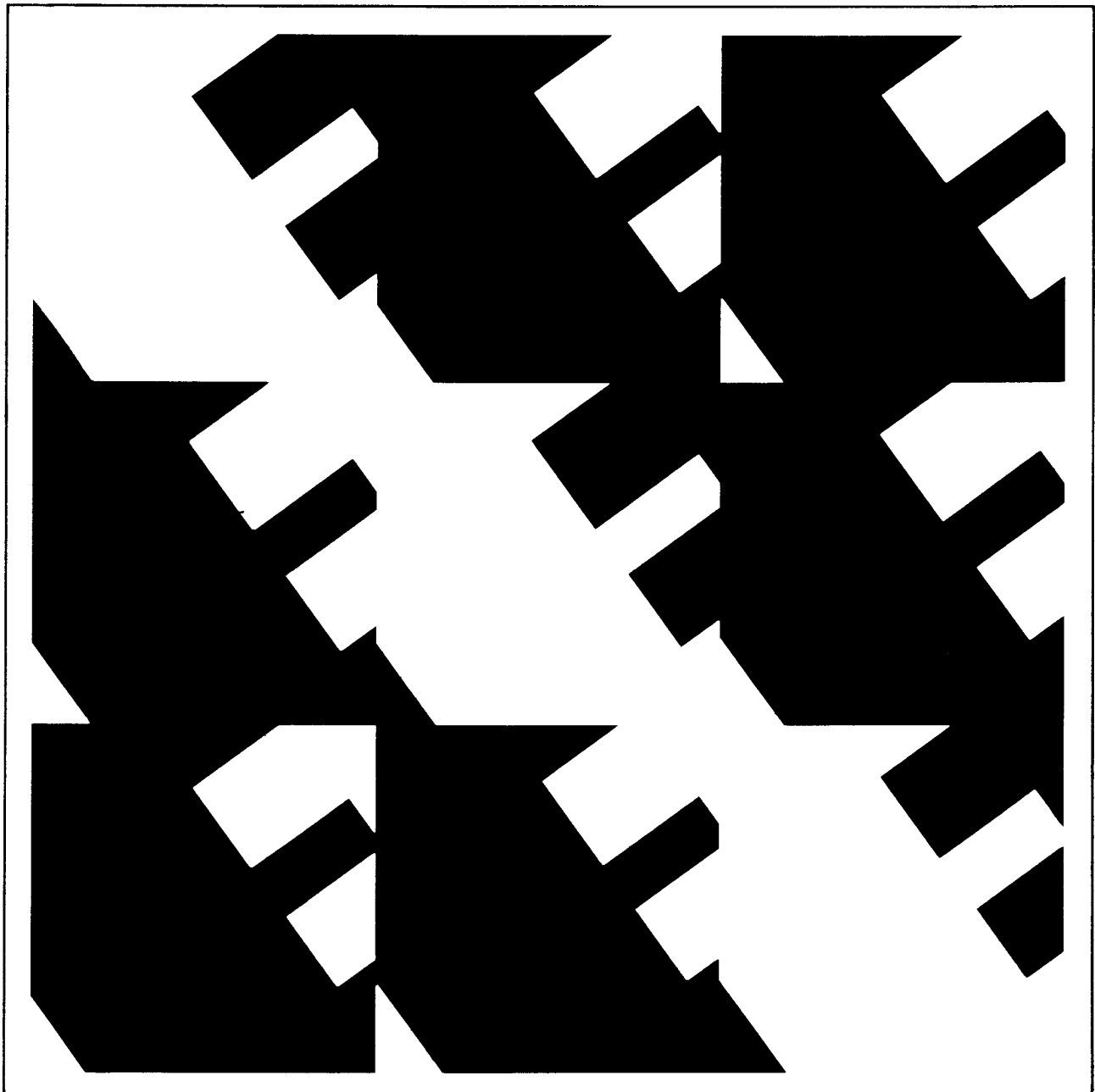


IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations



IEEE Std 692-1986



Published by The Institute of Electrical and Electronics Engineers, Inc 345 East 47th Street, New York, NY 10017, USA
February 10, 1986

SH10173

IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations

1. Introduction

1.1 Purpose. A complete nuclear power generating station security program consists of security personnel, barriers, security and contingency plans, procedures, and security equipment. The purpose of this standard is to establish criteria to guide the designer in the selection and application of equipment to detect, monitor, display, and record security conditions at nuclear power generating stations.

1.2 Scope. These criteria include minimum design, testing, and maintenance parameters for permanently or temporarily installed systems, subsystems, or components used by the security force for monitoring, surveillance, access control, communication, and data acquisition.

This standard is not intended to cover the following security-related topics:

- (1) Development of threat and response criteria
- (2) Barrier requirements
- (3) Security force composition or deployment
- (4) Classification of vital equipment or vital areas
- (5) Contingency plans
- (6) Mechanical locks and mechanical hardware
- (7) Construction security requirements

2. Definitions

Unique terms used in this standard are listed and defined below:

central alarm station (CAS). A continuously manned alarm station that provides the primary security system functions.

emergency egress. A path or route that provides an immediate exit path or way out of an area in the event of a sudden, unexpected, or dangerous occurrence.

intrusion detection. Sensing the presence of an intruder or object within specific confines.

isolation zones. Any area, adjacent to a perimeter physical barrier, cleared of all objects that conceal or shield an individual.

legitimate access. The proper and correct access authorization.

patrol tours. An inspection by a member of the security organization along a predetermined route to observe the route area's security conditions.

patrol tour stations. Points along patrol tour routes where security force member progress is acknowledged.

protected area. A controlled-access area encompassed by physical barriers.

restrike time. The time period during which a momentary loss or reduction of illumination results from the need to cool down to restrike the arc after a momentary loss or reduction of electrical power to a luminaire.

secondary alarm station (SAS). A continuously manned alarm station that is capable of providing all necessary backup security system functions in the event the central alarm station (CAS) is disabled or compromised.

security system. As used in the context of this standard, *security system* is intended to mean the aggregate assemblage of hardware that includes all components, equipment, barriers, etc, necessary for the physical protection of nuclear power generating stations against the design basis threat of radiological sabotage.

unimpaired observation. Conditions that enable an unobstructed view so as to ensure direct visual or closed circuit television (CCTV) surveillance of individuals or vehicles.

3. References

The following represents a partial listing of the references that were consulted for general background information during the development of this document. These references were used primarily for guidance rather than as standards. Specific identification of each reference at its point of usage has not been indicated.

- [1] ANSI/ANS 3.3-1982, Industrial Security for Nuclear Power Plants.¹
- [2] NRC Regulatory Guide 5.7, Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas.²
- [3] NRC Regulatory Guide 5.12, General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials.
- [4] NRC Regulatory Guide 5.44, Perimeter Intrusion Alarm Systems.
- [5] NUREG-0178, Basic Considerations for Assembling a Closed Circuit Television System.²
- [6] NUREG-0320, Interior Intrusion Alarm Systems.
- [7] NUREG-0908, Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans.
- [8] NUREG/CR-1327, Security Lighting Planning Document for Nuclear Fixed Site Facilities.

¹ ANSI standards are available from the Sales Department, American National Standards Institute, 1430 Broadway, New York, NY 10018.

² NRC and NUREG publications are available from the Division of Document Control, US Nuclear Regulatory Commission (NRC), Washington, DC 20555.

[9] SAND 76-0544, Intrusion Detection Systems Handbook.³

[10] SAND 77-1033, Revised Entry—Control Systems Handbook.

[11] UL 611-1978, Central Station Burglar Alarm Units and Systems.⁴

[12] W-A-00450B (GSA-FSS), Interim Federal Specifications: Alarm Systems, Interior Security, Components.⁵

4. Power Supplies

4.1 General. This section provides the designer with minimum requirements for the design, equipment selection, and installation of the security system power supply.

4.2 Description. The following paragraphs describe power supply systems and the equipment that should be powered from each.

4.2.1 Uninterruptible Power System. The uninterruptible power system shall supply power to all equipment required to maintain continuously monitored parameters. Examples of such equipment are computers (CPU), cathode ray tubes (CRTs), printers, annunciators, multiplexers, CCTVs, perimeter intrusion detection equipment, door controls (card readers, push-buttons, etc), and communications equipment. A typical uninterruptible power system consists principally of a normal supply, a static inverter, a static transfer switch, a battery charger, a battery, and an alternate supply.

4.2.2 Emergency Power System. The emergency power system shall supply power to equipment required to maintain intermittently sampled parameters or to supporting equipment whose failure could be tolerated for a period of time without affecting continuously monitored parameters. Examples are protected area lighting; uninterruptible power system battery charger; interior emergency lighting; critical heating, ventilation, and air-conditioning (HVAC) equipment; and data processing equipment not required for continuous monitoring. A

³ SAND standards are available from the Office of Safeguards and Security, United States Department of Energy, Washington, DC 20545.

⁴ UL standards are available from Underwriters Laboratories, Inc, Publications Stock, 333 Pfingston Rd, Northbrook, IL 60020.

⁵ This publication is available from the Standardization Division, Federal Supply Service, General Services Administration, Washington, DC 20406.

typical emergency power system consists of an emergency supply (standby generator set, automatic transfer equipment, and maintenance bypass switch) and a normal supply. The emergency power system can be either a dedicated standby generator or another plant power supply that meets the requirements of this section.

4.2.3 Plant Auxiliary Bus. The uninterruptible power system alternate supply and emergency interruptible power system normal supply shall be from separate plant auxiliary buses. The plant auxiliary buses can be supplied from off-site or onsite sources.

4.2.4 Battery Packs. Interior emergency lighting and equipment, when located such that providing power from the uninterruptible or emergency (interruptible) power system is not practical or required, can be powered from self-contained battery packs. Security posts and security areas that require illumination during the outage time before the emergency power system is started shall be provided with emergency lighting powered from battery packs.

4.3 Requirements

4.3.1 Location. All power supply equipment shall be installed within the protected area, and all power supply equipment, except the plant auxiliary bus, shall be installed in an area to which access is controlled, or within a tamper-resistant enclosure. A proper environment consistent with equipment rating shall be maintained.

4.3.2 Availability. Automatic switching or transfer of the uninterruptible power system shall not affect continuously monitored parameters. Upon loss of the battery charger and alternate supply, the uninterruptible power system shall be capable of sustaining operation for a minimum of 1 h without replacing or recharging batteries. Upon loss of the normal supply, an emergency supply shall be capable of sustaining operation for a minimum of 24 h. Maximum availability of both the normal supply and the alternate supply shall be a design goal.

Maintenance bypass switches shall be utilized to facilitate the repair of the security power supply.

4.3.3 Annunciation. Degradation of the emergency power source or uninterruptible power system shall be annunciated as equipment failure alarms in accordance with Section 13.

4.3.4 Capacity. The security system power supply shall be capable of supplying power to

all security system equipment in accordance with the manufacturer's specifications. Provisions shall be made to energize the largest connected load or motor, assuming that the system is otherwise fully loaded, without causing loss of other security system load due to voltage dip. The power supply shall be purchased with a minimum capacity 25% greater than the anticipated operational load.

4.3.5 Grounding. The security system power supply grounding shall be consistent with the approved grounding practices used on the power systems at the nuclear power generating station.

5. Security Lighting

5.1 General. This section is limited to the security application of lighting. This section does not replace existing standards concerning the lighting requirements for health and safety, nor does it replace existing standards concerning lighting equipment design or installation. This section does identify the minimal design considerations and criteria that constitute an adequate security lighting design.

5.2 Outdoor Lighting.

5.2.1 Requirements. Each facility shall develop an outdoor security lighting system that supports the surveillance, threat assessment, and adversary engagement functions of that facility's security system. Security lighting shall be provided for the isolation zones and all exterior areas of the protected area, including rooftops within 18 ft of a grade, and higher rooftops if direct unsecured exterior access (for example, ladders, cable raceways, pipes, etc) is available. The lighting shall be of such an intensity, uniformity, color, and location that it shall not hinder the security personnel's ability to observe the protected area by CCTV, direct human means, or both. Shadows shall not permit concealment of an individual. Glare shall not interfere with observation by the security force.

5.2.2 Design Considerations. The system designer shall take into account the following security lighting design considerations.

5.2.3.1 Illumination. The security lighting system shall provide the protected area with an illumination level sufficient to permit unimpaired observation throughout lamp life and service conditions.

5.2.3.1.1 Human Observation. A mini-

lum light level of 1 fc measured horizontally at ground level is recommended. In the context of direct, unaided human observation, sufficient light shall exist to permit an observer of average acuity and night-adapted vision (equal to the security lighting level) to make the following observations at a range of 100 m: the presence of an average-sized person; the physical action of the person (that is, lying, crawling, standing, walking, running, etc); and the direction of the action. The security force shall be able to perform protected area perimeter patrol tour duties without supplementary lighting.

5.2.3.1.2 CCTV Observation. The light level shall be sufficient to permit proper surveillance system operation. Appropriate consideration shall be given to reflectances, glare factors, climatic conditions, and light-to-dark area contrast ratio.

5.2.3.2 Light Source. The light source shall be selected to optimize spectral compatibility with the selected surveillance system; for example, if the security system includes CCTV observation of the protected area, the light source shall be selected to maximize the spectral sensitivity of the camera tube.

The light source selected for the security lighting system shall have the minimum practical restrike time. The security lighting system shall provide sufficient light to perform its functions within 2 min after the reapplication of power following an interruption. This light level shall be maintained at the end of the maintenance cycle, through the life of the light source, and without any contribution by natural or other artificial light sources.

5.2.3.3 Illumination Reliability. The security lighting system should be designed in such a way that it will continue to perform its functions after a passive failure of the system beyond the security lighting distribution panel.

5.2.3.4 Control. The security lighting system shall be turned on and off automatically. There shall be a manual override(s) to permit an operator to turn the lights on in the event of a failure of the automatic system. There shall be no single location beyond the security lighting distribution panel from which the entire lighting system can be switched off. The security lighting distribution panel(s) shall be located in a protected area.

5.3 Primary Portal Security Lighting.

5.3.1 Requirements. Primary personnel and

vehicle access portals to the protected area require lighting to support security activities and, where applicable, remote surveillance. Lighting for personnel viewing and identification, as well as vehicle searches, is required.

5.3.2 Design Considerations. The system designer shall take into account the following security portal lighting design considerations.

5.3.2.1 Illumination. Portal lighting shall be selected to permit accurate color distinction and shall have a minimum illumination level of 2 fc measured horizontally at ground level throughout lamp life and service conditions.

5.3.2.2 Application. At *personnel only* portals, a minimum 30 ft² area shall be lighted to the minimum illumination level. This 30 ft² area should straddle fence gate portals and should extend out from building portals. Lighting shall be arranged so that it does not present glare to the security personnel.

At vehicle entrances, the lighted area shall encompass 60 ft² on the outside of the portal barrier. Recessed lighting, reflective lighting, or some other means of direct undervehicle lighting (for example, portable hand-held lighting) shall be provided to permit vehicle undercarriage searches. Lighting shall be designed to illuminate the sides and top of all vehicles expected to enter or leave through the portal.

Security information signs at vehicle and personnel entrances should be illuminated to ensure visibility. Sign lighting shall not present glare for security personnel.

5.4 Interior Security Lighting

5.4.1 Requirements. Specific zones within vital areas or doors through vital areas might require lighting for either direct visual surveillance or for remote surveillance.

5.4.2 Design Considerations. The system designer shall take into account the following interior security lighting design considerations.

5.4.2.1 Illumination. A minimum illumination level of 2 fc throughout lamp life and service conditions shall be maintained in areas requiring direct visual surveillance. Usually, normal plant lighting is sufficient for direct visual surveillance; however, this fact should be verified during the design stage.

Areas requiring light for remote surveillance shall have illumination levels and light type compatible with the surveillance equipment.

5.4.2.2 Application. Lamp- and fixture-type selection shall be verified to be acceptable

and approved from a materials perspective for use in the area or location of installation.

Interior lighting for surveillance purposes might be required for particularly sensitive vital areas or for areas requiring frequent or extensive maintenance operations.

Remotely located equipment, or areas vital and nonvital, may warrant lighting for surveillance purposes.

5.5 Implementation. The security lighting design may be either implemented as an independent and dedicated system or be integrated with the general plant outside lighting system. In either case, the security lighting design requirements and hardware details shall be documented in a separate and distinguishable form.

6. Communications

6.1 General. This section establishes minimum requirements to guide the system designer in the design, testing, and maintenance of systems used for communications among the alarm stations, the local law enforcement agency, and members of the physical security force.

6.2 Requirements. The central alarm station and the secondary alarm station shall each have two or more two-way communication paths with each other, the local law enforcement agency, and the plant control room. Single acts of sabotage shall not be capable of severing both communication paths. Availability (that is, operating to meet its intended function[s]) requirements are as indicated in the following paragraphs.

6.2.1 Telephone Availability. The telephone communication path shall have at least 95% availability of operation, with a phone set that is independent of the plant switchboard.

6.2.2 Radio Availability. Plant equipment for local law enforcement agency radio communications shall have at least a 95% availability of operation.

6.2.3 Security Force Communication. All members of the security force shall have the ability for continuous two-way voice communication with the central alarm station, the secondary alarm station, and each other.

6.2.3.1 Availability. Equipment for onsite, two-way voice communication shall have a high percentage availability of operation.

6.2.3.2 Communications Coverage. The onsite security communications system coverage shall be such that the continuous communications requirement will be met wherever the members of the security force would be expected to operate. Localized communication dead zone areas may be acceptable but should be kept to a minimum. Dead zone areas should be identified for security purposes. If a dead zone is sufficiently large, alternate communication means (for example, telephone) should be provided.

6.2.5 Communication Protection. Centralized security communications equipment shall be located in a controlled-access area or protected with locks and tamper-indicating devices.

6.2.6 Antenna Protection. The fixed security radio antenna or antennas shall be located within a protected area.

6.2.7 Intelligence Protection. The security communications system should be either operated or designed so as to limit the amount of intelligence that an outsider can gain from monitoring the net.

6.2.8 Radio Interference Protection. The security communications system should be designed to preclude radio frequency interference from and with plant operating equipment.

6.2.9 Loss of Communication. Upon detection of a loss of one of the available communication paths, repairs are to be initiated immediately. Such repair will diminish the possibility that all communication paths will be out of service at the same time.

7. Patrol Tour Monitoring

7.1 General. If patrol tours are employed, the security officer's progress should normally be automatically logged and documented as patrol tour stations are activated.

7.2 Design Basis. Patrol tour monitoring devices shall be located in areas of the facility that require periodic physical inspection. Factors to be considered by the system designer are number of tours, travel time, number of stations, annunciation, and tour interruption.

8. Access Control

8.1 General. This section describes the minimum scope of the documentation required to

support the development of a security access control system unique to each facility. It describes the relationship between the documentation and the resulting system. The system is described as existing in two parts: access control and detection methods, and the operational procedures. The description of security operational procedures is limited to those features that directly affect hardware design.

8.2 Design Basis Documentation. The security design plan shall consist of three coordinated parts: design basis documentation, operating procedures, and implementing hardware. As a minimum, the following information shall be developed and documented to the extent necessary to permit its effective use in preparing the security system operating procedures and design of access control and associated detection hardware.

8.2.1 Threat Assessment. The security system design basis documentation shall contain a clear description of the postulated sabotage threat. The description shall address as a minimum the following details: the number of adversaries, the involvement of insider(s), the use of weapons, the use of diversion tactics, and the potential objective of the sabotage act (that is, public protest, harm to the facility, harm to the public, etc).

8.2.2 Control List. Based on the postulated sabotage threat, the physical layout of the plant, and the plant process, an analysis shall be carried out to determine the materials, equipment, and areas that are to be controlled in order to prevent a successful act of sabotage. This analysis shall result in a formal list of controlled materials, areas, and equipment. This list shall be used to assist in considering access control and access system requirements in the overall plant design.

8.2.3 Access Control and Detection Design Plan. An access control and detection design plan shall be developed based on the postulated threat and the list of vital equipment, areas, etc. The design plan shall identify all physical features, such as walls, floors, doors, fences, or other barrier elements employed to control access. The design plan shall quantify the degree to which each type of barrier element will restrict access. The design plan shall define the nature of the barrier and the penetration detection equipment employed around each security-vital area. It shall identify all hatches, doors, and removable

panels and indicate the nature of the access control required (that is, normal entrance/exit, emergency exit, maintenance only, etc).

8.2.4 Operational Procedures. The security design plan shall be implemented in two complementary forms: operational procedures and implementing hardware for control of access. The development of these procedures shall be based on the postulated threat, the vital equipment, and the need for legitimate access to vital areas during normal, abnormal, and emergency conditions. It is necessary that the basis security operating modes and all significant variations thereof be identified. The procedures shall cover personal identification, establishment of a need for access, authorization for access, execution of access, and the observation of any abnormal or threatening behavior.

As a minimum, requirements shall be created to permit the following functions under normal conditions:

- (1) Personal identity verification: direct, indirect, or both
- (2) Establishment of access authorization
- (3) Communication of access request and permission
- (4) Revocation of authorization
- (5) Logging of ingress and egress for vital and protected areas

As a minimum, requirements shall be created to permit the following functions under abnormal conditions:

- (6) Personal identity verification
- (7) Access control and portal penetration detection

As a minimum, requirements shall be created to permit the following emergency functions:

- (8) Emergency exit from any area
- (9) Emergency entrance for reasons of personal rescue or fire protection, etc.

8.3 Access Control Hardware. This section describes the minimum functional requirements of hardware when employed in the system to control access of personnel into a vital area. Access control consists of four elements: a barrier that restricts access, a device that communicates a request for access, a device that verifies authorization, and a device that permits access by allowing passage through the barrier.

8.3.1 Operational Access Control Hardware. Access control hardware shall be selected and installed in a manner to complement the access control and detection design plan and the