-job experience to be able to recognize a tampering act being attempted by the other individual.

5.9.7.4 Before initiation of work to repair or maintain the intrusion detection system to alleviate a failure and dismiss compensatory measures, the security organization shall be notified.

5.9.7.4.1 This notification should be made to the alarm station operators and include the anticipated duration of the effort.

5.9.7.4.2 In addition, after such repair or maintenance has been completed, the security organization shall be notified.

5.9.7.4.3 The completion of task notification should be made to the alarm station operators.

5.9.7.5 Following completion of repair or maintenance, tests should be completed.

5.9.7.5.1 These tests should include both performance and operability tests.

5.9.7.5.2 Operability tests are simple tests, such as having a person walk through a detection zone and confirming that alarm station operators received an alarm within a few seconds for the zone in which the perimeter where the intrusion was made.

5.9.7.5.3 Operability tests should include a test that verifies that the perimeter intrusion alarm system functions as intended when the standby power (e.g., uninterruptible power/secondary power) switches on.

5.9.7.5.4 Refer to the performance and operability test discussion in the Regulatory Position 3 of this RG and in NUREG-1959.

5.10 Perimeter intrusion detection alarm system assessment features

10 CFR 73.46(h)(4) states, in part, "[u]pon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, a material access area, or a vital area, or upon evidence or indication of intrusion into a protected area, a material access area, or a vital area, the licensee security organization shall: (i) Determine whether or not a threat exists, (ii) Assess the extent of the threat, if any."

10 CFR 73.46(h)(6) states: "To facilitate initial response to detection of penetration of the protected area and assessment of the existence of a threat, a capability of observing the isolation zones and the physical barrier at the perimeter of the protected area shall be provided, preferably by means of closed-circuit television or by other suitable means which limit exposure of responding personnel to possible attack."

5.10.1 To meet the NRC staff's expectation for this requirement, the licensee should, upon detection of abnormal presence or activity of persons or vehicles within the isolation zone, or indication of intrusion or potential attempted intrusion into the isolation zone or protected area, assess the location of the detection or indication to determine if a threat exits and, as appropriate, the extent of the threat.

5.10.2 The detection of abnormal presence or activity or indication of intrusion may be received from an individual reporting such an event, a detection alarm from the perimeter intrusion alarm system, or both.

5.10.3 Given these conditions of a possible malevolent threat, to the degree practicable, assessment should be performed using a camera system (e.g., CCTV) that captures a video- image and transmits it to a remote location (e.g., alarm station) for observation that eliminates or significantly reduces the probability of physical injury to the individual performing the assessment.

5.11 Early Warning System

5.11.1 If the licensee discovers that an early warning system (EWS) is needed in order to meet the general performance objective described in 10 CFR 73.20(a), then that system should meet the established intrusion detection alarm system criterion guidance in the Regulatory Position 8.13.5.1 through 8.13.5.4.

5.12 Power Supply

10 CFR 73.46(e)(6) states: "All alarms required by this section shall remain operable from independent power sources in the event of the loss of normal power. Switchover to standby power shall be automatic and shall not cause false alarms on annunciator modules."

5.12.1 To enable meeting this requirement, the licensee should design and implement an on-site standby electrical power system. The guidance in the Regulatory Position 1.3 of this guide, "System Electrical Specifications," should be followed.

5.12.2 Testing procedures should be developed and followed to determine if switchover to standby power is automatic when offsite power is lost and assessed that no false alarms are incurred during or after the switchover.

5.12.3 Testing of the switchover from offsite power to onsite power should be conducted at regular semi-annual intervals and the results thereof should be documented and retained as records for at least 3 years, consistent with 10 CFR 73.70.

6. GUIDANCE REGARDING PERIMETER INTRUSION ALARM SYSTEMS REQUIRED BY 10 CFR 73.50

6.0.1 10 CFR 73.50 is applicable to a formula quantity (also termed a Category I quantity) of strategic special nuclear material, as defined in 10 CFR 73.2, that is not readily separable from other radioactive material and that has a total external radiation dose rate in excess of 100 rem per hour at a distance of 3 feet from any accessible surfaces without intervening shielding other than at a nuclear reactor facility licensed under 10 CFR Parts 50 or 52.

10 CFR 73.50(b)(4) states: "An isolation zone shall be maintained around the physical barrier at the perimeter of the protected area and any part of the building used as part of that physical barrier. The isolation zone shall be monitored to detect the presence of individuals or vehicles within the zone so as to allow response by armed members of the license security organization to be initiated at the time of penetration of the protected area."

6.1 Protected area perimeter intrusion alarm system

6.1.1 In the isolation zone, perimeter intrusion alarm systems should use sensor devices that provide detection.

6.1.2 Applicable terrain exterior sensor detection devices include, but are not limited to, microwave sensors, electric field sensors, ported coaxial cable systems, active infrared sensors, taut wire sensors, and fence disturbance sensors.

6.1.3 Each of these listed sensors are described in NUREG-1959.

6.1.4 A perimeter intrusion alarm system should also contain five elements:

1. electronic processing equipment (that includes a means for maintaining and providing an alarm history),
2. a power supply,
3. signal transmission media,
4. an alarm monitor with display, and
5. an assessment system.

6.1.5 These elements are also described in NUREG-1959.

6.1.6 Because this requirement specifies an armed response in parallel with penetration of the protected area by persons or vehicles, sensors for detection installed in the isolation zone connected to a dedicated assembled alarm system should be implemented.

6.1.6.1 Specifically, to assess the cause of an alarm generated by a perimeter sensor, CCTV or similar video assessment equipment should be used that projects images in an alarm station that can be viewed by alarm station operators.

6.1.6.2 Alternatively, security personnel may be dispatched to observe the location of the sensor causing the alarm.

6.1.6.3 However, this method (i.e., dispatch of security personnel) has disadvantages because

6.1.6.3.1 the alarm may have been a false or nuisance alarm and the resources expended for security personnel dispatch would therefore have been unnecessary, and

6.1.6.3.2 immediate dispatch of security personnel without first determining the magnitude of the threat, if any, poses a significant risk of physical injury to those security personnel deployed, which may, in turn, reduce the ability of the licensee's security organization to protect the onsite special nuclear material against radiological sabotage or theft.

6.2 Isolation zone

6.2.1 An isolation zone should be a key feature of a protected area PIDAS.

6.2.2 The isolation zone should be established considering the zone of detection for the perimeter detection system and the assessment methods used (e.g., CCTV video-image capture or similar video assessment equipment, observation with optical devices such as binoculars, direct line of sight), so that accurate assessment may be made on either side of the perimeter barrier, either after receipt of an alarm or through proactive visual observation of the isolation zone by security force staff.

6.2.3 Positive assessment capabilities should be verified for all of the assessment methods used, during day, night, and various weather conditions, to ensure that the isolation zone

provides for observation of persons on either side of the protected area barrier in the event of its penetration.

6.2.4 Also, intrusion alarm detection subsystem capabilities should be verified in the isolation zone to ensure persons passing through the zone are detected.

6.3 Material access area perimeter intrusion detection systems

10 CFR 73.50(c)(4) states, in part, that "[u]noccupied vital areas and material access areas shall be protected by an active intrusion alarm system."

10 CFR 73.50(g)(3) states, in part, the following response requirement: "Upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, or a vital area; or upon evidence or indication of intrusion into a protected area, material access area, or vital area, the licensee security organization shall: (i) Determine whether or not a threat exists, (ii) Assess the extent of the threat, if any, and (iii) Take immediate concurrent measures to neutralize the threat."

6.3.1 For intrusion detection equipment at a material access area perimeter, a balanced magnetic switch should be used on each door or movable barrier to allow detection of attempted or actual unauthorized access.

6.3.2 Balanced magnetic switches should have the following characteristics:

6.3.2.1 Meet UL 634 requirements for a level 2 high-security switch, balanced magnetic switch.

6.3.2.2 Initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normal secured position.

6.3.2.3 Initiate an alarm when the door moves more than 2.5 centimeters (1 inch) from the fully closed position.

6.4 Isolation zone illumination

10 CFR 73.50(b)(5) states: "Isolation zones and clear areas between barriers shall be provided with illumination sufficient for the monitoring required by paragraphs (b)(3) and (4) of this section, but not less than 0.2-foot candles."

6.4.1 The established isolation zone is required to have a certain illuminance (i.e., light level or luminous flux) that enables positive assessment during low-light conditions.

6.4.2 Light technologies, lighting design, and the procedure for measuring light levels to ensure compliance with this illumination requirement are discussed in NUREG-1959.

6.5 Alarm annunciation

10 CFR 73.50(d)(1) states, in part, that "[a]ll alarms required pursuant to this part shall annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station… The annunciation of an alarm at the onsite

central station shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location."

6.5.1 To meet this requirement, all perimeter alarm detection signals must annunciate concurrently in both the central alarm station and the secondary alarm station.

6.5.2 Alarm devices and transmission lines should have the following capabilities:

- tamper indication,
- self-checking, and
- line supervision.

10 CFR 73.50(d)(1) states, in part, that "[a]ll alarms shall be self-checking and tamper indicating.... All intrusion alarms, emergency exit alarms, alarm systems, and line supervisory systems shall at minimum meet the performance and reliability indicated by GSA Interim Federal Specification W-A-00450 B (GSA-FSS). The GSA Interim Federal Specification has been approved for incorporation by reference by the Director of the Federal Register."

6.5.3 In accordance with 10 CFR 73.50(d)(1), a licensee must meet the GSA Interim Federal Specification W-A-00450 B.

However, GSA Interim Federal Specification W-A-00450 B is outdated and no longer in use. Therefore, the NRC recommends that licensees submit an exemption request, per 10 CFR 73.5, "Specific Exemptions," to use the following specifications:

- Underwriters Laboratories (UL) 1076, or 1610, or 1635, or
- Lines should have encryption in accordance with the National Institute of Standards and Technology Federal Information Processing Standard (FIPS) 197 Advanced Encryption Standard (AES) or equivalent.

6.5.4 To meet the self-checking and tamper-indicating requirement, licensees should ensure the following:

6.5.4.1 Each sensor should have a tamper-indicating feature.

6.5.4.2 Each data-gathering panel should have a tamper-indicating switch.

6.5.4.3 Each processor box for detection devices should have tamper-indicating switch.

6.5.4.4 Each alarm system and component thereof should send an automatic indication when failure occurs to each alarm station, and that indication should describe the component or system, location, and type of failure.

6.5.4.5 Line supervision should be established and maintained for transmission lines.

6.5.4.6 There should be the ability to display line supervision status on the monitors in each alarm station.

6.5.4.7 The status of all alarm and alarm zones (e.g., perimeter alarm zones, balanced magnetic switches inside the protected area, tamper switches on data-gathering

panels) should display on the monitors in each of the alarm stations. This is because, per 10 CFR 73.50(d)(1), "Alarm annunciation," states, "…shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location."

6.5.4.8 Tamper alarm testing procedures for intrusion alarm components (e.g., processor boxes, balanced magnetic switches, microwave sensors) are discussed in NUREG-1959.

6.6 Testing and maintenance of perimeter intrusion alarm systems

10 CFR 73.50(f) states: "Testing and maintenance. Each licensee shall test and maintain intrusion alarms, emergency alarms, communications equipment, physical barriers, and other security related devices or equipment utilized pursuant to this section as follows: (1) All alarms, communications equipment, physical barriers, and other security related devices or equipment shall be maintained in operable and effective condition. (2) Each intrusion alarm shall be functionally tested for operability and required performance at the beginning and end of each interval during which it is used for security, but not less frequently than once every seven (7) days."

6.6.1 For each perimeter intrusion alarm component, maintenance should be performed in accordance with the manufacturer's specifications.

6.6.2 Operability testing must be performed at the beginning of each interval (e.g., shift change) but not less frequently that every 7 days.

6.6.3 The phrase "required performance" in this context means that the perimeter intrusion alarm component functions as intended when a simulated intrusion is tested; this type of test is required in the same periodicity as the operability test.

6.6.4 In contrast, comprehensive performance tests should be designed to verify the level of performance of each perimeter intrusion alarm component through its range of intended function.

6.6.5 Comprehensive performance tests should be performed semi-annually and before operation after maintenance or initial installation.

6.6.6 Operability and performance tests for perimeter intrusion detection alarm components are discussed in NUREG-1959. Comprehensive performance tests are described as "performance tests" in NUREG-1959.

6.7 Alarm assessment system

For the assessment upon detection, 10 CFR 73.50(g) states, in part: "(3) Upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, or a vital area; or upon evidence or indication of intrusion into a protected area, material access area, or vital area, the licensee security organization shall: (i) Determine whether or not a threat exists, (ii) Assess the extent of the threat, if any."

6.7.1 An assessment of whether or not a threat exists must be performed if detection is made of abnormal presence or activity of persons or vehicles within an isolation zone or protected

area, or if detection occurs upon discovered evidence or indication of intrusion into a protected area, by line-of-sight observation, through the use of an optical viewer (e.g., CCTV, binoculars), or by a perimeter alarm sensor.

6.7.2 The assessment should preferably be accomplished in such a manner that security personnel, while conducting the assessment operations, have a minimum probability of physical harm (i.e., by using CCTV or a similar video assessment system).

6.7.3 The assessment process must produce two results:
1. the determination of whether or not a threat exists, and
2. a determination of the extent of the threat, if any.

6.8 Early Warning

6.8.1 If a licensee discovers that an early warning system (EWS) is needed in order to meet the response requirement described in 10 CFR 73.50(g)(3) in an adequate manner, then that system should meet the established intrusion detection alarm system criterion guidance in the Regulatory Position 8.13.5.1 through 8.13.5.4.

7 GUIDANCE PERTAINING TO STORED SPENT NUCLEAR FUEL AND HIGH-LEVEL RADIOACTIVE WASTE PERIMETER INTRUSION ALARM SYSTEMS AS REQUIRED BY 10 CFR 73.51

10 CFR 73.51(d)(3) describes the requirement for a protected area with a perimeter that has an intrusion detection system as follows: "The perimeter of the protected area must be subject to continual surveillance and be protected by active intrusion alarm system which is capable of detecting penetrations through the isolation zone."

7.1 Perimeter intrusion alarm system

7.1.1 Perimeter intrusion alarm systems should use sensor devices that provide detection**.**

7.1.2 Applicable terrain exterior sensor detection devices include, but are not limited to,
- microwave sensors,
- electric field sensors,
- ported coaxial cable systems,
- active infrared sensors,
- taut wire sensors, and
- fence disturbance sensors.

Each of these sensors are described in NUREG-1959.

7.1.3 A perimeter intrusion alarm system should also contain five elements:
1. electronic processing equipment (that includes a means for maintaining and providing an alarm history)
2. a power supply,
3. a signal transmission media,
4. an alarm monitor with display, and
5. as assessment system.

These elements are also described in NUREG-1959.

7.2 Alarm assessment system

10 CFR 73.51(d)(3), which states, in part, that "[a] timely means for assessment of alarms must also be provided."

7.2.1 A sensor detection generates an alarm. To ascertain the cause of the detection and corresponding alarm, an assessment should be performed. There are three types of alarm:

1. false alarm,
2. nuisance alarm,
3. actual alarm.

False and nuisance alarms are described in NUREG-1959.

7.2.2 The action of assessment may be conducted by security personnel through visual observation by line of sight, or through the use of video assessment equipment (e.g., CCTV) that has a video-image capture capability. Video-image capture assembles the before and after video frames of a sensor detection event. Captured video frames are then viewed by alarm station security personnel to determine the potential cause of the event. Video-image capture is described in NUREG-1959.

7.3 Isolation zone

10 CFR 73.51(d)(1) states: "Spent nuclear fuel and high-level radioactive waste must be stored only within a protected area so that access to this material requires passage through or penetration of two physical barriers, one barrier at the perimeter of the protected area and one barrier offering substantial penetration resistance. The physical barrier at the perimeter of the protected area must be as defined in 10 CFR 73.2. Isolation zones, typically 20 feet wide each, on both sides of this barrier, must be provided to facilitate assessment. The barrier offering substantial resistance to penetration may be provided by approved storage cask or building walls such as those of a reactor or fuel storage building."

7.3.1 An isolation zone should be a key feature of a PIDAS.

7.3.2 The isolation zone should be established considering the zone of detection for the perimeter detection system and the assessment methods used (e.g., CCTV with video-image capture, observation with optical devices such as binoculars, direct line of sight), so that accurate assessment may be made on either side of the perimeter barrier, either after receipt of an alarm or through proactive visual observation of the isolation zone by security force staff.

7.3.3 Positive assessment capabilities should be verified for all of the assessment methods used, during day, night, and various weather conditions, to ensure that the isolation zone provides for observation of persons on either side of the protected area barrier in the event of its penetration.

7.3.4 Also, intrusion alarm detection subsystem capabilities should be verified in the isolation zone to ensure persons passing through the zone are detected.

7.4 Illumination

10 CFR 73.51(d)(2) states: "Illumination must be sufficient to permit adequate assessment of unauthorized penetrations of or activities within the protected area."

7.4.1 To meet this requirement to enable adequate assessment of unauthorized penetrations of the protected area, the established isolation zone should have an illuminance (i.e., light level or luminous flux) that enables positive assessment during low-light conditions.

7.4.2 The recommended illumination level for monitoring and observation should be a level adequate for alarm station operators and other security personnel to perform discriminating assessment functions, but not less than 0.2 footcandle measured horizontally at ground level.

7.5 Surveillance within the protected area.

10 CFR 73.51(d)(4) states: "The protected area must be monitored by daily random patrols."

7.5.1 The protected area is required to be monitored by daily random patrols.

7.5.2 This function provides a secondary method of perimeter intrusion detection if the intrusion detection system located in the isolation zone is bypassed.

7.5.3 The discovery of unauthorized persons, vehicles, materials, or unauthorized activities within the protected area should generate apprehension in the security force.

7.5.4 This apprehension should then be resolved by a response that addresses the discovery and consequently potentially reduces an adversary's probability of success to conduct a successful theft or radiological sabotage scenario and exit or enter the protected area without being detected, interrupted, or neutralized.

7.6 Sufficient personnel necessary to operate the alarm system

10 CFR 73.51(d)(5) states, in part: "The security organization must include sufficient personnel per shift to provide for monitoring of detection systems and the conduct of surveillance, assessment, access control, and communications to assure adequate response."

7.6.1 The licensee should provide staff in sufficient numbers per shift in both the primary and secondary alarm stations so that:

- detection alarms can be recognized,
- assessment actions can be performed,
- access control device alarms may be assessed,
- communications can be transmitted, all in such a manner that adequate protection can be maintained.

7.6.2 Alarm system tamper indication and line supervision

10 CFR 73.51(d)(11), states, in part: "All detection systems and supporting subsystems must be tamper indicating with line supervision."

7.6.2.1 To meet the tamper-indicating and line supervision requirement, the systems should have the following characteristics:

7.6.2.1.1 Each sensor should have a tamper-indicating feature.

7.6.2.1.2 Each data gathering panel should have a tamper-indicating switch.

7.6.2.1.3 Each processor box for detection devices should have a tamper-indicating switch.

7.6.2.1.4 Each alarm system and component thereof should send an automatic indication when failure occurs to each alarm station, and that indication should describe the component, system, location, and type of failure.

As per 10 CFR 73.51(d)(11), line supervision must be established and maintained for the intrusion detection system transmission lines.

7.6.2.2 There should be the ability to display on the monitors in each alarm station the status of all alarm and alarm zones (e.g., perimeter alarm zones, balanced magnetic switches inside the protected area, tamper switches on data-gathering panels).

7.6.2.3 Line supervision standards that should be complied with include UL Standards 1076, 1610, or 1635, or lines may have encryption in accordance with National Institute of Standards and Technology FIPS 197 or equivalent.

7.6.2.4 Tamper alarm testing procedures for intrusion alarm components (e.g., processor boxes, balanced magnetic switches, microwave sensors) are discussed in NUREG-1959.

7.6.3 Alarm system maintenance

10 CFR 73.51(d)(11), states, in part: "All detection systems and supporting subsystems must be tamper indicating with line supervision. These systems, as well as surveillance/assessment and illumination systems, must be maintained in operable condition."

7.6.3.1 To meet the "maintained in operable condition" requirement, a maintenance program for the alarm system should be established.

7.6.3.2 The program should consist of procedures for each alarm system component.

7.6.3.3 Each procedure should specify the actions, and the periodicity of those actions, to be accomplished for maintenance in accordance with the manufacturer's specifications.

7.6.3.4 In addition, maintenance procedures should include maintenance insights provided by onsite alarm technicians.

7.6.4 Alarm system compensatory measures

10 CFR 73.51(d)(11) states, in part: "Timely compensatory measures must be taken after discovery of inoperability, to assure that the effectiveness of the security system is not reduced."

7.6.4.1 To meet the NRC staff's expectation for this requirement, the licensee should establish a compensatory measure program for the perimeter intrusion

detection alarm system through the development and application of procedures for them.

7.6.4.2 Compensatory measures should be developed and should be implemented for discovered failures.

7.6.4.3 As appropriate, compensatory measures should be proactively developed and established for anticipated probable failures that could be caused by events such as extreme weather conditions (e.g., hurricane), earthquakes, floods, fires, malevolent acts, and electrical power loss.

7.6.4.4 When compensatory measures are required for maintenance or repair of components of the intrusion detection system, the work should be performed by two individuals who have been trained in the operation of the equipment and should have sufficient on-the-job experience to be able to recognize tampering being attempted by the other individual.

7.6.4.5 Before initiation of work to repair or maintain the intrusion detection system to alleviate a failure, or accomplish maintenance, and dismiss compensatory measures, the security organization should be notified. This notification should be made to the alarm station operators and include the anticipated duration of the effort. In addition, after such repair or maintenance has been completed, the security organization should be notified with a completion of task notification made to the alarm station operators.

7.6.4.6 Following the completion of a repair or maintenance, functionality tests should be completed. Functionality tests should include both performance and operability tests**.** (Refer to the performance test (Regulatory Position 3) and operability test (Regulatory Position 5.9.4.1) discussions in this RG and in NUREG-1959.)

7.7 Record Requirements

10 CFR 73.51(d)(13), states, in part: "The following documentation must be retained as a record for 3 years after the records is made or until termination of the license…(iii) A log of all patrols…(iv) A record of each alarm received, identifying the type of alarm, location, date and time when received, and disposition of the alarm."

7.7.1 To meet the NRC staff's expectation for 10 CFR 73.51(d)(13)(iii), the licensee must log all protected area daily random patrols that are required per 10 CFR 73.51(d)(4).

7.7.2 To meet the NRC staff's expectation for 10 CR 73.51(d)(13)(iv), the licensee must retain records of each alarm received, together with the description of the type of alarm: (e.g., balanced magnetic switch); location of the alarm generation (e.g., door 34-bldg 10); date and time when received; and disposition of the alarm.

7.7.3 These log entries must be retained for 3 years after a record is made or until termination of the license.

7.8 Early Warning System

7.8.1 If a licensee discovers that an early warning system (EWS) is needed in order to meet the general performance objective described in 10 CFR 73.51(b), then that system should meet the established intrusion detection alarm system criterion guidance in the Regulatory Position 8.13.5.1 through 8.13.5.4.

8 NUCLEAR POWER PLANT LICENSEE PERIMETER INTRUSION ALARM SYSTEMS REQUIRED BY 10 CFR 73.55

10 CFR 73.55(e)(7)(i), states, in part: "An isolation zone must be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone shall be: (A) Designed and of sufficient size to permit observation and assessment of activities on either side of the protected area barrier; (B) Monitored with intrusion detection equipment designed to satisfy the requirements of 10 CFR 73.55(i) and be capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier."

8.1 Perimeter intrusion alarm systems

8.1.1 For the monitoring required under 10 CFR 73.55(e)(7)(i)(B), perimeter intrusion alarm systems should use sensor devices that provide detection.

8.1.2 Applicable terrain exterior sensor detection devices include, but are not limited to,

- microwave sensors,
- electric field sensors,
- ported coaxial cable systems,
- active infrared sensors,
- taut wire sensors, and
- fence disturbance sensors.

Each of these sensors is described in NUREG-1959.

8.1.3 If adversary tunneling is determined to be a threat for the facility, a tunnel detection system should be installed in the isolation zone. And the system, or components thereof, should be mathematically performance tested for the probability-of-detection design goal of 90 percent probability of detection with a 95 percent confidence level, as described in Regulatory Position 3 of this RG.

8.1.4 A perimeter intrusion alarm system should also contain five elements:

1. electronic processing equipment (that includes a means for maintaining and providing an alarm history),
2. a power supply,
3. signal transmission media,
4. an alarm monitor with display,
5. an assessment system.

These elements are also described in NUREG-1959.

8.1.5 Because this requirement includes detection of unauthorized access before penetration of the protected area barrier, the use of detection sensors with a field of view that extends outwards from or at the protected area barrier, coupled with a CCTV video-image capture system for assessment, or a similar video assessment system, is recommended.

8.1.6 Because this requirement specifies an armed response in parallel with penetration of the protected area by persons or vehicles, sensors for detection installed in the isolation zone connected to a dedicated assembled alarm system should be implemented.

8.1.7 Specifically, to assess the cause of an alarm generated by a perimeter sensor, CCTV or similar video assessment equipment should be used that projects images in an alarm station that can be viewed by alarm station operators.

8.1.8 Alternatively, security personnel may be dispatched to observe the location of the sensor causing the alarm.

8.1.9 However, this method (i.e., dispatching security personnel) has disadvantages because:

8.1.9.1 the alarm may have been a false or nuisance alarm and the resources expended for security personnel dispatch would therefore have been unnecessary,

8.1.9.2 immediate dispatch of security personnel without first determining the magnitude of the threat, if any, poses a significant risk of physical injury to those security personnel deployed, which may, in turn, reduce the ability of the licensee's security organization to protect the onsite special nuclear material against radiological sabotage or theft.

8.2 Alarm assessment system

10 CFR 73.55(e)(7)(i)(C), states that the isolation zone shall be "[m]onitored with assessment equipment designed to satisfy the requirements of 10 CFR 73.55(i) and provide real-time and play-back/recorded video images of the detected activities before and after each alarm annunciation."

10 CFR 73.55(e)(ii) states: "Obstructions that could prevent the licensee's capability to meet the observation and assessment requirements of this section must be located outside of the isolation zone."

8.2.1 A sensor detection generates an alarm. An assessment should be performed to ascertain the cause of the detection and corresponding alarm. There are three types of alarm:

1. false alarm,
2. nuisance alarm, and
3. actual alarm.

False and nuisance alarms are described in NUREG-1959.

8.2.2 The action of assessment may be conducted by security personnel through:

1) visual observation by line of sight, or

2) the use of video assessment equipment (e.g., CCTV) that has a video-image capture capability.

8.2.3 To meet this requirement, video assessment system with video-image capture capability should be used.

8.2.3.1 Video-image capture assembles the before, during, and after video frames of a sensor detection event.

8.2.3.2 Captured video frames are then viewed by alarm station security personnel to determine the potential cause of the event.

8.2.3.3 Details of video-image capture is described in NUREG-1959.

8.2.4 To meet the requirement of not having an obstruction that encumbers assessment capabilities associated with observation into the isolation zone, the design of the isolation zone should plan that objects that could potentially block the view of an assessment capability should be out of view of assessment capabilities.

Objects found after the implementation of the isolation zone that hinder assessment capabilities should be reconfigured to allow adequate assessment functions, or the licensee should design and implement a revised assessment strategy that allows assessment operations to function as intended.

8.3 Isolation zone

10 CFR 73.55(e)(7)(i), states, in part, "An isolation zone must be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone shall be: (A) Designed and of sufficient size to permit observation and assessment of activities on either side of the protected area barrier."

8.3.1 An isolation zone is a key feature of a PIDAS.

8.3.2 The isolation zone should be established considering the zone of detection for the perimeter detection system and the assessment methods used (e.g., CCTV with video-image capture, observation with optical devices such as binoculars, direct line of sight), so that accurate assessment may be made on either side of the perimeter barrier, either after receipt of an alarm or through proactive visual observation of the isolation zone by security force staff and surveillance of the area outside of the protected area.

8.3.3 Positive assessment capabilities should be verified for all of the assessment methods used, during day, night, and various weather conditions, to ensure that the isolation zone provides for observation of persons on either side of the protected area barrier in the event of its penetration.

8.3.4 Also, intrusion alarm detection subsystem capabilities should be verified in the isolation zone to ensure persons passing through the zone are detected.

8.4 Penetrations through the protected area barrier

10 CFR 73.55(e)(8)(ii) states: "Penetrations through the protected area barrier must be secured and monitored in a manner that prevents or delays and detects the exploitation of any penetration."

8.4.1 Passageways through the protected area barrier, such as gates or culverts, can be monitored by constant visual observation to provide detection.

8.4.1.1 However, the ability for personnel to maintain a constant visual alertness on one area will diminish after a 20-minute time period.

- In a 1999 study "The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies," by M.W. Green (Ref. 39), psychologists discovered the human attention span lasts roughly 20 minutes. After these 20 minutes, security guards will miss up to 95 percent of occurrences.

8.4.1.2 Therefore, to meet this requirement with an acceptable probability of detection (i.e., 90 percent probability of detection with 95 percent confidence), it is recommended to use a sensor system for detection.

8.4.2 Gates can be outfitted with a balanced magnetic switch or situated in the field of view of a microwave intrusion detection sensor, and other detection technologies may be found to be appropriate.

8.4.3 In the circumstance of unattended openings (e.g., culverts or pipes) that penetrate the protected area barrier or other security boundary, the license may install a fiber optic sensor in a grating physical barrier that has been shown to be effective at detecting intrusion and attempted intrusion to an acceptable probability of detection.

8.4.4 Penetrations through the protected area barrier may have physical barrier configurations that prevent or delay unauthorized intrusion into the protected area.

8.4.4.1 The securing and monitoring scheme of the penetration must be sufficient to detect, assess, and respond to an intrusion in enough time to meet the general performance objective set forth in 10 CFR 73.55(b)(1).

8.4.4.2 If the barrier configuration is intended to delay, with the objective to prevent exploitation of the opening, then the periodicity of monitoring should be sufficient to detect an unauthorized intrusion in enough time to provide an adequate security response that prevents adversarial exploitation of the penetration.

8.5 Detection/assessment for walls, roofs, and exterior areas within the protected area

10 CFR 73.55(e)(8) states, in part, "(iv) Where building walls or roofs comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary provided that the detection and assessment requirements of this section are met, appropriate barriers are installed, and the area is described in the security plans. (v) All exterior areas within the protected area, except for areas that must be excluded for safety reasons, must be periodically checked to detect and deter unauthorized personnel, vehicles, and materials."

8.5.1 To meet this requirement when a wall and/or roof comprises a portion of the protected area barrier, several physical protection elements may be used, depending on the wall's construction characteristics.

8.5.1.1 If the wall is not high enough to withstand the capabilities of the design-basis threat adversary, then per 10 CFR 73.55(e)(8)(iv) intrusion detection should be installed outside of the wall, or on the roof, and installed into any openings (e.g., windows) on the wall.

8.5.1.2 If the wall is not constructed with the durability to withstand a penetration from the design-basis threat adversary, then to meet 10 CFR 73.55(e)(8)(iv) the licensee should install detection on the outside of the wall, within the potential adversary pathways in the building, or on the inside of the specific wall.

8.5.1.3 In order to meet the requirements of 10 CFR 73.55(e)(8)(iv), if a roof may be accessed by a design-basis threat adversary, by scaling a wall of that building, the roof should have detection on it.

8.5.1.3.1 If the roof does not have intrusion detection installed on it and the roof may be penetrated by a design-basis threat adversary, the interior of the building should have intrusion detection capabilities in it.

8.5.1.3.2 An acceptable alternative would be to install intrusion detection at the bottom of the wall that is on the outside boundary of the protected area.

8.5.1.3.3 An assessment system must accompany any detection systems installed, as required in 10 CFR 73.55(i), "Detection and assessment systems."

8.5.1.4 In order to meet the requirements of 10 CFR 73.55(e)(8)(iv), if the roof cannot be penetrated by a design-basis threat adversary, then the pathway for an adversary entering the protected area that uses a wall or roof should have detection and assessment installed in that pathway.

8.5.1.4.1 The pathway could be up the outside wall, then across the roof, and down the wall inside the protected area.

8.5.1.4.2 An alternate pathway could be up the wall to the roof, through the roof, inside the building, and exiting the building into the protected area.

8.5.1.4.3 Other specific pathways that adversaries might use depend on the individual site characteristics.

8.5.1.5 In order to meet the requirements of 10 CFR 73.55(e)(8)(iv) and 10 CFR 73.55(i), all detection signals received to meet this requirement must have either:

1) security personnel viewing a visual display provided by a video assessment system (e.g., CCTV) that has video image capture capability, or
2) assessment capability that includes a security personnel response.

8.5.1.6 In order to meet the requirements of 10 CFR 73.55(e)(8)(iv), the wall and or roof areas where an isolation zone is not utilized shall be described in the security plans.

8.5.1.7 Exterior areas within the protected area, except for areas that must be excluded for safety reasons, must be periodically checked to detect and deter unauthorized personnel, vehicles, and materials, per 10 CFR 73.55(e)(8)(v).

8.5.1.7.1 This check activity along with its periodicity, whether a random check, performed a certain number of times per (e.g., day or shift), or a rigidly scheduled check sequence, should be documented in a procedure and described in security plans. Random checks have a greater probability to detect/interrupt an adversary's planned conduct of a malevolent act than regularly scheduled checks.

8.6 Detection at access portals

10 CFR 73.55(g)(1)(i)(B) states: "Equip access control portals with locking devices, intrusion detection equipment, and surveillance equipment consistent with the intended function."

8.6.1 The access portal and vehicle access portal for protected area personnel are both located at the perimeter of the protected area. Consequently, intrusion detection is required, as necessary in an access portal, to identify potential unauthorized access to the protected area.

8.6.2 Arrangements to provide intrusion detection to meet these requirements can consist of the following:

8.6.2.1 There are balanced magnetic switches on both entry and exit doors of the portal.

8.6.2.2 There are access denial turnstiles that alarm when the correct credentials are not applied and that are located after the search train equipment on the pathway from outside to inside the protected area.

8.6.2.3 Microwave sensors or other detection equipment is installed on the roof of the access portal.

8.6.2.4 Personnel gates to the vehicle inspection area are outfitted with balanced magnetic switches.

8.6.2.5 The vehicle gate that permits entry into the protected area is outfitted with a balanced magnetic switch.

8.6.2.6 All other adversary pathways around or through an access portal are outfitted with intrusion detection equipment (e.g., infrared, fence disturbance, microwave) as appropriate.

8.6.2.7 Surveillance equipment is installed that enables accurate assessment of any detection signal received from all of the intrusion detection sensors in an access portal area.

8.7 Detection and assessment systems

10 CFR 73.55(i) states, in part, that "(1) The licensee shall establish and maintain intrusion detection and assessment systems that satisfy the design requirements of 10 CFR 73.55(b) and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the effective implementation of the licensee's protective strategy. (2) Intrusion detection equipment must annunciate, and video assessment equipment shall display concurrently, in at least two continuously staffed onsite alarm stations, at least one of which must be protected in accordance with the requirements of the central alarm station within this section."

8.7.1 The requirements of 10 CFR 73.55(i)(1) can be met as described in Regulatory Position 7.1.

8.7.2 The requirements of10 CFR 73.55(i)(2) can be met by establishing an onsite system that enables intrusion detection signals to annunciate and video assessment signals to display simultaneously in both the central and secondary alarm station.

8.8 Alarm annunciation

10 CFR 73.55(i)(3) states, in part: "The licensee's intrusion detection and assessment systems must be designed to: (i) Provide visual and audible annunciation of the alarm."

8.8.1 To meet this requirement, the perimeter intrusion detection system should display a detection alarm signal of sufficient size and luminosity on the system's computer monitors in the central and secondary alarm stations that it provides unambiguous information that an alarm station operator can understand and consequently take the correct action to either resolve the alarm, and if necessary, initiate a security response.

8.8.2 In addition, to capture the alarm station operator's attention, the detection alarm signal should also activate an audible alert of sufficient decibels simultaneously with the visual display.

8.8.3 Both the visual and audible indicators should not stop annunciating until the alarm station operator takes specific action to stop them.

8.9 Visual alarm display

10 CFR 73.55(i)(3) states in part: "The licensee's intrusion detection and assessment systems must be designed to: … (ii) Provide a visual display from which assessment of the detected activity can be made."

8.9.1 To meet this requirement, the visual display for a perimeter intrusion detection alarm should have three components:

1. an indication of the alarm type (e.g., balanced magnetic switch),
2. an indication of the alarm location (e.g., door 15, building 25), and
3. a set of video frames that display the area of detection immediately before, during, and immediately after the initial detection event.

8.10 Alarm annunciation

10 CFR 73.55(i)(3) states, in part: "The licensee's intrusion detection and assessment systems must be designed to: … (iii) Ensure that annunciation of an alarm indicates the type and location of the alarm."

8.10.1 To meet this requirement, the visual or audible alarm annunciation from a perimeter intrusion detection event should describe the type of alarm (e.g., microwave-intrusion, microwave-failure, microwave-tamper) and location (e.g., perimeter sector 12) of the alarm.

8.11 Tamper indication

10 CFR 73.55(i)(3)(iv) states that the licensee's intrusion detection and assessment systems must be designed to "[e]nsure that alarm devices to include transmission lines to annunciators are tamper indicating and self-checking."

8.11.1 To meet this requirement, the perimeter intrusion detection alarm system should have tamper indication attributes.

8.11.2 Tamper indication should be a characteristic of each sensor, such as balanced magnetic switches and microwave sensors (this list is not all inclusive) and be installed at each data or electrical connection "box" (e.g., processor box, junction box, data gathering panel, control box, etc.) throughout the system.

8.11.3 At a data or electrical connection box, the tamper switch should alarm when the door to the box is opened 2.45 centimeters (1 inch).

8.11.4 In addition, self-checking should be an enabled feature of each perimeter intrusion detection sensor alarm device.

8.11.5 NUREG-1959 describes details of tamper switches and self-checking features.

8.12 Automatic indication

10 CFR 73.55(i)(3)(v) states that the licensee's intrusion detection and assessment systems be designed to "[p]rovide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply."

8.12.1 To meet this requirement, when the perimeter alarm system or a component thereof fails, an indication should be automatically given to the licensee alarm station staff.

8.12.2 In addition, if the perimeter alarm system switches to backup electrical power, an indication should be automatically given to the licensee alarm station staff.

8.12.3 These indications should consist of both an audible and visual signal, which can be heard and observed, respectively, by the licensee alarm station staff.

8.13 Timely response

10 CFR 73.55(i)(3)(vi) states that the licensee's intrusion detection and assessment systems must be designed to "[s]upport the initiation of a timely response in accordance with the security plans, licensee protective strategy, and associated implementing procedures."

8.13.1 To meet this requirement, perimeter alarm system sensor detection electronic signals should be announced in the alarm stations in adequate time for the licensee to execute the following four-step process:

1. Recognize the alarm
2. Assess the alarm
3. Initiate a response if necessary
4. As necessary, engage or neutralize the threat.

8.13.2 This four-step process should have the probability of success that supports the licensee protective strategy to meet the performance objective of 10 CFR 73.55(b).

8.13.3 The four-step process applies to each alarm received from the perimeter intrusion alarm system, which includes electronic sensor detection signals, tamper indications, failure indications, line supervision alarms, and backup power switchover.

8.13.4 The four-step process also applies to each alarm generated by the licensee's security force staff that was initiated by the licensee's staff (or the licensee's contractor staff) in response to an observation of potentially unauthorized person(s), vehicle(s), or material(s).

8.13.5 If it has been calculated that an early warning system (EWS) is necessary in order to meet the performance objective of 10 CFR 73.55(b), then that system should meet the established intrusion detection alarm system criterion.

8.13.5.1 Procedures for operability and performance testing of the EWS should be developed.

8.13.5.2 Testing of the EWS should be in accordance with the Regulatory Position 3 of this guide.

8.13.5.3 Procedures for maintenance of the EWS should be developed that include insights from the site alarm technicians.

8.13.5.4 The description of the EWS, its location, and how it will be utilized should be composed in the site security plans.

8.14 Power supply

10 CFR 73.55(i)(3)(vii) states that the licensee's intrusion detection and assessment systems must be designed to "[e]nsure intrusion detection and assessment equipment at the protected area perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power."

8.14.1 To meet this requirement, the licensee should have connected to the perimeter intrusion alarm system an uninterruptible power supply that provides immediate electrical power

when the normal source of electrical power is outside of a predetermined range (this includes both the detection and assessment capabilities of the system).

8.14.2 To accommodate normal power disturbances that last longer than the uninterruptible power supply can withstand, an electrical generator system should be in place to provide power to the electrical load when: 1) the uninterruptible power supply voltage declines below a predetermined set point, or 2) when the generator system reaches the desired and stabilized set point.

- RG 1.9 provides NRC guidance for onsite emergency AC power sources using EDGs.

- IEEE Std. 2420-2019, "IEEE Standard Criteria for Combustion Turbine-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations," provides criteria for the application and testing of combustion turbine-generator units as Class 1E standby power supplies in nuclear power generating stations. **The NRC staff has reviewed the IEEE Std. 2420-2019 and found it contains additional technical information and criteria for combustion gas turbines that licensees and applicants may find useful. However, the NRC staff does not endorse IEEE Std. 2420-2019** (Ref. 40) **in this revision of RG 5.44.**

8.14.3 If primary power is interrupted, the security system should have provisions for automatic switchover to emergency power without causing false alarms and without causing a loss of system function or data.

8.14.4 Emergency power should be capable of sustaining operation without external support for a minimum of 4 hours, or for a site-specific period of time determined according to station blackout criteria for power reactor facilities.

8.14.5 If emergency power is furnished by battery, all batteries (including stored batteries) should be maintained at full charge by automatic battery charging circuitry.

- IEEE Std. 946-2020, "IEEE Recommended Practice for the Design of DC Power Systems for Stationary Applications," provides guidance on lead-acid and nickel-cadmium storage batteries, static battery chargers, and distribution equipment. **The NRC staff has reviewed the IEEE Std. 946-2020 and found it contains additional technical information on emergency power furnished by batteries that licensees and applicants may find useful. However, the NRC staff does not endorse IEEE Std. 946-2020 in this revision of RG 5.44.**

- National Electrical Manufacturers Association (NEMA) PE5, "Utility Battery Chargers," contains guidance on battery chargers. **The NRC staff has reviewed the NEMA PE5 and found it contains additional technical information on emergency power furnished by batteries that licensees and applicants may find useful. However, the NRC staff does not endorse NEMA PE5 in this revision of RG 5.44.**

8.14.6 Emergency power design, implementation and testing should follow the guidance in Regulatory Position 1.3 of this guide, "System Electrical Specifications."

8.15 Disposition of alarm status

10 CFR 73.55(i)(4)(ii)(F) states: "Ensure that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device at a protected or vital area portal, without the knowledge and concurrence of the alarm station operator in the other alarm station."

8.15.1 To meet this requirement, the licensee should have a process implemented that ensures that when a detection alarm is activated in the perimeter intrusion alarm system, operators in the primary and secondary alarm stations both concur with the disposition of the alarm status when it is changed.

8.15.2 The process should consist of a detection point alarm disposition procedure (or similar) that the alarm station operators have been trained to follow.

8.16 Recordkeeping

10 CFR 73.55(i)(4)(ii)(H), states: "Maintain a record of all alarm annunciations, the cause of each alarm, and the disposition of each alarm."

8.16.1 To meet this requirement, the licensee should maintain a record of:

8.16.2 all perimeter intrusion alarm system annunciations,

8.16.3 the cause of those alarms, and

8.16.4 the alarm stations operators' disposition of each alarm.

8.16.5 These records should be established, maintained, and stored in the licensee's alarm communication and display system. Records of this type are recommended to be retained for 3 years.

8.17 Surveillance, observation, and monitoring

10 CFR 73.55(i)(5)(i) states: "The physical protection program must include surveillance, observation, and monitoring as needed to satisfy the design requirements of 10 CFR 73.55(b), identify indications of tampering, or otherwise implement the site protective strategy."

8.17.1 To meet this requirement, the licensee can perform surveillance, observation, and monitoring of the protected area perimeter.

8.17.2 In performing such activities, licensees will be acting as part of the perimeter intrusion alarm system.

8.17.3 All security personnel should be trained to perform surveillance, observation, and monitoring to identify unauthorized acts such as tampering, diversion, and unauthorized access.

8.17.4 In addition, all security personnel should be trained to immediately report to alarm station personnel unauthorized and potentially unauthorized acts when identified.

8.18 Unattended openings

In accordance with 10 CFR 73.55(i)(5)(iii): "Unattended openings that intersect a security boundary such as underground pathways must be protected by a physical barrier and monitored by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation."

8.18.1 In accordance with *10 CFR 73.55(i)(5)(iii),* unattended openings that are part of the protected area perimeter or other security boundary must have a means to detect and assess exploitation of the opening.

8.18.2 Either the licensee should have intrusion sensors installed that detect exploitation of the opening, or the licensee may use security personnel to monitor such openings at a periodicity that ensures detection of attempted exploitation.

8.18.3 For unattended openings (e.g., culverts or pipes) that penetrate the protected area barrier, the licensee may install a fiber optic sensor in a grating barrier that has shown to be adequate in both wet and dry environments. The installed fiber optic sensor system should be effective at detecting intrusion and attempted intrusion to an acceptable probability of detection.

8.18.4 The radiological sabotage threat applies to nuclear power reactors as described in 10 CFR 73.1(a)(1).

8.18.5 Consequently, if an adversary attack, as defined in 10 CFR 73.1(a)(1), exploits an unattended opening, it must be detected, assessed, and responded to in time to meet the general performance objective as stated in 10 CFR 73.55(b)(1).

8.19 Illumination

10 CFR 73.55(i)(6)(ii) states: "The licensee shall provide a minimum illumination level of 0.2 foot-candles, measured horizontally at ground level, in the isolation zones and appropriate exterior areas within the protected area. Alternatively, the licensee may augment the facility illumination system by means of low-light technology to meet the requirements of this section or otherwise implement the protective strategy."

8.19.1 Adequate assessment capabilities may be conducted through the use of CCTV cameras, or security personnel.

8.19.2 Guidance for lighting for assessment purposes can be found in NUREG-1959.

8.19.3 Alternatively, the licensee may use low-light (i.e., an environment that is illuminated to less than 0.2 foot-candles, measured horizontally at ground level) technology to meet this requirement that enables adequate assessment.

8.19.3.1 Adequate assessment should include the ability to ascertain whether object is an animal or a human, a threat or not a threat, if and when a small person (i.e., 35 kg (77 pounds) minimum) crouches into a ball and lies flat (i.e., minimized silhouette), in all of the darkest areas of the isolation zone.

8.19.3.2 This ability should be tested in low-moonlight nights by setting up a CCTV view with:

- dummy targets and humans,
- dummy targets (as appropriate for the site conducting the tests) (e.g., tumble weed, rabbit),
- no dummy targets or humans, and
- humans.

8.19.3.3 The setup activity should be accomplished without the alarm station viewer watching.

8.19.3.4 After the setup, the alarm station viewer should attempt, through observation, through line of sight, or camera views, to accurately define the targets, if any, given a timed 5-second interval to do so.

8.19.3.5 Procedures should be developed for these tests, and the tests themselves should be documented and kept as records. Records of this type are recommended to be retained for 3 years.

8.19.3.6 The assessment procedure of this type should be performed four times a year in order to have a test within each season.

8.19.3.7 The criteria for success should be 90 percent accurate assessment at 95 percent confidence as described in Regulatory Position 3 of this guide

8.20 Maintenance, testing, and calibration

10 CFR 73.55(n)(1)(i) states: "Establish, maintain, and implement a maintenance, testing and calibration program to ensure that security systems and equipment, including secondary and uninterruptible power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions."

8.20.1 To meet this requirement, the licensee must establish, maintain, and implement a maintenance, testing, and calibration program for the perimeter intrusion alarm system, which should include each component thereof.

8.20.2 Operability tests include simple tests such as having a person walk through a detection zone and confirming that alarm station operators received an alarm within a few seconds for the zone in which the perimeter intrusion was made.

8.20.3 Operability tests should include a test that verifies that the perimeter intrusion alarm system functions as intended when the secondary power and uninterruptible power switches on.

8.20.4 Performance tests should:

8.20.4.1 Be designed to verify the level of performance of each perimeter intrusion alarm sensor through its intended range of function.

8.20.4.2 Include verification that the system functions as intended when the secondary power (e.g., generator power kick-in after battery supply diminishes past set point or kick-in to generator power when the generator power stabilizes) switches on.

8.20.4.3 Include verification that the system functions as intended when the uninterruptible power (e.g., battery supply) switches on.

8.20.4.4 Include the use of all defeat methodologies applicable to the system.

8.20.4.5 Refer to the performance criterion for testing as described in Regulatory Position 2 of this guide.

8.20.4.6 Refer to the operability and performance testing discussion in the Regulatory Position 3 of this guide.

8.20.4.7 Refer to both performance and operability testing discussions in NUREG-1959.

8.20.5 If performance criteria are not specified in the Regulatory Position 2 of this guide for the type of sensor being tested, then performance criteria should be developed and utilized for the subject sensor.

8.21 Implementing procedures

10 CFR 73.55(n)(1)(ii) states: "Describe the maintenance, testing and calibration program in the physical security plan. Implementing procedures must specify operational and technical details required to perform maintenance, testing, and calibration activities to include, but not limited to, purpose of activity, actions to be taken, acceptance criteria, and the intervals or frequency at which the activity will be performed."

8.21.1 To meet the NRC staff's expectation for this requirement, licensees should establish a documented preventive maintenance program for the intrusion detection alarm system through the development of procedures.

8.21.2 Procedures for preventive maintenance should include periodic observations of all components of an intrusion detection system to assess potential damage from environmental conditions, inadvertent employee actions, and potential tampering.

8.21.3 Proactive servicing of all intrusion detection alarm components should be conducted in accordance with manufacturer instructions.

8.21.4 Preventive maintenance procedures should include actions informed by the intrusion alarm technician's insights on the actions necessary to keep the intrusion detection system functioning as intended.

8.21.5 Preventive maintenance procedures should include actions to remedy either more than one false alarm per zone per day or more than one nuisance alarm per zone per day.

8.21.6 Testing should be performed in accordance with Regulatory Positions 2 and 3 of this guide.

8.21.7 NUREG-1959 discusses preventive maintenance for an intrusion detection alarm system.

8.21.8 Maintain records of the results of all tests performed.

8.21.8.1.1 These records should include the segment number, date, time, and relevant environmental conditions when tests were performed.

8.21.8.1.2 Records should be maintained consistent with 10 CFR 73.70.

10 CFR 73.55(n)(1)(ii) provides that the licensee shall describe the maintenance, testing and calibration program in the physical security plan.

8.21.9 The testing and maintenance program for the intrusion detection alarm system should be broadly described in the physical security plan. For example, testing and maintenance activities that are planned to be conducted each year can be described.

8.22 Finding criteria

10 CFR 73.55(n)(1)(iii) states: "Identify in procedures the criteria for determining when problems, failures, deficiencies, and other findings are documented in the site corrective action program for resolution."

8.22.1 The criteria should apply to the following (this list is not all inclusive):

- the system as a whole,
- the uninterruptible power supply interface,
- the secondary power interface,
- each sensor,
- transmission lines,
- assessment system components (e.g., illumination systems, CCTV),
- data-gathering panels,
- the alarm station's alarm communication and display systems,
- sensors repeatedly (e.g., more than three back-to-back 30/40 test sequences) not meeting the design goal of 90 percent probability of detection with 95 percent confidence,
- recurrent problems, failures, or deficiencies in a particular perimeter sector, and
- excessive false or nuisance alarms.

8.23 Operability testing

10 CFR 73.55(n) states, in part: "(2) The licensee shall test each intrusion alarm for operability at the beginning and end of any period that it is used for security, or if the period of continuous use exceeds seven (7) days. The intrusion alarm must be tested at least once every seven (7) days. (3) Intrusion detection and access control equipment must be performance tested in accordance with the security plans and implementing procedures."

8.23.1 The program should include operability tests, which are simple tests such as having a person walk through a detection zone and confirming that alarm station operators received an alarm within a few seconds for the zone in which the perimeter intrusion was made.

8.23.2 Operability tests should include a test that verifies that the perimeter intrusion alarm system functions as intended when the secondary power and uninterruptible power switches on.

8.23.3 Refer to the operability test discussions in the Regulatory Position 3 of this guide and in NUREG-1959.

8.24 Testing after out of service periods

10 CFR 73.55(n)(8) states: "Security equipment or systems shall be tested in accordance with the site maintenance, testing and calibration procedures before being placed back in service after each repair or inoperable state."

8.24.1 To meet this requirement, each component of the licensee's perimeter intrusion alarm system should have a procedure that specifically describes the maintenance, testing, and calibration actions to be applied before the component is placed back in service after each repair or inoperable state.

8.24.2 The performance criteria for sensors described in the Regulatory Position 2 of this guide should be utilized, as appropriate.

8.25 Compensatory measures

10 CFR 73.55(o)(1) states: "The licensee shall identify criteria and measures to compensate for degraded or inoperable equipment, systems, and components to meet the requirements of this section."

8.25.1 To meet this requirement, the licensee should identify criteria and measures for compensatory measures applicable to the degraded or inoperable intrusion detection alarm system equipment, systems, and components thereof.

8.25.2 These criteria and measures should be developed and documented in procedures.

8.26 Level of protection by compensatory measures

10 CFR 73.55(o)(2) states: "Compensatory measures must provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system, or components."

8.26.1 To meet this requirement, when compensatory measures are implemented, the licensee should provide an equivalent or greater level of protection that was established by the perimeter intrusion detection alarm system, equipment, or components.

8.26.2 For example, the design goal of the implemented compensatory measure for a perimeter intrusion detection sensor system should be a 90 percent probability of perimeter intrusion detection with 95 percent confidence.

9 INTRUSION DETECTION ALARM SYSTEM FOR THE PROTECTION OF CATEGORY II AND CATEGORY III SPECIAL NUCLEAR MATERIAL REQUIRED BY 10 CFR 73.67

For Category II and III licensees, the requirements under 10 CFR 73.67, "Licensee fixed site and in-transit requirements for the physical protection of special nuclear material of moderate and low strategic significance," provide, in part:

(a) General performance objectives.

(1) Each licensee who possesses, uses, or transports special nuclear material of moderate or low strategic significance shall establish and maintain a physical protection system that will achieve the following objectives:

(i) Minimize the possibilities for unauthorized removal of special nuclear material consistent with the potential consequences of such actions; and

(ii) Facilitate the location and recovery of missing special nuclear material.

(2) To achieve these objectives, the physical protection system shall provide:

(i) Early detection and assessment of unauthorized access or activities by an external adversary within the controlled access area containing special nuclear material; and

(ii) Early detection of removal of special nuclear material by an external adversary from a controlled access area.

For Category II licensees, the requirement under 10 CFR 73.67(d)(3) states: "Monitor with an intrusion alarm or other device or procedures the controlled access areas to detect unauthorized penetration or activities."

For Category III licensees, the requirement under 10 CFR 73.67(f)(2) states, "Monitor with an intrusion alarm or other device or procedures the controlled access areas to detect unauthorized penetrations or activities."

9.1 An acceptable means to meet both early detection and monitoring requirements for Category II and Category III special nuclear material are described in RG 5.59.

10. GUIDANCE TO SUPPORT NRC ORDER EA 02-025, COMPENSATORY MEASURES TO ADDRESS THE HIGH-LEVEL THREAT ENVIRONMENT (REFERENCE SAND2007-5591)

10.1 Testing of the Perimeter Intrusion Alarm System

10.1.1. Tests of the perimeter intrusion alarm system should be performed and documented.

10.1.2. Tests should be conducted by following developed procedures.

10.2 Operability Tests

10.2.1 Operability testing should be performed at the beginning of each interval (e.g., shift change) but not less frequently that every 7 days.

10.2.2 Operability tests should include having an individual pass through the zone of detection of an intrusion detection sensor and verifying that an alarm is generated.

10.2.3 Operability tests are discussed in NUREG 1959.

10.3 Performance Tests

10.3.1 Performance tests should be conducted at least semi-annually.

10.3.2 Performance testing procedures which mathematically test for the probability of detection design goal of 90 percent probability of detection with a 95 percent confidence level are described in Regulatory Position 3, "Recommended Testing Procedures."

10.4 Maintenance

10.4.1 The conduct of maintenance on the perimeter intrusion detection system should follow developed procedures.

10.4.2 Maintenance should be conducted in accordance with manufacturers' specifications.

10.4.3 Maintenance procedures should include insights from alarm technicians who have serviced the perimeter intrusion alarm system.

10.5 Compensatory Measures

10.5.1 If the perimeter intrusion detection system has become deficient, compensatory measures should be implemented as soon as possible.

10.5.2 Compensatory measures should be equal to or greater than in detection capability of the perimeter intrusion alarm system when it was functioning as intended.

10.6 Physical Protection System Probability of Effectiveness

10.6.1 Perimeter intrusion alarm detection subsystem capabilities (i.e., sensing and assessment) should be verified, with response capabilities, to ensure that an adversary passing into or through the perimeter is adequately engaged by response forces.

10.6.2 Response actions associated with detection of a potential adversary incursion into the perimeter should be adequate to provide a satisfactory probability of physical protection system effectiveness (Reference SAND2007-5591).

D. IMPLEMENTATION

The NRC staff may use this RG as a reference in its regulatory processes, such as licensing, inspection, or enforcement. However, the NRC staff does not intend to use the guidance in this RG to support NRC staff actions in a manner that would constitute backfitting as that term is defined in 10 CFR 50.109, "Backfitting," 10 CFR 70.76, "Backfitting," and 10 CFR 72.62, "Backfitting," and as described in NRC Management Directive 8.4, "Management of Backfitting, Forward Fitting, Issue Finality, and Information Requests" (Ref. 41), nor does the NRC staff intend to use the guidance to affect the issue finality of an approval under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

The staff also does not intend to use the guidance to support NRC staff actions in a manner that constitutes forward fitting as that term is defined and described in Management Directive 8.4. If a licensee believes that the NRC is using this RG in a manner inconsistent with the discussion in this Implementation section, then the licensee may file a backfitting or forward fitting appeal with the NRC in accordance with the process in Management Directive 8.4.

APPENDIX A
CHECKLIST

This appendix contains checklists for each type of detection system described in this guide. 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 or ground with a constant slope to prevent shadowing (inadequate detection in depressions).
- For comer overlap applications, keep intersection angles of microwave beams as close as possible to 90 degrees, i.e., orthogonal.
- Never mount on the same post two microwave receivers for different segments or zones (or on the same channel).
- Remember that dynamic multipath signals from 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, traffic, or surface discontinuities may cause nuisance alarms. However, reflection of microwave signals may sometimes be used effectively to extend coverage where terrain or structures are not amenable to standard installation.
- Be aware that microwave sensor detection zones that parallel a road with vehicular traffic or long fence lines may 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. Crowned surface grades and gravel beds can reduce or eliminate standing water.
- Note that, after a heavy rain, moving water under the microwave detection zone may produce nuisance alarms.

- 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 5.6 cm (2.2 inches) per hour is likely to cause microwave sensors to produce nuisance alarms.

- Consider that electro-magnetic interference (EMI), either reflected or direct, can strike the microwave receiver and cause nuisance alarms. Shielded radomes or enclosures with shielded wiring and proper grounding can reduce or eliminate the effects of EMI. Refer to RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," for guidance.

- 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 comers 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 should 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.
- Note that the detection zone may be elongated at curves.
- Note that the sensor may react to strong sources of radio frequency energy.
- 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 cannot 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- detection systems.

Vibration – or Strain – Detection Systems

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

- Fence fabric should 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.

- If not encapsulated in conduit, system wiring should be interwoven in the fence fabric, rather than simply clipped to it, to prevent removal as a means of defeating the system.

GLOSSARY

Access mode	A 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	A type used with a microwave sensor, a sensor consisting of a transmitter and receiver remote from each end of a microwave link.
Bridging	Circumvention of a perimeter detection system by traversing above the zone of detection using hand-carried aids or nearby objects.
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.
Early Warning System (EWS):	An intrusion detection alarm system that is implemented outside of the protected area to ensure adequate responder timelines or to potentially enhance responder timelines, due to potential unauthorized access to the owner-controlled 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 no more than one per zone per day.
Formula quantity of special nuclear material	In accordance with 10 CFR 73.2, “Definitions,” formula quantities of special nuclear material = Category I quantities of special nuclear material.
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. (Note: For facilities required to have double protected area barriers, this zone should extend 6.1 meters (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 6.1 meters (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 sightsystem	As used with intrusion detection systems, a sensor that requires a terrain surface that is relatively flat, with no significant contour depressions or elevations.
Monostaticsystem	As used with a microwave sensor, a sensor that has the receiver and transmitter located in the same head or unit.
Multi-mode 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 no more than 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. Operability testing and operational testing are synonymous in this context.
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 trans- mission 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	A 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 multi-mode fiber that is being illuminated by a laser source.
Terrain-following	As used with intrusion detection systems, a sensor with a detection pattern that can adapt tosystem some changes in the terrain's contour.
Tunneling	To make a tunnel through or under; to make (one’s way or a way) by digging a tunnel. (Ref: Webster’s)
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).

BIBLIOGRAPHY

Underwriters Laboratory “UL 2050," National Industrial Security Systems,” issued November 5, 2010. It can be found at: https://www.ul.com.

US Department of Energy (DOE), Order 473.1A, "Physical Protection Program," issued August 31, 2021. It can be found at https://www.directives.doe.gov/news/new-doe-o-473-1a-physical-protection-program.

US DOE, Sandia National Laboratories, SAND2021-7077, “Security System Design Reference, Alarm Communication and Display and Security Communications,” June 2021, (contains Unclassified Controlled Nuclear Information and Official Use Only Information).

US DOE, Sandia National Laboratories, SAND2021-0543, “Security System Design Reference, Intrusion Detection and Video Assessment,” January 2021, (contains Unclassified Controlled Nuclear Information and Official Use Only Information).

US DOE, Sandia National Laboratories, SAND2021-13518, “Security System Design Reference, Entry Control & Contraband Detection, June 2021. (contains Unclassified Controlled Nuclear Information and Official Use Only Information).

US DOE, Sandia National Laboratories, SAND2021-15454, “Security System Design Reference, Interim Access Delay Manual, June 2021. (contains Unclassified Controlled Nuclear Information and Official Use Only Information).

REFERENCES [4]

1 U.S. Code of Federal Regulations (CFR), "Physical Protection of Plants and Materials," Part 73, Chapter 1, Title 10, "Energy."

2 CFR, "Standards for Protection Against Radiation," Part 20, Chapter 1, Title 10, "Energy."

3 CFR, "Domestic Licensing of Source Material," Part 40, Chapter 1, Title 10, "Energy."

4 CFR, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter 1, Title 10, "Energy."

5 CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter 1, Title 10, "Energy."

6 CFR, "Domestic Licensing of Special Nuclear Material," Part 70, Chapter 1, Title 10, "Energy."

7 CFR, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High Level Radioactive Waste, and Reactor-Related Greater than Class C Waste," Part 72, Chapter 1, Title 10, "Energy.

8 U.S. NRC, Security Order, EA 02-025, "Order for Compensatory Safeguards Measures," issued March 25, 2002, Washington, DC. (ML020840303).

4 Publicly available NRC published documents are available electronically through the NRC Library on the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html The documents can also be viewed online or printed for a fee in the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov.

Copies of the non-NRC documents included in these references may be obtained from the publishing organization.

Copies of IEEE documents may be obtained from the Institute of Electrical and Electronics Engineers, Inc., IEEE Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855.

Copies of American National Standards Institute (ANSI) standards may be purchased from ANSI, 1819 L Street, NW. Washington, DC 20036, on its Web site at http://webstore.ansi.org/; telephone (202) 293-8020; fax (202) 293-9287; or e-mail storemanager@ansi.org.

Copies of International Atomic Energy Agency (IAEA) documents may be obtained through its Web site at WWW.IAEA.Org/ or by writing the International Atomic Energy Agency, P.O. Box 100, Wagramer Strasse 5, A-1400 Vienna, Austria; telephone (+431) 2600-0; fax (+431) 2600-7; or e-mail at official.mail@IAEA.org.

Copies of Underwriter's Laboratory documents may be obtained from UL, 151 Eastern Avenue, Bensenville, IL 60106; Telephone: Toll-free: 1-888-UL33512 or 1-888-853-3512. Purchase information is available through the UL Website at http://ulstandards.ul.com/access-standards/Or http://www.comm-2000.com/Catalog.aspx

Copies of Garcia-SNL literature may be obtained from, Manager of Special Sales, Elsevier Science, 200 Wheeler Road, 6th Floor Burlington, MA 01803.

Copies of International Association of Automation (ISA) documents may be obtained through its Web site at www.ISA.org/products

Copies of NIST documents may be obtained through its Web site at www.NIST.gov/publications

9 U.S. NRC, NUREG-1959, “Intrusion Detection Systems and Subsystems: Technical Information for NRC Licensees,” Washington, DC.

10 U.S. NRC, Regulatory Guide (RG) 1.128, “Installation Design and Installation of Vented Lead-Acid Storage Batteries for Nuclear Power Plants,” Washington, DC.

11 U.S. NRC, RG 1.129, “Maintenance, Testing, and Replacement of Vented Lead-Acid Storage Batteries for Nuclear Power Plants,” Washington, DC.

12 U.S. NRC, RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Washington, DC.

13 U.S. NRC, RG 1.9, “Application and Testing of Safety-Related Diesel Generators in Nuclear Power Plants,” provides guidance for onsite emergency alternating current (AC) power sources using emergency diesel generators (EDGs),” Washington, DC.

14 U.S. NRC, RG 5.59, “Standard Format and Content for a Licensee Physical Security Plan for the Protection of Special Nuclear Material of Moderate or Low Strategic Significance,” Washington, DC.

15 U.S. NRC, RG 5.69, “Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements,” Washington, DC. (not publicly available)

16 U.S. NRC, RG 5.70, “Guidance for the Application of the Theft and Diversion Design-Basis Treat in the Design Development, and Implementation of a Physical Security Program that Meets CFR 73.45 and 73.46,” Washington, DC. (not publicly available)

17 Garcia, M.L., “The Design and Evaluation of Physical Protection Systems” (1st ed.), Butterworth Heinemann, 2001.

18 Institute of Electrical and Electronics Engineers (IEEE) Std. 1682-2011, “IEEE Standard for Qualifying Fiber Optic Cables, Connections, and Optical Fiber Splices for Use in Safety Systems in Nuclear Power Generating Stations,” Piscataway, NJ.

19 IEEE Std. 1428-2004, “IEEE Guide for Installation Methods for Fiber Optic Cables in Electric Power Generating Stations and in Industrial Facilities,” Piscataway, NJ.

20 American National Standards Institute (ANSI) (/International Association of Automation (ISA), ANSI/ISA-18.2, “Management of Alarm Systems for the Process Industries,” Research Triangle Park, NC.

21 National Institute of Standards and Technology (NIST), SP 880-53, “Security and Privacy Controls for Information Systems and Organizations,” Gaithersburg, MD.

22 U.S. NRC, “Nuclear Regulatory Commission International Policy Statement,” Federal Register, Vol. 79, No. 132, July 10, 2014, pp. 39415-39418.

23 U.S. NRC, Management Directive 6.6, “Regulatory Guides,” Washington, DC.

24 International Atomic Energy Agency (IAEA), Nuclear Security Series No. 13, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities,” INFCIRC/225, Vienna, Austria.

25 IEEE Std.946-2020, “IEEE Recommended Practice for the Design of DC Power Systems for Stationary Applications,” Piscataway, NJ.

26 IEEE Std. 1106-2015 “Recommended Practice for Installation, Maintenance, Testing, and Replacement of Vented Nickel-Cadmium Batteries for Stationary Applications” Piscataway, NJ.

27 IEEE Std. 1187-2013, “Recommended Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Batteries for Stationary Applications,” Piscataway, NJ.

28 IEEE Std. 1188-2005, “Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications," Piscataway, NJ.

29 IEEE Std. 2420-2019, “Standard Criteria for Combustion Turbine-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations,” Piscataway, NJ.

30 National Electrical Manufacturers Association (NEMA) PE5, “Utility Battery Chargers.”

31 Underwriter Laboratories (UL) Standard 1076, “Standard for Proprietary Burglar Alarm Units and Systems.”

32 UL Standard 1610, “Standard for Central-Station Burglar-Alarm Units.”

33 UL Standard 1635, “Standard for Digital Alarm Communicator System Units.”

34 NIST, Federal Information Processing Standards (FIPS) 197, “Advanced Encryption Standard (AES),” available at https://csrc.nist.gov/publications/detail/fips/197/final.

35 U.S. Department of Energy, “Nuclear power plant security assessment technical manual,” Sandia Report, SAND 2007-5591, 2007.

36 IEEE Std. 142-1991, “IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems,” Piscataway, NJ.

37 IEEE Std. C2-2023, “2023 National Electrical Safety Code(R) (NESC(R),” https://standards.ieee.org/ieee/C2/10814/.

38 UL Standard 634, “Standard for Connectors and Switches for Use with Burglar-Alarm Systems.”

39 U.S. Department of Justice, Green, M.W., “The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies,” 1999, https://www.ncjrs.gov/school/178265.pdf.

40 IEEE Std. 2420-2019, "IEEE Standard Criteria for Combustion Turbine-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations," Piscataway, NJ.

41 U.S. NRC, "Management of Facility-Specific Backfitting and Information Collection," Management Directive 8.4, Washington, DC.