



U.S. NUCLEAR REGULATORY COMMISSION

REGULATORY GUIDE

OFFICE OF STANDARDS DEVELOPMENT

REGULATORY GUIDE 5.44
(Task SG 479-4)

PERIMETER INTRUSION ALARM SYSTEMS

A. INTRODUCTION

* Part 73, "Physical Protection of Plants and Materials," of Title 10, Code of Federal Regulations, specifies performance requirements for the physical protection of special nuclear materials and associated facilities. Section 73.20 describes the general performance objective and requirements that must be met through the establishment of a physical protection system. Performance capabilities necessary to meet the requirements of § 73.20 are described in § 73.45. Paragraph 73.45(c) requires that only authorized activities and conditions be permitted within protected areas, material access areas, and vital areas through the use of detection and surveillance subsystems and procedures to detect, assess, and communicate any unauthorized access or penetrations or such attempts by persons, vehicles, or materials. Furthermore, § 73.46 outlines typical specific safeguards measures that will often be included in an overall system that meets the requirements of §§ 73.20 and 73.45. The use of an intrusion alarm subsystem with the capability to detect penetration through the isolation zone is specifically called out in paragraph 73.46(e)(1). For power reactors, paragraph 73.55(c)(4) requires that detection of penetration or attempted penetration of the protected area or the isolation zone adjacent to the protected area barrier ensure that adequate response by the security organization can be initiated.

This guide describes six types of perimeter intrusion alarm systems and sets forth criteria for their performance and use as a means acceptable to the NRC staff for meeting specified portions of the Commission's regulations. It also references a document (SAND 76-0554) that provides additional information in this area, especially on the subject of combining sensors to yield a better overall performance.

* Lines indicate substantive changes from Revision 1.

B. DISCUSSION

Perimeter intrusion alarm systems can be used to detect intrusion into or through the isolation zone at the perimeter of the protected area. A system generally consists of one or more sensors, electronic processing equipment, a power supply, signal lines, and an alarm monitor. Detection of an intruder is accomplished by the alarm system responding to some change in its operating condition caused by the intruder, e.g., interruption of a transmitted infrared or microwave beam or stress exerted on a piezoelectric crystal. The choice of a perimeter alarm system is influenced by considerations of terrain and climate. At present, no single perimeter intrusion alarm system is capable of operating effectively in all varieties of environment.

The mode of installation of the perimeter alarm system influences its effectiveness. In general, dividing the site perimeter into segments that are independently alarmed and uniquely monitored assists the security organization responding to an alarm by localizing the area in which the alarm initiated. Segmenting of the perimeter alarm system also allows testing and maintenance of a portion of the system while maintaining the remainder of the perimeter under monitoring. It is generally desirable that the individual segments be limited to a length that allows observation of the entire segment by an individual standing at one end of the segment.

Effective use of a perimeter intrusion alarm system is facilitated by a regular program of system testing. Operability testing can be performed by a guard or watchman penetrating the segment protected by the alarm system during routine patrols. Performance testing, i.e., manufacturer's specification testing and detection probability testing, however, is usually more elaborate. In any case, testing can be conducted without compromising security only if performed under controlled circumstances such as direct visual observation or by closed-circuit television of the area being tested while a specified test is conducted.

USNRC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the NRC staff of implementing specific parts of the Commission's regulations, to delineate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

Comments and suggestions for improvements in these guides are encouraged at all times, and guides will be revised, as appropriate, to accommodate comments and to reflect new information or experience. This guide was revised as a result of substantive comments received from the public and additional staff review.

Comments should be sent to the Secretary of the Commission, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, Attention: Docketing and Service Branch.

The guides are issued in the following ten broad divisions:

- | | |
|-----------------------------------|-----------------------------------|
| 1. Power Reactors | 6. Products |
| 2. Research and Test Reactors | 7. Transportation |
| 3. Fuels and Materials Facilities | 8. Occupational Health |
| 4. Environmental and Siting | 9. Antitrust and Financial Review |
| 5. Materials and Plant Protection | 10. General |

Copies of issued guides may be purchased at the current Government Printing Office price. A subscription service for future guides in specific divisions is available through the Government Printing Office. Information on the subscription service and current GPO prices may be obtained by writing the U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, Attention: Publications Sales Manager.

To ensure secure operation, the system may periodically monitor the sensor transducer and signal processing circuits. This self-checking feature can vary depending on the type and design of the alarm system. Many systems require self-excitation of the sensor transducer (e.g., vibration, strain, pressure) while others monitor the signal level at the receiving transducer (e.g., microwave, infrared). However, several worthwhile commercially available perimeter alarm systems provide little or no self-checking circuitry. To ensure normal operation for those alarm systems that do not incorporate self-checking circuitry, the licensee should institute a test program that will periodically test each segment of a perimeter alarm system to verify that it maintains the proper sensitivity to detection.

In order to increase the probability of detection and lower the false alarm rates, a combination of sensors may be desirable in certain environments. Additional factors to be considered in the selection and application of single sensors or a combination of sensors are presented in a Sandia Laboratories report prepared for the Department of Energy entitled "Intrusion Detection Systems Handbook" (IDSH), SAND 76-0554, and in particular Sections 8.3 and 3.2. Additional information in this area, i.e., integrated perimeter systems, is scheduled for development by the NRC. An important element of an intrusion detection system is the assessment capability associated with the perimeter intrusion alarm system. Alternative assessment capabilities such as video assessment, hardened observation posts, and armored response vehicles are discussed in Regulatory Guide 5.61, "Intent and Scope of the Physical Protection Upgrade Rule Requirements for Fixed Sites," in the discussion of paragraph 73.46(h)(6). System design considerations for video assessment systems are discussed in Section 6.3 of the IDSH.

The following discussion describes the operations, limitations, and environmental considerations of six basic types of commercially available perimeter alarm systems: microwave, E-field, ferrous metal detector, pressure-sensitive, infrared, and vibration- or stress-fence protection systems.

1. Microwave Perimeter Alarm System

Each link of a microwave perimeter alarm system is composed of a transmitter, receiver, power supply, signal processing unit, signal transmission system, and annunciator. The microwave transmitter produces a beam-like pattern of microwave energy directed to the receiver, which senses the microwave beam. A partial or total interruption of the beam will cause an alarm. The microwave beam can be modulated to reduce interference from spurious sources of radiofrequency energy, to increase sensitivity, and to decrease the vulnerability to defeat from "capture" of the receiver by a false microwave source.

Successive microwave links can be overlapped to form a protective perimeter around a facility. Since the transmitter/receiver link is a line-of-sight system, hills or other obstructions will interrupt the beam, and ditches or valleys may provide crawl space for an intruder. Moreover, objects such as tumbleweed, paper, and bushes moving in the path of the

beam can cause nuisance alarms. Since the beam is wider than other systems, care must be taken to ensure that authorized activities do not create nuisance alarms. Systems using the Doppler shift for motion detection are especially sensitive to the motion of trees and grass and to falling rain and snow.

The maximum and minimum separation of the transmitter and receiver is usually specified by the manufacturer. Typically, a microwave perimeter alarm system will operate effectively in the range between 70 and 150 meters.

2. E-Field Perimeter Alarm System

An E-field perimeter alarm system consists basically of a field generator that excites a field wire, one or more sensing wires, and a sensing filter; an amplifier; and a discriminatory and annunciator unit. The field wire transmits essentially an omnidirectional E-field to ground. A large body approaching the system changes the pattern of the E-field. When sensing wires are placed at different locations within the transmitted E-field pattern, they pick up any changes occurring in that pattern. If the changes are within the frequency bandpass of human movement, an alarm signal is generated. The field wire and one or more parallel sensing wires can be either connected to a chain link fence or mounted as an above-ground, freestanding system of an isolation zone.

The E-field system can offer about 300 meters of perimeter protection per segment, but shorter lengths of 100 meters are recommended in order to have effective alarm assessment and response capabilities. The system can be mounted on metal, plastic, or wooden posts using specially designed electrical isolators that allow for small movements of the posts without disturbing the field and sensing wires. Both the field and sensing wires need to be under a high degree of spring tension to produce high-frequency vibrations when they are struck by small foreign objects or blown by the wind, both of which are out of the passband of the receiving circuitry. In addition, in order to keep the sensitivity of the system from varying, the E-field detector needs to be well grounded.

The E-field detector is not a line-of-sight system and therefore can be installed on uneven terrain and in an irregular line. The surrounding terrain should be kept clear of shrubs, tree limbs, and undergrowth since they act as moving ground objects. The basic system is a two-wire system with the sensing wire located between 200 and 450 millimeters above the ground and the field wire located approximately 1 meter above and parallel to the sensing wire. The width of the detection zone is variable and depends to a large degree on the size of the target. Generally, it is approximately 0.6 meter wide on either side of the field wire. To prevent an intruder from jumping over the top of the E-field detector, a second sensing wire can be installed approximately 1 meter above the field wire. When installed on a chain link fence, standoffs approximately 0.5 meter long are used for mounting the wires. The E-field generated in this configuration does not penetrate the fence but parallels it.

3. Ferrous Metal Detector Perimeter Alarm System

A ferrous metal detector system consists of buried electrical cables, amplifiers, inhibitors, power supply, signal processing unit, signal transmission lines, and annunciator. The system is passive and is susceptible to changes in the earth's ambient magnetic field. Such changes are caused either by electromagnetic disturbances such as lightning or by ferrous metal being carried over the buried cables. The change in the local ambient magnetic field induces a current in the buried cable which is filtered and sensed by the electronics. If the change exceeds a predetermined threshold, an alarm is generated. To reduce nuisance alarms from external electromagnetic sources (e.g., electrical power transmission lines), the electrical cable is laid in loops that are transposed at regular intervals. Also, an inhibitor loop can be used to reduce nuisance alarms from electromagnetic interference. The inhibitor, which operates on the same principle as the sensor cable loops and is buried near the sensor cable, senses strong temporary electromagnetic interferences (e.g., lightning) and disables the alarm system for approximately one second, thus reducing nuisance alarms.

The ferrous metal detector system is not a line-of-sight system and therefore can be installed on uneven ground in an irregular line. The sensor subloops formed by the cables must be fairly regular, however. Since the system will detect only ferrous metal, animals, birds, or flying leaves will not initiate alarms. However, electromagnetic interferences can cause nuisance alarms or disable the alarm system when the interference is severe.

Each sensing cable (and amplifier) can monitor a security segment up to 500 meters in length. Increasing the length of the security segment beyond 500 meters usually results in a high nuisance alarm rate. Multiple cables and amplifiers can be used to extend the monitoring length.

4. Pressure/Strain-Sensitive Perimeter Alarm System

Buried pressure/strain transducers detect small variations in the mechanical stress exerted on the surrounding soil by the presence of an individual passing above the sensor. The signals produced by the transducers are amplified and compared with a preestablished threshold. If the signal exceeds the threshold, an alarm occurs. The transducer may be a set of piezoelectric crystals, a fluid-filled flexible tube, a specially fabricated stress/strain electrical cable, or an insulated wire in a metallic tube.

Like the ferrous metal detector system, the pressure-sensitive system does not require line-of-sight installation and can be sited on uneven terrain. However, soil condition and composition have a significant effect on sensor sensitivity. Installation in rocky soil may result in damage to the pressure transducers either during installation or as a result of soil settlement after installation. Wind-generated movement in trees and poles can create nuisance alarms. High winds can produce pressure waves on the ground surface which, if sensed by the transducer, could necessitate operation at reduced sensitivity in order to avoid nuisance

alarms. Features to compensate for wind-generated noise can be designed into the equipment but in turn may cause a decrease in system sensitivity. Pressure systems will lose sensitivity when the buried sensors are covered by snow, by snow with a frozen crust that will support the weight of a man, or by frozen ground. Other natural phenomena such as hail and rain can cause nuisance alarms.

The sensitive area consists of a narrow corridor, usually about 1 meter in width. A greater degree of security can be achieved by employing two such corridors to prevent an intruder from jumping over the buried transducers. A typical length monitored by a transducer (i.e., set of piezoelectric crystals, a liquid-filled tube, or an electrical cable) is about 100 meters.

5. Infrared Perimeter Alarm System

Like the microwave system, each link of an infrared system is composed of a transmitter, receiver, power supply, signal processor, signal lines, and alarm annunciator. The transmitter directs a narrow infrared beam to a receiver. If the infrared beam between the transmitter and receiver is interrupted, an alarm signal is generated. As with the microwave system, the infrared system is a line-of-sight system. In addition, the infrared beam is usually modulated. Since the infrared beam does not diverge significantly as does the microwave beam, multiple infrared beams between transmitter and receiver can be used to define a "wall." If this "wall" is then penetrated by an individual, an alarm will result.

Fog both attenuates and disperses the infrared beam and can cause nuisance alarms. However, the system can be designed to operate properly with severe atmospheric attenuation. Dust on the faceplates will also attenuate the infrared beam as will an accumulation of condensation, frost, or ice on the faceplates.

Such condensation, frost, or ice, however, may be eliminated through the use of heated faceplates. Sunshine on the receiver may cause an alarm signal. Misalignment of transmitter and receiver caused by frost heaves may also cause an alarm signal. Like the microwave system, vegetation such as bushes, trees, or grass and accumulated snow will interfere with the infrared beam, and ditches, gullies, or hills will allow areas where the passage of an intruder may go undetected.

The typical distance between transmitter and receiver is about 100 meters; some systems are capable of monitoring a distance up to 300 meters under ideal conditions.

6. Vibration- or Strain-Detector Perimeter Alarm System

A variety of devices that detect strain or vibration are available for use as fence protection systems. Although the devices vary greatly in design, each basically detects strain or vibration of the fence 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. Vibration- or

strain-detection devices for fence protection generally are susceptible to nuisance alarms caused by wind vibrating the fence or by hail stones or large pieces of trash blowing against the fence. The frequency of nuisance alarms due to the wind can be reduced by rigidly mounting the fence and thereby lessening the propensity of the fence to vibrate in the wind. This situation is especially common with post-mounted switch-contact-type alarm systems. The use of electronic signal processing equipment in conjunction with signal-generating strain transducers can effectively reduce nuisance alarm rates without sacrificing sensitivity to climbing or cutting the fence. However, most fence alarm systems can be easily bypassed by a variety of methods.

Depending on the variety of sensor, each sensor can monitor a length of fence ranging from about 1 meter to several hundred meters.

C. REGULATORY POSITION

1. Minimum Qualification for Perimeter Intrusion Alarm Systems

a. General

(1) *Electrical.* All components—sensors, electronic processing equipment, power supplies, alarm monitors—should be capable of meeting the typical design requirements for fire safety of nationally recognized testing laboratories such as Underwriters Laboratory (UL) or Factory Mutual (FM). The system should contain provisions for automatic switchover to emergency battery and generator or emergency battery power without causing an intrusion system alarm in the event primary power is interrupted. Emergency power should be capable of sustaining operation for a minimum of 24 hours without replacing or recharging batteries or refueling generators. If sufficient battery or fuel capacity is not attainable for 24-hour operation as stated above, additional batteries or fuel should be stored on site expressly for augmenting the emergency power supply. If emergency power is furnished by battery, all batteries (including stored batteries) should be maintained at full charge by automatic battery-charging circuitry. Batteries should be checked in accordance with IEEE Standard 450-1975 as endorsed by Regulatory Guide 1.129, "Maintenance Testing and Replacement of Large Lead Storage Batteries for Nuclear Power Plants," and IEEE Standard 308-1974 as endorsed by Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants."

(2) *Tamper Indication.* All enclosures for equipment should be equipped with tamper switches or triggering mechanisms compatible with the alarm systems. The electronics should be designed so that tamper-indicating devices remain in operation even though the system itself may be placed in the access mode.¹

¹ Access mode means the condition that maintains security over the signal lines between the detector and annunciator and over the tamper switch in the detector but allows access into the protected area without generating an alarm.

All controls that affect the sensitivity of the alarm system should be located within a tamper-resistant enclosure. All signal lines connecting alarm relays with alarm monitors should be supervised; if the processing electronics is separated from the sensor elements and not located within the detection area of the sensor elements, the signal lines linking the sensors to the processing electronics should also be supervised.²

All key locks or key-operated switches used to protect equipment and controls should have UL-listed locking cylinders (see Regulatory Guide 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials").

(3) *Environment.* Perimeter intrusion alarm systems should be capable of operating throughout the climatic extreme of the environs in which they are used; as a minimum, the outdoor systems should be capable of effective operation between -35°C and +50°C. Components that necessarily must be located out of doors should be protected from moisture damage by such methods as hermetic sealing, potting in an epoxy compound, conformal coating, or watertight enclosures.

(4) *Alarm Conditions.* Perimeter intrusion alarm systems, whether using single or complementary sensors, should generate an alarm or indication under any of the following conditions:

(a) Detection of stimulus or a condition for which the system was designed to react,

(b) Indication of a switchover to the emergency or secondary source(s) of power and also upon loss of emergency power,

(c) Indication of tampering (e.g., opening, shorting, or grounding of the sensor circuitry) which renders the device incapable of normal operation,

(d) Indication of tampering by activation of a tamper switch or other triggering mechanism,

(e) Failure of any component(s) to the extent that the device is rendered incapable of normal operation. Self-checking circuitry is normally used for detecting components that have failed in a device.

Under normal environmental conditions, including seasonal extremes, the total perimeter alarm system should not average more than one false alarm per week per segment and should not average more than one nuisance alarm per week per segment while maintaining proper detection sensitivity. Where the segment can be fully observed at all times, either visually or by closed circuit television, the false alarm rate and nuisance alarm rate may be increased to one alarm per day per segment. *False alarms* are defined as those alarms that have been generated without any apparent cause. *Nuisance alarms* are alarms generated by an identified input to a sensor or monitoring device that does not

² Signal line supervision is discussed in NUREG-0320, "Interior Intrusion Alarm Systems," issued in February 1978.

represent a safeguards threat. *Proper detection probability* is defined as the ability to detect an intruder with at least 90% probability for each segment of the isolation zone under the conditions stated in the Performance Criteria of each type of alarm system.

An automatic and distinctly recognizable indication should be generated by the alarm monitor upon switchover to emergency power. Loss or reduction of power (either primary or emergency) to the degree that the system is no longer operating properly should also be indicated in the central alarm station.

Placement of any portion of a perimeter intrusion alarm system into the access mode should be indicated automatically and distinctly by the alarm monitor. Moreover, the segment(s) of the system placed in the access mode should be indicated clearly.

(5) *Installation.* It is recommended that perimeter intrusion alarm systems be located inside the perimeter physical barrier at a distance that prohibits use of the barrier to illicitly traverse the alarm zone. If, however, installation is outside the perimeter barrier, a second barrier or a fence (e.g., a cattle or snow fence) should be erected so that the alarm system is located between the barriers. The second barrier or fence will serve to reduce the incidence of nuisance alarms from animals and passersby. The separation between the second barrier and the perimeter barrier should be sufficient to preclude bridging of the perimeter alarm system; in all cases, it should not be less than 6 meters. Fence protection systems should be located on an inner fence.

Where possible, the perimeter should be segmented so that an individual standing at one end of a segment will have a clear view of the entire segment. In no case should any segment exceed 200 meters in length. Each segment should independently and uniquely indicate intrusion and should be capable of placement into the access mode independently of the other segments.

b. Microwave Perimeter Alarm System

(1) *Performance Criteria.* A microwave perimeter alarm system should be capable of detecting an intruder weighing a minimum of 35 kilograms passing between the transmitter and receiver at a rate between 0.15 and 5 meters per second, whether walking, running, jumping, crawling, or rolling. The beam should be modulated, and the receiver should be frequency selective to decrease susceptibility to receiver "capture." Generally, because of susceptibility to motion beyond the area to be protected, monostatic Doppler microwave systems should not be used as perimeter intrusion alarms.

(2) *Installation Criteria.* The transmitters and receivers should be installed on even terrain clear of trees, tall grass, and bushes. Each unit should be mounted rigidly at a distance of about 1 meter above the ground. Because of variances in the antenna pattern of different microwave systems, this height may have to be varied slightly in order

to obtain proper ground coverage. The distance between a transmitter and its receiver should be in accordance with the manufacturer's specifications and site-specific requirements. Neither the transmitter nor the receiver should be mounted on a fence. To prevent passage under the microwave beam in the shadow of an obstruction, hills should be leveled, ditches filled, and obstructions removed so that the area between transmitter and receiver is clear of obstructions and free of rises or depressions of a height or depth greater than 15 cm. The clear area should be sufficiently wide to preclude generation of alarms by objects moving near the microwave link (e.g., personnel walking or vehicular traffic). Approximate dimensions of the microwave pattern should be provided by the manufacturer.

If the microwave link is installed inside and roughly parallel to a perimeter fence or wall, the transmitter and receiver should be positioned so as to prevent someone from avoiding detection by jumping over the microwave beam into the protected area from atop the fence or wall. Typically, a chain link security fence with an overall height of 2.4 meters will necessitate a minimum of 2 meters between the fence and the center of the microwave beam.

Successive microwave links and corners should overlap at least 3 meters to eliminate the dead spot (areas where movement is not detected) below and immediately in front of transmitters and receivers. The overlap of successive links should be arranged so that receiver units are within the area protected by the microwave beam.

c. E-Field Perimeter Alarm System

(1) *Performance Criteria.* An E-field perimeter alarm system should be able to detect an individual weighing a minimum of 35 kilograms at least 0.5 meter from the sensing wire whether crawling and rolling under the lower sensing wire, stepping and jumping between the field and sensing wires, or jumping over the top sensing wire of the system. The field and sensing wires should be supervised to prevent the undetected cutting or bypassing of the system through electronic or clandestine means. The system design should employ techniques to minimize alarms caused by high winds, thunderstorm-related electrical phenomena, and small animals.

(2) *Installation Criteria.* The E-field sensor should consist of a minimum of one field wire and two sensing wires. One sensing wire should be located no more than 0.45 meter above ground level with the second located approximately 2.6 meters above ground level. The field wire should be located between the sensing wires approximately 1 meter above ground level. The surrounding terrain within 3 meters of E-field wires should be free of all shrubs, trees, and undergrowth. The control unit should be well grounded using a 1-meter or longer grounding rod or equivalent electrical ground. When mounted to a chain link fence, the fence should also be well grounded approximately every 23 meters using a 1-meter or longer grounding rod or equivalent electrical ground.

d. Ferrous Metal Detector Perimeter Alarm System

(1) *Performance Criteria.* A ferrous metal detector perimeter alarm system should be able to detect a 400-pole-centimeter (CGS units) magnet moving at a rate of 0.15 meter per second within a radius of 0.3 meter of a sensor cable. The detection system should be equipped with inhibitor coils to minimize nuisance alarms due to electromagnetic interference. No more than six sensing loops per inhibitor coil should be used in order to prevent simultaneous desensitizing of the entire system.

(2) *Installation Criteria.* To determine if the ferrous metal detection system will operate in the proposed environment, a preengineering site survey should be made using an electromagnetic detection survey meter. This survey meter can be furnished by the manufacturer. If the electromagnetic disturbances are within the limits prescribed by the manufacturer, this type of system can be used effectively. Special looping configurations can be made in areas of high electromagnetic interference to reduce the incidence of nuisance alarms.

The sensing loops of electrical cable should be buried in the ground according to the manufacturer's stated depth. Multiple units (cable and amplifier) should be used to protect a perimeter. All associated buried circuitry should be buried within the protected zone and packaged in hermetically sealed containers. The cable should be laid in accordance with the manufacturer's recommended geometrical configurations to reduce nuisance alarms from external sources. When cable is being installed in rocky soil, care should be taken to remove sharp rocks during backfilling over the cable.

Inhibitors should be buried in the ground at least 6 meters from the cable inside the protected perimeter.

Continuous electromagnetic interference obstructs the detection of an intruder carrying metal over the buried cable by keeping the inhibitor activated, thereby preventing the alarm unit from responding to a change in flux caused by the intruder. The device should therefore be used only where the environment is relatively free of severe man-made electromagnetic interference (e.g., overhead power cables, pole-mounted transformers, generators). The cable should never be installed close to overhead power transmission lines. Moreover, the cable should be placed at least 3 meters from parallel-running metal fences and at least 20 meters from public roads to minimize nuisance alarms.

e. Pressure-Sensitive Perimeter Alarm System

(1) *Performance Criteria.* A pressure-sensitive perimeter alarm system should be capable of detecting an individual weighing more than 35 kilograms crossing the sensitive area of the system at a minimum speed of 0.15 meter per second, whether walking, crawling, or rolling. The system design should employ techniques (e.g., electronic signal processing) to eliminate nuisance alarms from wind and other adverse environmental phenomena.

(2) *Installation Criteria.* The sensors should be installed at the depth below the ground surface stated by the manufacturer. To obtain a high probability of detection, the sensors should be in two separate parallel lines at a distance of 1.5 to 2 meters apart. The sensors and electronic circuitry buried in the ground should be of a durable, moistureproof, rodent-resistant material. When a pressure-sensitive perimeter alarm system is being installed in rocky soil, all rocks should be removed during backfilling to prevent damage to sensors. If the frost line exceeds 10 cm, a buried pressure-sensitive system should not be used unless the soil is specifically prepared to eliminate freezing above the sensor.

f. Infrared Perimeter Alarm Systems

(1) *Performance Criteria.* An infrared perimeter alarm system should be a multibeam modulated type consisting of a minimum of three transmitters and three receivers per unit. An infrared perimeter alarm system should be capable of detecting an individual weighing a minimum of 35 kilograms passing between the transmitters and receivers at a rate between 0.15 and 5 meters per second, whether walking, running, jumping, crawling, or rolling. Furthermore, the systems should be able to operate as above with a factor of 20 (13db) insertion loss due to atmospheric attenuation (e.g., fog) at maximum range (100 meters).

(2) *Installation Criteria.* An infrared perimeter alarm system should be installed so that, at any point, the lowest beam is no higher than 21 cm above grade and the highest beam at least 2.6 meters above ground. Sufficient overlap of beams should exist such that an individual could not intrude between the beams and remain undetected. The ground areas between the infrared beam posts should be prepared to prevent tunneling under the lower beam within at least 15 cm of the surface. This may be accomplished by using concrete, asphalt, or a similar material in a path at least 1 meter wide and 15 cm deep or alternatively 15 cm wide and 1 meter deep between the posts.

The transmitters and receivers should be mounted rigidly (e.g., installed on a rigid post or concrete pad) to prevent nuisance alarms from vibrations. Each transmitter and receiver post should be provided with a pressure-sensitive cap to detect attempts at scaling of or vaulting over the infrared beam post. The maximum distance between transmitter and receiver should be selected to permit proper operation during conditions of severe atmospheric attenuation that are typical for the site, generally a maximum of 100 meters.

It is recommended that the infrared perimeter alarm system be installed inside the physical perimeter barrier with the transmitter and receiver units positioned a minimum of 3 meters from the barrier. Installation of the infrared alarm system inside and directly adjacent to the perimeter barrier should be avoided since the barrier may provide a solid base from which an intruder can jump over the beams into the protected area.

g. Vibration or Strain Detection

This vibration- or strain-detection system should be used only as a secondary or backup perimeter alarm system except when one of the other five types of perimeter alarm systems will not work (e.g., because of the environment) and after the NRC's approval has been received. If there is a need to use this system, the following criteria should apply:

(1) *Performance Criteria.* Vibration- or strain-detection systems used for fence protection should detect an intruder weighing more than 35 kilograms attempting to climb the fence. The system should also detect any attempt to cut the fence or lift the fence more than 15 cm above grade. The system should not generate alarms due to wind vibration of the fence from a wind force of up to 48 kilometers/hour.

(2) *Installation Criteria.* The vibration or strain sensors should be attached firmly to the fence (post or fabric, as appropriate) so that the vibration/stress caused by an intruder climbing, cutting, or lifting the fence will generate an alarm.

2. Testing of Perimeter Intrusion Alarm Systems

All tests and test results should be documented. The documented test results will establish the performance history of each perimeter alarm system and each segment of the isolation zone. The test results should be available for inspection and analysis.

a. Operability Testing

Perimeter intrusion alarm systems should be tested on all segments of the isolation zone at least once each 7 days. Testing may be conducted during routine patrols by the members of the licensee security force. The testing should be conducted by crossing the segment of the isolation zone where the alarm system is located or by climbing the fence to which the system is attached to provide the required alarm stimulus. Where appropriate, a specific test procedure should be followed. Prior to making the test, the individual making the test should notify the central alarm station that a test is about to be conducted. The area under test should be maintained under visual observation by a member of the security organization.

All segments of the isolation zone should be tested in a different, preferably random, order every 7 days and the testing should be conducted throughout the week, not all tests on 1 day. The operability testing should result in 100% detections on all segments each 7 days. If the perimeter alarm system fails to detect an intrusion on one or more segments, corrective actions should be taken and documented. See the operability testing section of Appendix A to this guide for a sample method for determining the testing order for the segments and a suggested method for determining if the detection rate of the perimeter alarm system has decreased to below 90%. Other testing methods may be used if the methods are fully documented and approved by the NRC.

b. Performance Testing

At least quarterly, i.e., once each 93 calendar days, after each inoperative state, and after any repairs, the perimeter intrusion alarm system should be tested against its manufacturer's design specifications and for proper detection probability. An inoperative state for an alarm system or component exists when (1) the power is disconnected to perform maintenance or for any other reason, (2) both primary and backup power sources fail to provide power, and (3) when power is applied and one or more components fail to perform their intended function. Placing a properly operating alarm system in the access mode would not constitute an inoperative state unless accompanying or followed by any of the above three conditions.

(1) *Specification Testing.* The test procedure recommended by the manufacturer should be followed. While the test is being conducted, the area under test should be maintained under visual observation by a member of the security organization. For all perimeter systems, tests should be conducted to verify that no obvious dead spots exist in the segment of protection. As a minimum, the tests should include line supervision and tamper proofing when testing in both the access and secure modes. If the perimeter alarm system does not meet the manufacturer's specifications, corrective actions should be taken and documented.

(2) *Detection Probability Testing.* Proper detection probability is defined as the ability to detect an intruder with at least 90% probability in each segment of the isolation zone, with 95% confidence, under the conditions stated in the Performance Criteria of each type of alarm system. While the detection probability testing is being conducted, the area under test should be maintained under visual observation by a member of the security organization. One sample testing method for demonstrating compliance with detection probability and confidence levels is given in the detection probability testing section of Appendix A to this guide. Other testing methods may be used if the methods are fully documented and approved by the NRC.

D. IMPLEMENTATION

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

Except in those cases in which the applicant or licensee proposes an acceptable alternative method, the staff will use the methods described herein in evaluating an applicant's or licensee's capability for and performance in complying with specified portions of the Commission's regulations after April 1, 1980.

If an applicant or licensee wishes to use the method described in this regulatory guide on or before April 1, 1980, the pertinent portions of the application or the licensee's performance will be evaluated on the basis of this guide.

VALUE/IMPACT STATEMENT

A separate value/impact analysis has not been prepared for the proposed revision to this regulatory guide. The changes were made to make the guide consistent with the upgraded physical protection amendments to the regulations published in final form in the *Federal Register* of November 28, 1979 (44 FR 68184). A value/impact anal-

ysis prepared for the proposed amendments was made available in the Commission's Public Document Room at the time the proposed amendments were published. This analysis is appropriate for the final amendments as well as for the regulatory guide revisions appropriate to those amendments.

APPENDIX A*

EXAMPLES OF TESTING METHODS FOR PERIMETER INTRUSION ALARM SYSTEMS

BACKGROUND

The purpose of this appendix is to provide an example of a testing method to determine detection capability of perimeter intrusion alarm systems. This example should not be interpreted as a regulatory requirement. Other testing methods for determining compliance with detection probability and confidence levels may be used if fully documented and approved by the NRC. The purpose of testing a perimeter intrusion alarm system is to ensure that the installed system is operating according to the three testing criteria stated below.

1. *Operability Testing* - Paragraph C.2.a of this guide states: "Perimeter intrusion alarm systems should be tested on all segments of the isolation zone at least once each 7 days.... The operability testing should result in 100% detections on all segments each 7 days."
2. *Specification Testing* - Paragraph C.2.b of this guide states: "At least quarterly, ... the perimeter intrusion alarm system should be tested against its manufacturer's design specifications ..."
3. *Detection Probability Testing* - Paragraph C.2.b(2) states: "Proper detection probability is defined as the ability to detect an intruder with at least 90% probability in each segment of the isolation zone, with 95% confidence ..."

DEFINITIONS

In order to ensure uniform testing, the following terms are defined:

1. *Zone (Isolation Zone)* - The entire perimeter adjacent to the protected area.
2. *Segment* - A portion of the isolation zone that is independently alarmed and monitored.
3. *Running* - Entering and leaving the zone of detection at an approximate velocity of 5 meters per second.
4. *Walking* - Entering and leaving the zone of detection with a normal stride.
5. *Crawling* - Entering and leaving the zone of detection by lying prone to the ground, perpendicular to the zone of detection, with a low profile at an approximate velocity of 0.15 meter per second.

6. *Jumping* - Leaping from a height above the zone of detection to a point at ground level across the zone of detection, e.g., standing on the fence and attempting to leap across the zone of detection.
7. *Rolling* - Entering and leaving the zone of detection prone to the ground with a low profile, parallel to the zone of detection, and rolling slowly at an approximate velocity of 0.15 meter per second.

TESTING

Operability Testing

Operability testing is a check to ensure that the alarm system is operating and that the detection sensitivity of the alarm system has not decreased from the 90% detection rate. The perimeter alarm systems should be tested on each segment of the isolation zone at least once during a 7-day period. For example, the guard may violate the detection field by walking through the sensitive zone. The ordering of the tests on the segments should be in a different, preferably random, order each week, and the testing should be conducted throughout the week. For an example of randomizing the segments, assume that there are 10 segments and 21 shifts per week (3 shifts per day and 7 days per week). Select at random (using a random number table or a random number generator) 10 of the shifts out of the 21 possible shifts, retaining the order in which the shifts were drawn. Then pair these 10 shifts with the segments 1 through 10. In this example, let the 10 shifts selected be 6, 14, 9, 6, 20, 16, 19, 18, 10, 7.

Table 1

Shift No.	Segment No.
6	1
14	2
9	3
6	4
20	5
16	6
19	7
18	8
10	9
7	10

The segment to be tested on each day of the week and the specific shift (1, 2, or 3) can be seen more clearly by reorganizing this information (see Table 2).

* Although this appendix is a substantive addition to Revision 2, no lines are added in the margin.

Table 2

Shift No.	Day - Shift	Segment No.
1	Mon. - 1	None
2	Mon. - 2	None
3	Mon. - 3	None
4	Tues. - 1	None
5	Tues. - 2	None
6	Tues. - 3	1, 4
7	Wed. - 1	10
8	Wed. - 2	None
9	Wed. - 3	3
10	Thurs. - 1	9
11	Thurs. - 2	None
12	Thurs. - 3	None
13	Fri. - 1	None
14	Fri. - 2	2
15	Fri. - 3	None
16	Sat. - 1	6
17	Sat. - 2	None
18	Sat. - 3	8
19	Sun. - 1	7
20	Sun. - 2	5
21	Sun. - 3	None

The testing could be conducted such that no shift tests more than one segment if the number of segments is less than the number of shifts. There are many other possible methods for ordering the segments, depending on the number of segments and the number of shifts. For example, if there are more segments than shifts, the ordering method could require that each shift test at least one segment.

The test results should be documented on a success/failure basis. If the test on a segment results in a failure, corrective actions should be taken and documented. For example, if the test of a segment results in no alarm, the alarm system should be checked for an obvious problem such as an incorrect setting and should be retested four more times during the same shift if possible. If all four of these tests result in alarms, the alarm system on the segment should be tested five more times on the next day. If all these five tests result in alarms, the weekly testing schedule for this segment can be resumed since the 90% detection rate can be confirmed. If any failures occurred during the nine additional tests, the alarm system for the segment will need to be thoroughly checked, repaired, and retested according to the detection probability testing method to demonstrate that the alarm system for the segment is now detecting intrusions with at least a 90% detection rate, with 95% confidence. A table similar to Table 3 (see page 5.44-11) may be used for recording the test results.

Specification Testing

The licensee should conduct a manufacturer's design specification test of the system under test before the detection probability tests have been conducted on all segments and the results documented. The licensee should follow the test procedures recommended by the manufacturer of that system. If the system does not meet the

manufacturer's specifications, the recommended actions include retesting and calling the manufacturer's representative for repairs or upgrading of the system.

Detection Probability Testing

The following is one example of a method for detection probability testing:

1. Determine the most vulnerable area of each segment, and determine the method of approach most likely to penetrate that segment, i.e., walking, running, jumping, crawling, rolling, or climbing. This determination will, in most cases, be terrain dependent.
2. Test all segments using all the applicable penetration approaches at the most vulnerable area 30 times initially, after installing a new system, after repairing or upgrading the system, or after the system failed to meet the minimum number of the successful detection criterion given below. All 30 tests must have resulted in successful detections of the intrusion in order to have at least a 90% probability of detection, with 95% confidence.

If the minimum number of successful detections is not achieved, the system should be checked. If no problems with the system are discovered, 10 more tests should be made and if the minimum number of successful detections is achieved for the new number of tests (given in Table 4), in this case 39 out of 40, the testing can be ended for this segment for this quarter. If no problems with the system can be discovered and the minimum number of successful detections is not achieved after one more test of 10 intrusions, the system would need to be upgraded to increase the detection probability to the required level. If problems with the systems are discovered, the system should be repaired and 30 new tests performed. If there are 30 successful detections, testing can be ended.

For the subsequent tests at 90-day intervals, each segment should be tested 10 times. Each segment should show at least 9 successful detections out of 10 approaches and the cumulative results (combining the present results with the results from previous quarters) should have at least the minimum number of successful detections given in Table 4.

Table 4

Total No. of Tests	Minimum No. of Successful Detections	Maximum No. of Failures to Detect
30	30	0
40	39	1
50	48	2
60	57	3
70	67	3
80	76	4
90	85	5
100	95	5
110	104	6
120	114	6

Table 3

OPERABILITY TESTING RESULTS
(Success = 1, Failure = 0)

Week x, Quarter y, 19zz

	<u>Date</u>	<u>Time</u>	<u>Environmental Conditions</u>	<u>Result</u> 1 or 0	<u>4 Retests</u>	<u>5 Retests</u>
Segment 1	_____	_____	_____	_____	_____,_____,_____,_____,_____	_____,_____,_____,_____,_____,_____
Segment 2	_____	_____	_____	_____	_____,_____,_____,_____,_____	_____,_____,_____,_____,_____,_____
Segment 3	_____	_____	_____	_____	_____,_____,_____,_____,_____	_____,_____,_____,_____,_____,_____
•						
•						
•						

Attempt all applicable penetration approaches for a man-on-the-ground target. The penetration approach most likely not to be detected should be attempted more frequently if an equal number of tests per approach is not possible. For example, if the applicable penetration approaches for a given segment in the system are running, walking, and crawling, the 10 quarterly tests would be divided among the 3 approaches. If crawling has the worst detection record, running would be attempted three times, walking three times, and crawling four times.

4. Randomize the order in which the segments are tested. Randomization is a means of ensuring that environmental effects and other unknown factors that may affect the test results (detection or nondetection) do not always favor or handicap the same segment or method of approach. For example, if Segment 1 is always tested in the morning and Segment 2 is always tested in the afternoon and if the detection equipment is slightly more sensitive to intrusions in the morning, the conclusion might be drawn, based on the test results, that Segment 2 is less protected than Segment 1. However, the difference noted between the two segments might be due only to the morning vs. afternoon difference. Similarly, by randomizing the methods of approach, no approach will be continually favored if the time sequence (ordering) affects the test results. Randomization is protection against disturbances that may or may not occur and that may or may not be serious if they do occur. Randomization can be accomplished by using a random numbers table to assign the order in which the segments will be tested.

5. Maintain records of the results of all tests performed. Included in these records should be the segment number, date, time, and relevant environmental conditions when tests were performed. Table 5 (see page 5.44-13) provides a suggested format for recording the test results. The test results in the "Overall" (totals) row in the columns headed (b), (c), (b'), and (c') are the important summary values. For the initial testing or when retesting the perimeter alarm system after it has failed to meet the minimum number of successful detections given in Table 4, the (b) and (c) values should be 30 and 30, or 39 and 40, or 48 and 50. For the subsequent quarterly testing, (b) must be 9 or 10 and (c) is 10 and (b') must be at least the number under "Minimum No. of Successful Detections" for the (c') value ("Total No. of Tests") in Table 4.

Detection Probability Statements

One method for assessing the probability of detection of the entire detection system is to use the "chain model," i.e., the weakest "link" in the system determines the probability of detection for the system. In this case, the approach to a particular segment that has the lowest probability of detection would equal the probability of detection for the system. This is a "worst case" approach; however, it is the vulnerable areas of the system that need to be discovered and eliminated.

One of the problems in testing intrusion-detection systems is the need for a large number of tests to be performed on each segment to estimate well the probability of detection in each segment. One example of a method to be used to avoid performing a large number of tests on each segment each quarter is to use an empirical Bayesian approach to estimate the probability of detection. The empirical Bayesian method¹ combines the present quarter's data with those of previous quarters. Using the empirical Bayesian method, the performance criterion can be tested without a large number of tests being performed each quarter.

For the total number of tests less than 100 on each segment, the performance criteria are relaxed to be "at least 88% probability of detection in a segment with 95% confidence." When the number of tests is 100 or more, the performance criterion of "at least 90% probability of detection in a segment with 95% confidence" is used.

Table 6 gives the probability statements for the number of tests between 30 and 120 with a given minimum number of successful detections.

Table 6

Table No. of Tests	Minimum No. of Successful Detections	Statement: The probability of detection is at least __%, with 95% confidence
30	30	90.5
40	39	88.7
50	48	87.9
60	57	87.6
70	67	89.3
80	76	88.9
90	85	88.7
100	95	89.8
110	104	89.6
120	114	90.4

For example, one is 95% sure that the probability of detection is at least 89.8% for the test results of 95 successful detections out of 100 tests, i.e., the lower 95% confidence limit for the probability of detection is 89.8%.

Appendix B to this guide gives the details for deriving these statements. Table 1 in Appendix B gives the probability statements associated with all the numbers of successful detections out of the total number of tests performed that result in at least a 90% probability of detection with a 95% confidence level. The total number of tests covered in this table range from 30 to 120 in increments of 10 tests.

Using Table 1 in Appendix B, stronger statements can be made about the probability of detection for the number of

¹For a discussion of Bayesian methods, see H. F. Martz, Jr., and R. A. Waller, "The Basics of Bayesian Reliability Estimation from Attribute Test Data," Los Alamos Scientific Laboratory Report LA-6126, February 1976.

Table 5

DETECTION PROBABILITY TESTING RESULTS

Date: _____

Time: _____

Environmental Conditions: _____

<u>Segment x</u>		<u>Quarter y, 19zz Data Only</u>			<u>Data Combined from Quarter s, 19tt to Quarter y, 19zz</u>			
<u>Method of Approach</u>	<u>(a) No. of Failures to Detect</u>	<u>(b) No. of Successful Detections</u>	<u>(a)+(b)=(c) Total No. of Tests</u>	<u>(b)/(c) Prob. of Detection</u>	<u>(a') Combined No. of Failures to Detect</u>	<u>(b') Combined No. of Successful Detections</u>	<u>(a')+(b')=(c') Combined Total No. of Tests</u>	<u>(b')/(c') Combined Prob. of Detection</u>
Running	--	--	--	--	--	--	--	--
Walking	--	--	--	--	--	--	--	--
Crawling	--	--	--	--	--	--	--	--
Jumping	--	--	--	--	--	--	--	--
Rolling	--	--	--	--	--	--	--	--
Climbing	--	--	--	--	--	--	--	--
Overall	--	--	--	--	--	--	--	--

successful detections greater than the minimum number. For example, if there were 98 detections out of 100 tests, one should state: "The probability of detection is at least 93.8% with 95% confidence."

In addition to the overall lower confidence limit on the probability of detection for a segment considered previously, a point estimate can be computed for the probabilities of detection for each method of approach for each segment, as well as a point estimate for the overall probability of detection for each segment. The point estimate of a probability of detection is the number of successful detections divided by the total number of tests of the type being considered. Note that these point estimates are different from the lower 95% confidence limits discussed previously. The benefit of computing point estimates for each method of approach in each segment is to recognize a segment that may be particularly vulnerable to a specific method of approach. The concept is to look for trends occurring in the data. For example, if all or most of the failures to detect in a segment are in one method of approach, this segment should be suspected as being vulnerable to this method of approach. As a specific example, let the initial 30 tests be 6 tests each of running, walking, crawling, jumping, and rolling. Assume that no failures to detect intrusion occurred. The point estimate for the overall probability of detection is $30/30 = 100\%$; the point estimate for the probability of detection for a crawling approach is $6/6 = 100\%$. Let the subsequent quarterly tests be two tests each of the five methods of approach. In the next three quarters, assume that one failure to detect occurred in a crawling approach. Table 7 below gives the point estimates for the overall probability of detection and for the crawling approach.

Note that the minimum number of successful detections are achieved for the total number of tests and 9 successful detections are achieved for the 10 quarterly tests. However, by computing the point estimates for each method of approach the trend can be seen that a crawling approach has a fairly

Table 7

Quarter	Overall Probability of Detection	Probability of Detecting Crawling
1st (initial)	$30/30 = 1$	$6/6 = 1$
2nd	$39/40$	$7/8 = .875$
3rd	$48/50$	$8/10 = .8$
4th	$57/60$	$9/12 = .75$

high likelihood of not being detected. Additional testing should be performed to verify that the particular approach is a system weakness, not random failures that coincidentally occurred in the same method of approach. If the weakness is verified, it should be eliminated, perhaps by increasing the sensitivity of the detector or by installing an additional device to detect this type of approach with a higher probability. If, on the other hand, the failures of detection come from varying approaches and if the overall probability of detection in the segment is sufficiently high, i.e., the maximum number of failures to detect for the total number of tests is not exceeded, no specific weakness is indicated for this segment.

Caution : When the data indicate a problem with the detection system and the problem is corrected, do not combine (sum) the next quarter's data with the data from previous quarters for the problem segment. Begin accumulating the data again for this segment, starting with the 30 tests from the current quarter's testing that were conducted after correcting the problem.

A table similar to Table 5 can be used for recording and reporting the test results for each method of approach, each segment, and each quarter. The date and time of day and relevant environmental conditions such as weather, microwave field intensity, E-field intensity, and changes in light level should be recorded.

APPENDIX B*

CALCULATING THE CONFIDENCE LIMIT ON THE DETECTION PROBABILITY

Assume a binomial model for the number of successful detections, i.e., the probability of a successful detection is a fixed value, designated "p", and the tests for detection are independent. Let the number of tests performed be "n" and the number of successful detections "x".

The point estimate of p, $\hat{p}$, is x/n .

However, the problem is to obtain a confidence interval for p, which in this case is a lower one-sided 95% confidence limit.

The normal approximation to the binomial distribution is a valid approximation only when $n\hat{p}$ and $n(1 - \hat{p})$ are both equal to or greater than 5. For example, for the performance criterion of 48 successes out of 50 tests, $n(1 - \hat{p})$ equals 2. Also, when there are no failures in detection, it is not possible to use the normal approximation since $\text{var}(\hat{p}) = n\hat{p}(1 - \hat{p}) = 0$.

The exact lower 95% confidence limit on p is given by

$$\frac{x}{x + [(n - x + 1) \cdot F_{.05}(2n - 2x + 2, 2x)]} \quad (1)$$

where $F_{.05}(a,b)$ is the value of the F distribution with "a" and "b" degrees of freedom which leaves 5% in the upper tail of the distribution.

Three examples given in Appendix A to this guide can be derived as follows:

1. For x = 48 successes and n = 50 tests,

$$\frac{48}{48 + 3(2.19)} = \frac{48}{54.57} = 87.96\%$$

* Although this appendix is a substantive addition to Revision 2, no lines are added in the margin.

using $F_{.05}(6,96) \approx 2.19$.

2. For x = 95 successes and n = 100 tests,

$$\frac{95}{95 + 6(1.80)} = \frac{95}{105.8} = 89.79\%$$

using $F_{.05}(12,190) \approx 1.80$.

3. For x = 98 successes and n = 100 tests,

$$\frac{98}{98 + 3(2.14)} = \frac{98}{104.42} = 93.85\%$$

using $F_{.05}(6,196) \approx 2.14$.

Table 1 gives the lower 95% confidence limits for the probability of detection for n = 30, 40, 50, 60, 70, 80, and 90 beginning with x values such that the lower confidence limit is approximately equal to 88%; and for n = 100, 110, and 120 beginning with x values such that the lower confidence limit is approximately equal to 90%. The lower confidence limits for n = 30, 40, and 50 were abstracted from "Percentage Points of the Incomplete Beta Function," Robert E. Clark, *Journal of the American Statistical Association* 48: 831-843 (1953). The lower confidence limits for n = 60, 70, 80, 90, and 100 were abstracted from "Tables of Confidence Limits for the Binomial Distribution," James Pachares, *Journal of the American Statistical Association* 55: 521-533 (1960). The lower confidence limits for n = 110 and 120 were computed using Formula (1).

Clark's article gives confidence limits for all values of n from 10 to 50 for all values of x from 1 to n. Pachares' article gives confidence limits for values of n from 55 to 100 in increments of 5 for all values of x from 1 to n. The confidence limits for any values of n and x can be computed using Formula (1).

Table 1
LOWER 95% CONFIDENCE LIMITS FOR p

<u>No. of Tests</u>	<u>No. of Successful Detections</u>	<u>Statement: The probability of detection is at least % with 95% confidence.</u>
n = 30	x = 30	90.5
n = 40	x = 39	88.7
	40	92.8
n = 50	x = 48	87.9
	49	90.9
	50	94.2
n = 60	x = 57	87.6
	58	89.9
	59	92.3
	60	95.1
n = 70	x = 67	89.3
	68	91.3
	69	93.4
	70	95.8
n = 80	x = 76	88.9
	77	90.6
	78	92.3
	79	94.2
	80	96.3
n = 90	x = 85	88.7
	86	90.1
	87	91.6
	88	93.2
	89	94.8
	90	96.7
n = 100	x = 95	89.8
	96	91.1
	97	92.4
	98	93.8
	99	95.3
	100	97.0
n = 110	x = 104	89.6
	105	90.7
	106	91.9
	107	93.1
	108	94.4
	109	95.7
	110	97.3
n = 120	x = 114	90.4
	115	91.4
	116	92.5
	117	93.7
	118	94.8
	119	96.1
	120	97.5

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

**OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, \$300**

**FIRST CLASS MAIL
POSTAGE & FEES PAID
USNRC
PERMIT No. G-67**