U.S. NUCLEAR REGULATORY COMMISSION

Revision 1
June 1976

REGULATORY GUIDE

OFFICE OF STANDARDS DEVELOPMENT

REGULATORY GUIDE 5.44

PERIMETER INTRUSION ALARM SYSTEMS

A. INTRODUCTION

Paragraph 73.50(b)(4) of 10 CFR Part 73, "Physical Protection of Plants and Materials," requires at fuel reprocessing plants and certain other plants at which high enriched uranium, uranium-233, or plutonium is used or processed that the isolation zone surrounding the physical barrier at the perimeter of the protected area be monitored to detect the presence of individuals or vehicles within the zone so as to allow response by armed members of the licensee security organization to be initiated at the time of penetration of the protected area.[a] 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.

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 which 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. Testing for operability can be performed by a guard or watchman penetrating the zone protected by the alarm system during routine patrols. Functional performance testing, however, usually is more elaborate. In any case, testing can be meaningful without compromising security only if performed under controlled circumstances, such as direct visual observation of the area being tested while a specified test is conducted.

To ensure normal 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 may institute a test program that will periodically test each zone of a perimeter alarm system to verify that it maintains the proper sensitivity to detection.

[a]Paragraph (b)(3) of proposed rule 73.55, "Requirements of licensed activities in nuclear power reactors against industrial sabotage," will have similar requirements to monitor the isolation zone around the physical barrier at the perimeter of the protected area and any part of a building used as part of that physical barrier.

*Lines indicate substantive changes from previous issue.

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 condition. 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. 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 usually is 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 which 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 this 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 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 free standing system in the center of an isolation zone.

The E-field system can offer about 300 meters of perimeter protection, but shorter lengths of 100 meters are recommended in order to have effective alarm 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 so as 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 grounded 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 1/2 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 which 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 cable sensor, senses strong temporary electromagnetic interference (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 only detect 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 zone up to 500 meters in length. Increasing the length of the security zone 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 upon 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 pre-established 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, installation in rocky soil may result in damage to the pressure transducers either during installation or as a result of soil settlement after installation. 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; however, 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 which 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 one 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 line-of-sight. 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 also will attenuate the infrared beam as will an accumulation of condensation, frost, or ice on the faceplates.

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 of the fence. However, most fence alarm systems can be easily bypassed by a variety of methods.

Depending upon the variety of sensor, each sensor can monitor a length of fence ranging from about one 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 meet the requirements of Underwriters Laboratory (UL) for fire safety. The system should contain provisions for automatic switchover to emergency battery and generator or emergency battery power without causing an 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 daily in accordance with manufacturers' instructions to ensure that available capacity is not less than 80% of rated capacity.

(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.[a]

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.[b]

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 of Facilities and Special Nuclear Material").

(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 systems should be capable of effective operation between −35° and +50°C. Components which necessarily must be located out of doors should be protected from moisture damage by such methods as hermetic sealing or potting in an epoxy compound.

(4) *Alarm Conditions.* Perimeter intrusion alarm systems should generate an alarm under any of the following conditions:

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

(b) Failure of emergency power to properly operate the system in the event of loss of primary 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 or aging 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 aged or failed in a device.

Under normal environmental conditions, perimeter alarm systems should not average more than one false alarm per week per zone and should not average more than one nuisance alarm per week per zone while maintaining proper detection sensitivity. Where the zone is under continuous visual observation, the false alarm rate and nuisance alarm rate may be increased to one alarm per day per zone. *False alarms* are defined as those alarms which have been generated without any apparent cause. *Nuisance alarms* are defined as those alarms generated by the alarm system detecting a change in the operating environment. *Proper detection sensitivity* is defined as the ability to detect an intruder in the secured zone ninety-five out of one hundred times 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, if primary power is supplied from the central alarm station.

[a]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.

[b]Signal line supervision will be discussed in a regulatory guide currently under development on interior intrusion alarm systems. Reference should be made to the Interim Federal Specification W-A-00450B (GSA-FSS) February 16, 1973, paragraph 3.5.

Loss or reduction of power (either primary or emergency) to the degree that the system is no longer *operating properly should result in an alarm condition or* be otherwise 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.* Perimeter intrusion alarm systems generally may be located on either side of the perimeter physical barrier. 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 second barrier should be separated a minimum of 10 meters from the inner fence to prevent bridging of the perimeter alarm system. 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 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, 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. Due to 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 at least 50 meters. 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 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 widths 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 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 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 transmitter 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 crawling and rolling under the lower sensing wire, stepping and jumping between the field and sensing wires, and jumping over the top sensing wire of the system. The field and sensing wires should be supervised to prevent the cutting or bypassing of the system through electronic or clandestine means. The system design should employ techniques to eliminate alarms caused by high winds 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 should be located between the sensing wires approximately 1 meter above ground level. The surrounding terrain 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, etc.). 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 meters per second, whether walking, crawling, or rolling. The system design should employ techniques (e.g., electronic signal processing) to eliminate nuisance alarms from wind.

(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 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.

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 prevent 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 outside and parallel to an outer fence or wall with the transmitter and receiver units positioned greater than 3 meters from the barrier. If it is desired to reduce nuisance alarms caused by stray animals, blowing trash, or the general public, then the infrared perimeter alarm system may be placed inside the outer fence. However, the transmitter and receiver units should be positioned between 2.0 and 2.5 meters from the fence to prevent an individual from jumping over the infrared beams from atop the fence or sprinting through the beams. Installation of the infrared alarm system inside the perimeter and adjacent to an outer wall should be avoided since the wall provides a solid base from which an intruder can jump over the beams into the protected area.

g. Vibration or Strain Detection

(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.

The fence alarm system should only be used 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 Commission's approval has been received.

(2) *Installation Criteria.* The vibration or strain sensors should be attached firmly to the fence (post or fabric, as appropriate) such 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

a. Performance Testing

Perimeter intrusion alarm systems should be tested at least once each 7 days. Testing may be accomplished during routine patrols by the members of the licensee security force. The alarm systems should be tested in segments at random with only one or two segments tested per patrol. However, every segment should be tested at least once every 7 days. The testing should be conducted by crossing the isolation zone where the alarm system is located or by climbing the fence to which the system is attached. 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.

b. Specification Testing

At least quarterly, the perimeter intrusion alarm system should be tested against its manufacturer's design specifications. The test procedure recommended by the manufacturer should be followed. While the test is being conducted, the area under test should be maintained under direct 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 zone of protection.

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 December 1, 1976.

If an applicant or licensee wishes to use the method described in this regulatory guide on or before December 1, 1976, the pertinent portions of the application or the licensee's performance will be evaluated on the basis of this guide.