IEEE Std 692-1997
(Revision of IEEE Std 692-1986)

IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations

Sponsor

**Nuclear Power Engineering Committee
of the
IEEE Power Engineering Society**

Approved 26 June 1997

IEEE Standards Board

Abstract: Criteria are provided for the design of an integrated security system for nuclear power generating stations. Requirements are included for the overall system, interfaces, subsystems, and individual electrical and electronic equipment. This standard addresses equipment for security-related detection, surveillance, access control, communication, and data acquisition.
Keywords: access control, alert, central alarm station, duress alarms, integrated security system, intrusion detection, line supervision, perimeter intrusion alarm, portal security lighting, remote video surveillance, secondary alarm station, security lighting, security systems, uninterruptible power supply (UPS) system, voice communications

---

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

ISBN 1-55937-941-3

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Introduction

(This introduction is not a part of IEEE Std 692-1997, IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations.)

The physical protection and security of nuclear power generating stations concerns utilities, manufacturers, the general public, and those who are responsible for licensing and regulating nuclear power generating stations. The requirements to ensure an acceptable security system at a nuclear power generating station have been evolutionary in nature. This standard is intended to establish both guidance and minimum requirements for acceptable security system design for such nuclear facilities.

The criteria in this standard were developed to provide guidance in determining design features, minimum conditions of operation, and surveillance requirements related to the security system of the nuclear facility. The development of these criteria was undertaken in January 1978, and the standard was originally issued in 1986. This revision has modified the original standard to reflect currently acceptable criteria for security systems and to reflect advancements in security systems equipment technology. These criteria are intended to be used to establish new nuclear power generating station security system designs, and as a guide when making improvements to existing security systems at operating nuclear power generating stations. In either case, safeguards information, developed as a result of the design effort, shall be protected in accordance with existing regulatory requirements.

The focus of this standard is on the various security-related electrical and electronic equipment, including its integration to achieve an acceptable security system. As a result, this standard is not intended to cover all security-related topics. An understanding of the goals and objectives of the security system with an appreciation for the financial, operational, testing, and maintenance functionality of the site will enhance the compatibility of the various plant systems, features, and operator actions required to mitigate events such as radiological, fire, loss of site power, and security events. The plant layout must be compatible with the need to control access and maintain separation of areas due to pipe break accident, missiles, fire, radiation exposure, and flooding considerations. Physical protection measures should be incorporated into the design prior to the start of construction to enhance physical protection and non-obtrusive security system installation and to minimize cost.

Consequently, such features as listed below should be incorporated in the initial design:

— Embedment of card readers/conduit
— Hardened walls, floors, and ceilings
— Bullet-resistant features
— Minimized utility ports
— Utility port barriers
— Security door hardware

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

— Development of threat and response criteria
— Security force composition, deployment, or weaponry
— Classification of vital equipment or vital areas
— Contingency plans
— Security requirements during the plant construction stage
— Personnel screening

The following additional IEEE standards are recommended for use to ensure that quality security systems are engineered, designed, and installed for use in the commercial nuclear industry:

IEEE Std 141-1993, IEEE Recommended Practice for Electric Power Distribution for Industrial Plants (IEEE Red Book) (ANSI).

IEEE Std 142-1991, IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems (IEEE Green Book) (ANSI).

IEEE Std 242-1986 (Reaff 1991), IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems (IEEE Buff Book) (ANSI).

IEEE Std 446-1995, IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications (IEEE Orange Book) (ANSI).

IEEE Std 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (ANSI).

IEEE Std 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (ANSI) [specifically, for additional guidance and references on basic computer system quality and EMI issues].

Future activities for the working group include the following:

— Staying abreast of technological developments in the security area for consideration toward inclusion into this standard.

— Expanding the definitions clause to include terms descriptive of current or future security design features such as seismic-magnetic buried lines and seismic buried lines.

— Evaluating through coordination with the Illuminating Engineering Society of North America (IESNA) the potential for improvement in requirements for security lighting levels (e.g., maximum to minimum ratio to improve camera resolution) and approaches (e.g., horizontal vs. vertical, and ground vs. working level measurements).

— Further improving the consistency of the way in which design basis and its associated documentation are addressed among the various clauses of this standard.

Suggestions for other improvements of this standard are welcomed and should be sent to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Participants

This standard was prepared by Working Group 3.7 of Subcommittee 3, Operations, Surveillance and Testing, of the Nuclear Power Engineering Committee of the Power Engineering Society. At the time this standard was prepared, Working Group 3.7 had the following membership:

David A. Horvath, *Chair*

Stephen Ortiz Douglas E. Thomas Fray Thompson

The Working Group would like to gratefully acknowledge the valuable support provided by Paul Phelps of Virginia Power toward completion of this revision of the standard.

At the time this standard was approved, the members of Subcommittee 3 were as follows:

S. Kasturi, *Chair*

M. R. Allen
G. Ballassi
B. Bharteey
J. L. Edson
W. A. Johnson
D. A. Horvath
S. Ortiz
S. Z. Parsons
J. Taylor
D. E. Thomas
J. P. Vora
C. S. Weary

The following members of the Nuclear Power Engineering Committee were on the balloting committee:

Wes W. Bowers
Dan F. Brosnan
Nissen M. Burstein
Aris S. Candris
S.P. Carfagno
Robert C. Carruth
Robert L. Copyak
Gary L. Doman
Edward F. Dowling
Arthur R. DuCharme
Rich E. Dulski
Jay Forster
J. R. Fragola
John M. Gallagher
Wil C. Gangloff
Louis W. Gaussa
Luis C. Gonzalez
Lawrence P. Gradin
J.K. Greene
Britton P. Grim
Robert E. Hall
Joe T. Hazeltine
Gregory K. Henry
Sonny Kasturi
James T. Keiper
J. Donald Lamont
Alex Marion
John R. Matras
R. B. Miller
Burt Nemroff
Newell S. Porter
Neil P. Smith
Donald J. Spellman
Peter B. Stevens
James E. Stoner
Peter Szabados
James E. Thomas
John T. Ullo
Raymond Weronick
G. O. Wilkinson
Mark S. Zar
James B. Zgliczynski

When the IEEE Standards Board approved this standard on 26 June 1997, it had the following membership:

Donald C. Loughry, *Chair* **Richard J. Holleman,** *Vice Chair*

Andrew G. Salem, *Secretary*

Clyde R. Camp
Stephen L. Diamond
Harold E. Epstein
Donald C. Fleckenstein
Jay Forster*
Thomas F. Garrity
Donald N. Heirman
Jim Isaak
Ben C. Johnson
Lowell Johnson
Robert Kennelly
E. G. “Al” Kiener
Joseph L. Koepfinger*
Stephen R. Lambert
Lawrence V. McCall
L. Bruce McClung
Marco W. Migliaro
Louis-François Pau
Gerald H. Peterson
John W. Pope
Jose R. Ramos
Ronald H. Reimer
Ingo Rüsch
John S. Ryan
Chee Kiow Tan
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal
Alan H. Cookson

Valerie E. Zelenty
IEEE Standards Project Editor

Contents

IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations

1. Overview

1.1 Scope

This standard provides criteria for the design, testing, and maintenance of security system equipment for nuclear power generating stations. Such equipment includes permanently or temporarily installed systems, subsystems, and components used by the security force for physical protection of the station against security threats. It includes equipment for security-related detection, surveillance, access control, communication, and data acquisition.

1.2 Purpose

This standard establishes criteria for the design of an integrated security system for nuclear power generating stations. The criteria assists in the selection and application of equipment to detect, monitor, display, and record security conditions and events. The security system defined here is not intended to be a safety system as defined by IEEE Std 603-1991.

2. References

This standard shall be used in conjunction with the following publications.

IEEE Std 100-1996, IEEE Standard Dictionary of Electrical and Electronics Terms.[1]

IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (ANSI).

[1]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.

3. Definitions

IEEE definitions are found in IEEE Std 100-1996. The following are terms used in this standard:

3.1 access control: The means to allow authorized entry and prevent unauthorized entry of persons, vehicles, and materials into an area.

3.2 acknowledge: Operator action to indicate awareness of an event or alarm.

3.3 alarm: A signal for attracting attention to some abnormal condition. A warning of danger, safeguard threat, equipment failure, or other condition requiring attention.

3.4 alert: A notification to be watchful that shall not be considered the same priority as an alarm.

3.5 badge number: A numeric character code assigned to a badge.

3.6 barrier: An obstruction composed of suitable construction and materials or a time delay mechanism that imposes a delay for an intended purpose.

3.7 card reader: A device used to read a coded credential at an entry point.

3.8 central alarm station (CAS): A continuously manned location that provides primary security system monitoring and communications functions.

3.9 clear: Operator action to remove specific displays.

3.10 degraded mode: When part of the central alarm station equipment is inoperable, causing less then optimal operational conditions.

3.11 detection zone: Any area equipped to sense the presence of an intruder.

3.12 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.

3.13 event: Change of status or condition.

3.14 false alarm: An indicated alarm where no danger, safeguards threat, or equipment failure condition exists.

3.15 inactive mode: When the alarm input is in an unmonitored mode for testing.

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

3.17 isolation zone: Any area, adjacent to a perimeter physical barrier, cleared of objects that could conceal or shield an individual. The inner isolation zone is inside of the perimeter physical barrier; the outer isolation zone is outside of the perimeter physical barrier.

3.18 legitimate access: The proper and correct access authorization.

3.19 nuisance alarm: An alarm warning that does not represent danger, safeguards threat, or equipment failure conditions requiring an actual response.

3.20 patrol tour: An inspection by a member of the security organization along a predetermined route to observe the route area’s security conditions.

3.21 physical security: The application of methods for preventing malevolent acts against safeguards and security interests, detecting such acts as they occur, and responding to such acts.

3.22 protected area (PA): A controlled-access area encompassed by physical barriers.

3.23 safeguards: Security measures for the physical protection of nuclear material and vital equipment at a nuclear power generating station.

3.24 secondary alarm station (SAS): A continuously manned location that is capable of providing backup security system monitoring and communications functions.

3.25 security system: As used in the context of this standard, the aggregate assemblage of hardware and associated software 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.

3.26 tamper: To interfere with the performance of a security sensor or the electrical connections within an alarm communications system.

3.27 trouble: Equipment malfunction or loss of power.

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

3.29 vital area: An area that contains vital equipment.

3.30 vital equipment: Any equipment, system, device, or material, the failure of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems that would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital.

4. Integrated security system

4.1 General

This clause provides the overall requirements and equipment interfaces for an integrated security system. Criteria that are specific to the various individual types of equipment (or subsystems) that comprise the overall security system are provided in 4.2 through 4.5.

4.2 List of security system equipment (or subsystems)

The types of security system equipment (or subsystems) that shall be included in an integrated security system and that are addressed by this standard are as follows:

a) Perimeter intrusion alarm
b) Security lighting
c) Remote video surveillance
d) Access control
e) Interior intrusion detection
f) Data acquisition, processing, and display
g) Voice communications
h) Line supervision

i) Duress alarms
j) Power supplies

Also included in an integrated security system are equipment interconnecting cables and raceways and power distribution systems.

4.3 Performance requirements

An integrated security system shall be capable of detecting, delaying, and responding to threats to the physical security of the nuclear power generating station, such that the physical protection objectives for that facility are met.

4.3.1 Integrated security system interfaces

A typical arrangement of the interfaces among security system equipment (or subsystems) is illustrated in Figure 1.

4.3.2 Physical protection elements

Determination of the physical protection objectives and analysis of the system adequacy to meet them are not within the scope of this standard but are important related elements of plant security. The relationship of physical protection elements and illustration of those that fall within the scope of this standard are shown in Figure 2.

4.3.3 Security areas

The security system design encompasses many areas of the plant. Figure 3 is a diagram of typical security areas and features. The security system design would also typically include the use of barriers to protect against the malevolent use of vehicles to gain unauthorized access to nuclear power generating stations.

4.4 Design basis

The security system at nuclear power generating stations shall be engineered, designed, manufactured, constructed, and operated in accordance with documents that specify the design basis and requirements of the subsystems and components included in the integrated security system. Some of these documents are listed in the bibliography of this standard (see Annex A). Other documents are specific to each site and installation. Security equipment, both indoor and outdoor, should be sufficiently protected against lightning strikes and resulting surges, such that equipment failure or malfunction is minimized to the extent economically feasible but not allowing reliability to be detrimentally affected.

4.5 Functional design verification

Engineering and design shall be reviewed by cognizant personnel other than the originators. Equipment and subsystems shall be tested and verified to meet the requirements of the subsystem/component specifications by cognizant personnel other than those persons directly involved in the manufacture or construction of the equipment or component. The system shall be factory tested to ensure operability of the system prior to shipping. The integrated system, upon installation, shall be tested and verified to meet the integrated system specifications by cognizant personnel other than those persons directly involved in the construction of the integrated system and the verification shall occur before the integrated system is placed into operation. Subsystems shall be operated, tested, and maintained in accordance with the manufacturer’s recommendations unless otherwise justified. Modifications to the subsystems and components shall be subject to the same level of design specification and verification as the original subsystem unless otherwise justified.

The security system at a nuclear power station is not subject to the quality assurance criteria for safety-related equipment in nuclear power plants, contained in the Code of Federal Regulations, Part 50, Appendix B (see [B30]).[2]

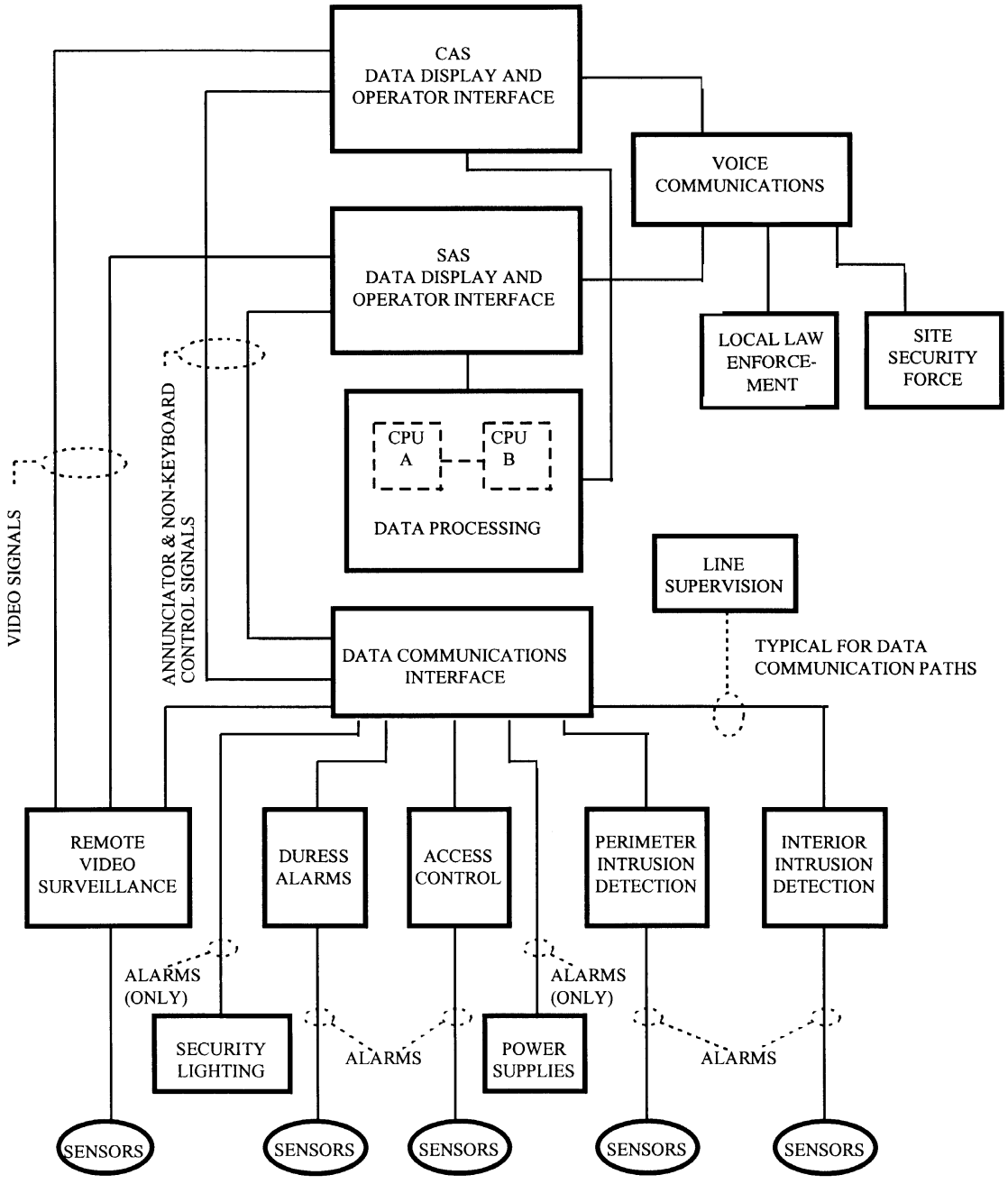

Figure 1—Integrated security system interfaces

[2]The numbers in brackets correspond to those of the bibliography in Annex A.

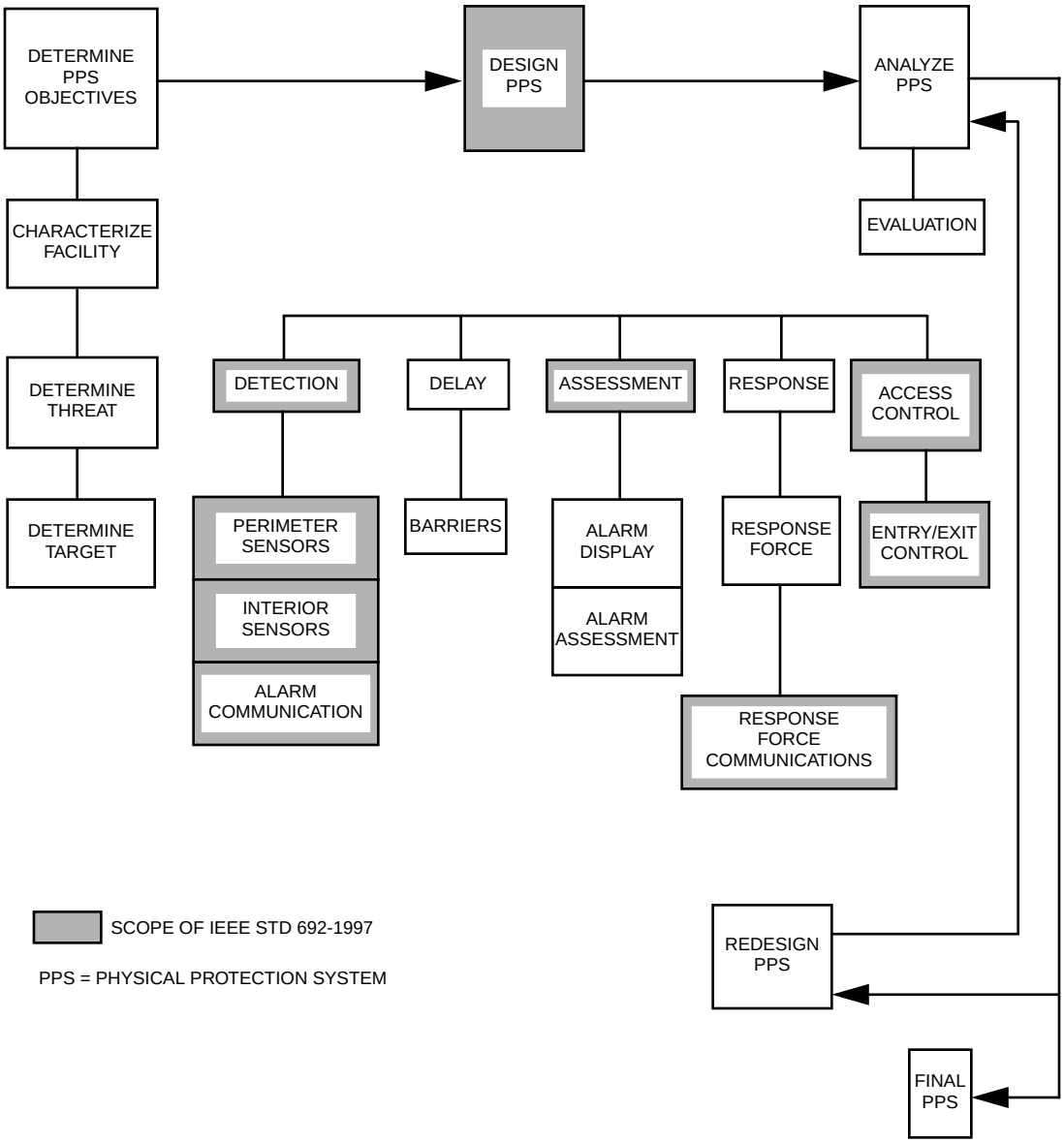

Figure 2—Physical protection elements

5. Perimeter intrusion alarm system

5.1 General

A perimeter intrusion alarm system must consider site-specific evaluation, performance requirements, and safeguards. A perimeter intrusion alarm system is used to detect entry into or through the isolation zone (consists of inner and outer isolation zone) and to initiate an alarm signal.

5.2 Description

Some types of perimeter intrusion alarm system sensors that have been found acceptable are

a) Microwave sensors
b) Electric-field (E-Field)
c) Seismic-magnetic buried-line
d) Seismic buried-line
e) Magnetic buried-line
f) Disturbance (fence)
g) Point
h) Infrared
i) Ported coaxial cable
j) Video motion detection
k) Breakwire system
l) Fiber optic

The acceptability of any sensor shall be determined by site-specific evaluation, performance requirements, and safeguards as discussed in 5.3 through 5.5.

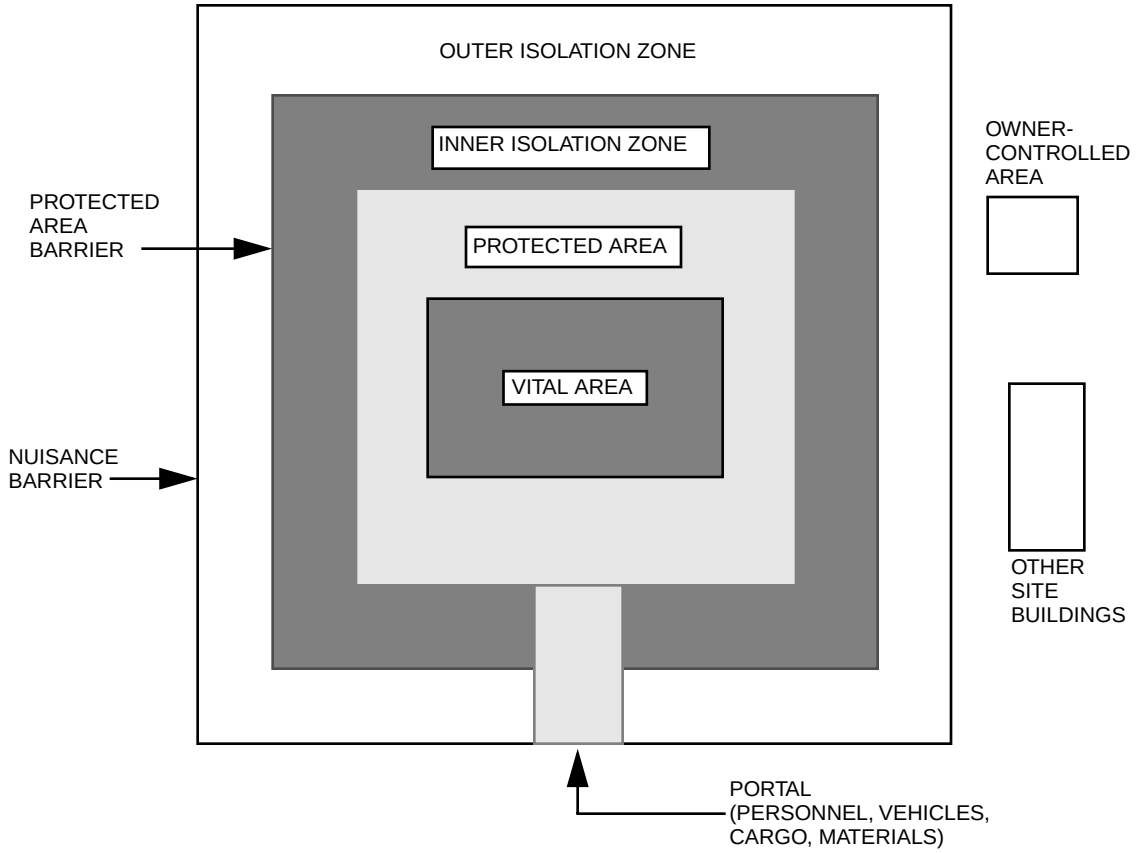

Figure 3—Typical security areas

5.3 Site evaluation

A comprehensive site evaluation shall be conducted to select perimeter intrusion alarm system sensors. Site conditions that can affect perimeter intrusion alarm systems include, but are not limited to, the following:

a) Topography
b) Vegetation
c) Wildlife
d) Background noise
e) Climate and weather (rain, sleet, snow, fog)
f) Soil and pavement
g) Traffic patterns (air and ground)
h) Size and location of the protected area (PA)
i) Salt spray
j) Electric and magnetic fields
k) Sun angle

The intrusion detection system shall be located or designed such that topographic features that affect the detection and assessment systems are minimized. The sensitivity of the sensors shall be compatible with the site conditions. Topographic features that should be considered when selecting and locating sensors are steep slopes, gullies or ditches, waterways, and surface water.

Vegetation, which can degrade sensor performance, shall be minimized.

Potential adverse effects of wildlife shall be considered. Wildlife can cause nuisance alarms and sensor damage. Control can be enhanced with fencing or repellents.

Potential sources of audible, inaudible, and electromagnetic background noise, which are variable and difficult to control, shall be identified. Sensors shall be selected or protected such that they are not functionally degraded by the identified background sources.

Climate and weather (rain, sleet, snow, fog) shall be considered in the selection, location, and mounting of electrical equipment. Appropriate equipment enclosures, mounting configurations, and temperature rating shall be specified. The use of equipment heating and/or cooling devices shall be considered. The use of wipers on camera lenses shall also be considered.

Soil and pavement considerations shall be compatible with the operational requirements of the sensors and selected to minimize nuisance alarms. Splashing water, bouncing hail stones, and puddling water can be sources of nuisance alarms.

Traffic pattern and ground vibration shall be compatible with the operational requirements of the sensors and designed to minimize nuisance alarms. Vehicular and personnel traffic may introduce devices that cause electromagnetic background noise, and vehicles may cause splashing of water or bouncing of stones. These can all be a source of nuisance alarms. Traffic patterns shall also be considered in the layout of CCTV cameras for assessment. Lights from vehicles on nearby roadways can temporarily blind a camera if shined directly into the camera.

The size and location of the PA will influence the quantity of sensors, the size of the security system, and the ultimate cost of installation, ongoing maintenance, and replacement (life cycle costs). The size and location of the PA shall not impede the operational, testing, and maintenance functions at the site and shall be compatible with the goals and objectives of the site.

Effects of electrical noise from electromagnetic fields shall be mitigated. Sensors shall be selected or protected such that they are not functionally degraded by electrical noise. Sources of electrical noise could be such items as overhead power lines, power transformers, walkie-talkies, and hand-held radios.

Salt spray, where applicable, shall be considered in the selection, location, and mounting of electrical equipment. Appropriate equipment enclosures and mounting configurations shall be specified.

Care shall be taken when determining the layout for CCTV cameras so that the sun does not adversely affect their operation. Low sun angles such as those found during sunrise and sunset could cause the camera to face directly into the sun, thereby eliminating the usefulness of the camera during this period.

5.4 Performance requirements

5.4.1 Location

The location of exterior sensors shall be chosen to maximize the detection capability and minimize the nuisance and false alarm rates. Sensors shall be located between perimeter double barriers (typically the outside barrier is a nuisance barrier and the inside barrier is a protected barrier) whenever possible. The sensors shall be located at a height and distance to prevent the use of the barrier or barriers to easily circumvent detection.

The sensors shall be installed to provide detection of individual segments (often referred to as zones) of the perimeter; overlapping detection of adjoining segments shall be provided unless otherwise justified. The individual segments shall be limited to a length that allows observation of the entire segment for assessment purposes. Assessment may be provided either by a person responding to the location of an alarm or by the use of CCTV.

5.4.2 Probability of detection

The selection and placement of sensors shall provide a perimeter intrusion alarm system with at least 90% probability of detection in each segment with a 95% confidence level. Periodic tests of sensors shall be conducted to validate the area of detection and the probability of detection within this area. The sensor shall be capable of detecting an intruder weighing a minimum of 77 lb (35 kg) passing through the detection zone at a rate between 0.5 ft/s and 16 ft/s (0.15 m/s and 5 m/s).

Under normal environmental conditions, the total perimeter alarm system shall not average more than one false alarm per week per segment or alarm point and not more than one nuisance alarm per week per segment or alarm point while maintaining proper detection sensitivity. Multiple false alarms, nuisance alarms, or both, caused by one transient event shall be considered as a single alarm. A second sensor may be installed to reduce the nuisance alarm rate to ensure 90% probability of detection in all varieties of environment. The sensor selected shall be complementary to the sensor that is already installed (e.g., a microwave combined with a fence sensor so different methods must be used on each sensor to circumvent the perimeter alarm system).

Where the segment can be fully observed at all times, either visually or by CCTV, the false alarm rate and nuisance alarm rate can be increased to one alarm per day per segment or alarm point.

Alarm rate averages are intended to identify trends and shall be determined quarterly.

5.4.3 Alarm conditions

The perimeter intrusion alarm system shall initiate an alarm signal upon introduction of a stimulus or a condition into the area of coverage for which the sensor was designed to detect.

5.5 Tamper protection

Tamper switches or other triggering mechanisms shall be provided for the sensors and associated equipment enclosures that are not self protected or not located within a sensor's area of detection. These tamper devices shall initiate a tamper signal upon detection of a stimulus or condition (e.g., removing a cover) for which it was designed to react. These devices shall be supervised in accordance with Clause 12.

6. Security lighting

6.1 General

The criteria for the design and installation of security lighting is limited to the security application of lighting. The criteria do not replace existing standards concerning the lighting requirements for health and safety, lighting equipment design, or installation. 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 shall be documented as part of the integrated security system design. The security lighting system supports the surveillance, threat assessment, and adversary engagement functions of the facility's security force.

6.2 Outdoor security lighting

6.2.1 Locations

Outdoor security lighting shall be provided for the isolation zones and all outdoor areas of the PA, including rooftops within 18 ft (5.4 m) of grade, and higher rooftops if direct unsecured exterior or interior access (e.g., ladders, cable raceways, pipes, stairwells) is available. The power distribution panel(s) for outdoor security lighting shall be located within the PA. 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 PA 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.

6.2.2 Illumination

Outdoor security lighting shall provide an illumination level sufficient to permit unimpaired observation by direct visual and CCTV methods throughout lamp life and service conditions.

The minimum light level throughout the PA shall be 0.2 fc (2.2 lx) measured horizontally at ground level; the optimum level is a site-specific level. 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 328 ft (100 m): the presence of a person [5 ft high (1.5 m), 9 in thick (23 cm)]; the physical action of the person (e.g., lying, crawling, standing, walking, running); and the direction of the action. The security force shall be able to perform PA perimeter patrol tour duties without supplementary lighting. The light level shall also be sufficient to permit proper surveillance system operation. Appropriate consideration shall be given to reflectances, glare factors, climatic conditions, CCTV camera minimum light level, uniformity of lighting, and light-to-dark area contrast ratio to verify that these conditions will not adversely affect the usefulness of the CCTV cameras for surveillance or assessment purposes. See 7.2.3 for further details.

6.2.3 Light level uniformity

If CCTV is used for surveillance and assessment then uniform levels of lighting and consistent type of lighting shall be used throughout each alarm segment in order to provide for the optimum operation of the cameras.

6.2.4 Light source

The light source shall be selected to ensure spectral compatibility with the CCTV system.

6.2.5 Illumination reliability

The failure mode, affects, and restoration efforts associated with security lighting shall be analyzed to determine the period of time to be tolerated without significantly affecting the operation of the security system. This period of time should be based on data from the threat analysis conducted for the facility. Backup power should be considered.

6.2.6 Illumination control

Outdoor security lighting shall be switched on and off automatically. There shall be a manual override to permit an operator to switch the lights on in the event of a failure of the automatic system. The manual override switch shall be located in the central alarm station (CAS), secondary alarm station (SAS), or a vital area.

6.2.7 Restart after power interruption

Outdoor security lighting shall provide sufficient light for assessment of alarms or surveillance within 2 min (maximum) following a power interruption. Backup power or supplementary lighting for the detection zones during power interruptions should be considered for areas most critical for the protection of assets (facilities and personnel). Sufficient light shall be maintained at the beginning of the operation cycle and throughout the life of the light source. It is recommended that no total loss of lighting occur in all isolation zones at any one time due to a common mode failure of equipment located within the PA under expected plant conditions.

6.2.8 Lighting structures

When towers, poles, masts, or other structures are used to support lighting fixtures and/or other related equipment, they shall be designed to withstand the plant’s expected wind and ice conditions during all seasons of the year (excluding hurricanes and tornadoes). The perimeter lighting structures shall be located to prevent the use of the lighting structure to easily circumvent the intrusion detection system.

6.3 Primary portal security lighting

6.3.1 Locations

Primary personnel and vehicle access portals to the PA require lighting to support security activities and, where applicable, remote video surveillance. Lighting for personnel viewing and identification, as well as vehicle searches, shall be provided.

6.3.2 Illumination

Portal lighting shall permit accurate color distinction and shall have a minimum illumination level of 2 fc (22 lx) measured horizontally at ground level throughout lamp life and service conditions.

6.3.3 Coverage

At personnel-only portals, a minimum 30 ft^2 area (e.g., 3 ft × 10 ft) [3 m^2 (0.9 m × 3 m)] shall be lighted to the minimum illumination level of 2 fc (22 lx) measured horizontally at ground level throughout lamp life and service conditions. This 30 ft^2 (3 m^2) area shall straddle fence gate portals and shall extend out from building portals. Lighting shall be arranged so that it minimizes glare to the security personnel and is compatible with the CCTV system. At vehicle entrances, the lighted area shall encompass 100 ft^2 (9 m^2) on the outside of the portal barrier and shall have a minimum illumination level of 1 fc (11 lx) measured horizontally at ground level throughout lamp life and service conditions. Recessed lighting, reflective lighting, or other means of direct under-vehicle lighting (e.g., 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 shall be illuminated to ensure visibility. Sign lighting shall not present glare for security personnel and shall be compatible with the CCTV system.

6.4 Interior security lighting

6.4.1 Requirements

Vital areas or doors through vital areas shall be lighted for either direct visual surveillance or for remote surveillance, as applicable.

6.4.2 Design considerations

The system designer shall take into account the interior security lighting design considerations in 6.4.2.1 and 6.4.2.2.

6.4.2.1 Illumination

A minimum illumination level of 0.5 fc (5.4 lx) measured horizontally at the floor level 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 shall be verified during the design stage.

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

6.4.2.2 Application

Lamp type and fixture type shall be compatible from a materials perspective for use in the area or location of installation.

7. Remote video surveillance

7.1 General

A remote surveillance system that is suitable for the protection of nuclear power generating stations against the design basis threat shall be established. To facilitate the initial response to PA penetration and assessment of the existence of a threat, capability of observing the isolation zones and the physical barrier at the perimeter of the PA must be provided, preferably by means of CCTV or other suitable means that limits the expo-

sure of responding personnel to possible attack. The information displayed in the CAS and SAS is required to assess the cause of an alarm and the existence of a threat by observing the isolation zones and the physical barrier at the perimeter of the PA and the various personnel, vehicle, and cargo access portals. The remote surveillance system is also useful in assessing the nature and potential threat of activities in other areas of the site. The integration of both electronic surveillance technology and security personnel into the surveillance program is essential to the success of the security program. A human factors review of the alarm stations will ensure that monitors are properly sized and located, and that quality scenes are displayed for operator assessment.

The display image of the conditions in the detection zone at the time of any perimeter alarm shall enable the operator to assess the cause of the alarm and the nature of the potential threat. The display image from the vehicle portal and of the security officer inspecting the vehicle shall enable the operator to assess the existence of any coercive influence on the security officer.

7.2 Performance requirements

The remote surveillance system shall be operational 24 hours a day. The system shall remain usable under normal (expected) environmental conditions. Abnormal conditions (hurricanes, tornadoes, snow and ice storms, probable maximum precipitation and wind intensities) occur at random for a limited period of time and may degrade the system's capabilities.

The CCTV system shall be compatible for use with other systems such as lighting, power distribution, and detection devices.

7.2.1 Coverage

The CCTV system shall provide the operator(s) with an unrestricted view of the detection zones and the vehicle portal. Unrestricted means there shall be no obstructions large enough for a person to hide behind while in the detection zone viewed by the camera(s). An acceptable exception is a blind spot if it is smaller than the profile of a human 5 ft high by 9 in thick (3.75 ft^2) [1.5 m high by 23 cm thick (0.35 m^2)].

A camera's field of view shall be limited to that distance beyond which the operator cannot interpret the nature of an object. This means the operator's ability to determine that the object is or is not human when moving, standing, or lying in any position and assessing the behavior or actions of the object. The surveillance system's minimal acceptable limit of resolution is defined as a 1 ft (0.3 m) high object occupying no less than 1% of the horizontal field of view. [This can also be stated as a scene having a width of no more than 100 ft (30 m).]

Fixed cameras shall be provided to cover the entire width and length of the detection zone. This shall provide the operator(s) with an immediate view of any portion of the detection zone in which an intrusion alarm has occurred. This shall include the sides and tops of buildings or any other structure that is located in the detection zone. The following features shall also be provided:

a) Some cameras shall be equipped with pan/tilt/zoom (PTZ) equipment to assist in checking exterior areas within the PA. The limit of resolution shall apply with the zoom lens at its narrowest setting.

b) The CCTV system shall permit the operator to view the vehicle portal(s). At least one camera (per portal) shall be equipped with PTZ controls with sufficient resolution to permit close supervision of the inspecting officer.

c) The field of view of fixed cameras shall be coordinated with the perimeter intrusion alarm system sensor locations such that no more than two cameras shall be required to view the entire detection zone. To the extent practical, the numbering sequences for fixed cameras and zones shall be oriented in the same direction (clockwise or counterclockwise) around the perimeter.

7.2.2 Display

The CAS and SAS shall have the same video capabilities and controls.

A video switcher shall be provided to permit manual or automatic video display of any camera and manual or automatic control of any PTZ control mechanism. Each operator shall have independent control of all functions. (Simultaneous control of the same PTZ camera is excluded.)

The system shall respond to perimeter intrusion sensor alarms by simultaneously displaying all cameras required to observe the alarmed zone. This response shall override any operator action and control shall be returned to the operator(s) as soon as the display is switched on.

Video displays called-up in response to an alarm shall be displayed on monitors in front of the operator's normal station. The monitor size shall be selected based upon a human factors review of the alarm stations. The proper sizing and location of the monitors shall assure that the scenes displayed meet the requirements for operator assessment. The operators may access these monitors by manual control.

The scenes from all cameras shall be displayed sequentially. This shall be called a rotating display. It will be presented to the operator on a group of rotating display monitors. All scenes on all of the rotating display monitors shall change at the same time. Each display duration shall last for no less than 3 s plus one additional second for each monitor in excess of two. The monitor size shall be selected based upon a human factors review of the alarm stations. A single security operator shall not be required to observe a rotating display containing more than ten monitors. A dedicated monitor shall be used to observe the scene of the PTZ camera at the vehicle portals.

7.2.3 Scene illumination

Sufficient lighting shall be provided to permit 24 hour a day operation without loss of image resolution. The variation of the illumination level within the scene shall not conceal or hide images or activity from view on the monitor. An acceptable design limit for the light-to-dark ratio is 6:1. See 6.2.2 for additional lighting requirements.

These design requirements (and the associated illumination calculations, if developed) shall assume

- Only lights supported by the security system power supply are available
- The end of life and dirty fixture output of all luminaries
- The failure of any one luminaire contributing to a scene
- The camera sensitivity required for full video output
- The minimum luminaire operating voltage
- The lens "f" stop
- The glass transmission factors
- The minimum illumination level within the scene

7.2.4 Camera placement

The design of the CCTV system shall consider placement of CCTV cameras on existing building structures and dedicated towers. Towers and structures used to support remote surveillance cameras and/or other related equipment shall be designed to withstand the plant's expected wind and ice conditions during all seasons of the year (excluding hurricanes and tornadoes). Towers shall be located to prevent the use of the tower to easily circumvent the intrusion detection area.

7.2.5 Video power

Unless a separate synchronization signal is distributed to the cameras, the security system ac power line shall be used for system synchronization. All video equipment shall be powered from the same single-phase source to provide their synchronous pulses in phase with each other.

7.2.6 Video recorder

A video recorder or other type of image capture system is not required; however, one should be considered as a means to review events and as a training tool. It should simultaneously capture the view from each camera associated with a perimeter alarm.

7.2.7 Time/date/zone

All video displays shall include the current time and date. This may be applied to the video by the video switcher. All video displays shall include the camera identification and/or the alarm zone number. The displayed information shall be sufficient to determine the geographic location of the video scene. This shall be introduced into the display by the video switcher or it shall appear as a label in the actual scene.

7.2.8 Signal transmission

Video transmission systems shall be designed to minimize environmental degradation. In particular, when cables are installed directly underground in ducts and conduits, the effects of moisture and water, signal bandwidth and attenuation, volume of conductors, electromagnetic interference, radio frequency radiation, lightning and surge voltages, and normal plant radiation levels in the selection, installation, and maintenance of the video signal transmission system shall be considered.

7.2.9 Surge protection

Cameras that may be subject to lightning strikes shall be isolated from the remainder of the video system by an appropriate energy limiting device or an optic transmission medium.

7.3 Minimum equipment standards

An acceptable system shall be based on complete technical specifications including compliance with Electronic Industries Association (EIA) standards for cameras and monitors. The enclosures (outdoor use) shall be appropriate for the environmental conditions at the site, including spray from cooling towers.

7.4 Documentation

An adequate remote surveillance system design shall include the following documentation:

a) *Limit of resolution.* Calculations showing the dimensions of the field-of-view for each camera lens size and mounting elevation based on the limit of resolution established in the design criteria.

b) *Camera coverage.* Drawings showing the coverage of the detection zones, including the fence locations and camera mounting locations.

c) *Camera coordination.* Drawings showing the relationship of the camera scenes and the perimeter intrusion alarm zones.

8. Access control

8.1 General

The development of a security access control system is unique to each facility. The system is described as consisting of two parts: access control and detection methods, and operational procedures. The description of security operational procedures is limited to those features that directly affect hardware design. Access control shall not excessively impede the operational, testing, and maintenance functions at the site and shall be compatible with operator actions to mitigate events such as radiological, fire, loss of site power, and security events.

8.2 Design basis documentation

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:

a) *Threat assessment.* The security system design basis documentation shall contain a clear description of the postulated sabotage/intruder threat.

b) *Control list.* Based on the postulated 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.

c) *Access control and detection design plan.* The access control and detection design plan shall identify the means and features to permit legitimate access to and from the PA of personnel, packages, cargo, and vehicles. The means and features shall address such issues as search for unauthorized materials and devices, detection and alarms, doors, gates, turnstiles, search areas, etc.

d) *Operational procedures.* The security design plan shall be implemented as operational procedures and implementing hardware for legitimate access to protected and vital areas. The development of these procedures shall be based on the postulated threat, the vital equipment, and the need for legitimate access to protected and vital areas during normal, abnormal, and emergency conditions.

8.3 Access control hardware

Access control consists of the following four elements:

— A barrier that restricts access
— A device that communicates a request for access
— A device that verifies authorization
— A device that permits authorized 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 operational procedures. Equipment design requirements and location shall be based on the design basis documentation.

8.3.2 Access control barrier

The design of electrical control devices for each door, hatch, portal, etc. identified as part of a barrier to restrict access into the PA and vital areas shall be selected and installed on the basis of providing physical penetration resistance consistent with the postulated threat, in addition to structural requirements outside the scope of this standard.

8.3.3 Access request

Access requests are transmitted to a point where the request is processed and recorded. The function of the access control equipment is to verify the identity of the individual or access control device, as applicable, requesting access and to verify that the individual is authorized access to the area. The means of verifying the identity shall have a 99% probability of detecting an impostor and a nuisance or false rate of rejection of less than 2%. The identity verification techniques shall be compatible with the environmental conditions and provide access in a time appropriate for the portal.

The following acceptable means shall be included in a system for implementing access requests:

a) *Personal identity verification.* At the entrance to the PA, means to verify identity shall be utilized to effect a direct measurement of some unique and unalterable human characteristic; this activity may be performed by a security officer. The verification technique shall be compatible with the plant's environmental conditions of dirt, contamination, protective clothing, etc. Identity verification time shall be considered in the design and selection of methods and equipment.

b) *Access control identification device.* A device (e.g., a card for a card reader) used to communicate the user's identity and access request to the access control system, which shall meet the following requirements:

— It shall contain identity information in a coded format that shall resist detection and duplication.

— The identity codes shall be distributed on a random basis among those authorized to have access.

— It shall be designed and installed to resist nondestructive covert manipulation for surreptitious entry by an expert using any tools available in the facility for less than the duration of routine surveillance in the area.

— It shall resist any form of physical attack carried out in ignorance of the correct code, including total destruction of the reader without causing the associated access control device to unlock or open.

— It shall transmit a valid tamper signal to the access control system in sufficient time to prohibit access request authorization.

— It shall resist failure by manipulation that would transmit an apparently valid request to the access control system.

c) *Access actuating device.* A device in or on a barrier element to permit control of access into the PA and vital areas by the access control system. The device shall

— Be considered in the design of the barrier.

— Not constitute a weakness in the penetration resistance of the barrier element.

— Incorporate devices to monitor each of the true access conditions of the barrier (open, closed, locked, unlocked, and tamper).

— Be provided with an external mechanical override with automatic alarm-initiating device (at least on each vital area barrier).

— Be compatible in design with the need for emergency egress (crash-bar override).

— Allow for incorporation of normal personnel egress from the PA by a "one way out" portal equipped with "log-out" capabilities.

9. Interior intrusion detection

9.1 General

Interior intrusion detection shall cause an alarm signal upon passage of an intruder through the boundary of a controlled access area, or upon movement of an intruder within a normally unoccupied controlled access area. A controlled access area could consist of a closed structure, a room within a closed structure, or a clearly demarcated area within a closed structure. An unoccupied area is not regularly visited or inhabited by authorized personnel.

9.2 Description

Some types of interior intrusion detection sensors that are considered acceptable include

a) Ultrasonic
b) Microwave
c) Infrared
d) Sonic
e) Capacitance
f) Vibration
g) Door and window
h) Pressure
i) Video monitor detection

The acceptability of any sensor is based upon site-specific evaluation performance requirements and safeguards as discussed in 9.3 through 9.5.

9.3 Site evaluation

A comprehensive site evaluation shall be conducted to select interior intrusion detection sensors. Site conditions that can affect interior intrusion detection systems include

a) Structural or area configuration
b) Personnel and vehicle traffic
c) Objects in motion
d) Movable objects
e) Background noise
f) Environment
g) Air movement

The size and shape of the controlled access areas, the penetration resistance of the physical barriers, and the types of openings in the physical barriers should be considered.

Personnel and vehicle traffic during normal plant operation, emergencies, and peak maintenance periods shall be considered. Identifying traffic patterns will assist the designer in determining which openings require access control.

Objects in motion such as operating equipment, in the controlled access area and possibly outside the controlled access area, can initiate alarm signals. Limited pattern coverage to protect only the key areas is necessary.

The interior intrusion detection system shall be designed so that movable objects, such as cranes or cargo, will not degrade the effectiveness of the detection sensors. Potential sources of audible, inaudible, and electromagnetic background noise, which is variable and difficult to control, shall be identified. Sensors shall be selected or protected such that they are not functionally degraded by the identified sources.

Normal and abnormal environmental conditions shall be considered in the selection of the sensors to be used. The sensors shall function properly over the entire normal environmental range. Environmental conditions that can affect sensor operation include pressure, radiation, relative humidity, and temperature.

9.4 Performance requirements

9.4.1 Location

The location of sensors shall be chosen to maximize the detection capability and minimize the nuisance and false alarm rates. The sensors shall be located so as to prevent the use of adjacent structures or objects to circumvent detection.

9.4.2 Probability of detection

The selection and placement of sensors shall provide an interior intrusion detection system with at least 90% probability of detection with a 95% confidence level. Sensors shall be capable of detecting an intruder weighing a minimum of 77 lb (35 kg) passing through the detection field or barrier at a rate between 0.5 ft/s and 16 ft/s (0.15 m/s and 5 m/s).

9.4.3 Alarm conditions

Interior intrusion detection sensors shall initiate an alarm signal upon detection of a stimulus or a condition for which the sensor was designed to react.

9.5 Tamper protection

Tamper switches or other triggering mechanisms shall be provided for the sensors and associated equipment enclosures, where applicable. These tamper devices shall initiate a tamper signal upon detection of a stimulus or a condition (e.g., removing a cover) for which the device was designed to react. These devices shall be supervised in accordance with Clause 12.

10. Data acquisition, processing, and display

10.1 General

The security system shall accurately gather data from remote devices, analyze the data in a timely manner, and display required information concisely and comprehensively.

Consideration must be given to the flexibility and level of security provided for performing data acquisition, processing, and display functions. The designer shall consider future expansion capability in the original design. The system shall also incorporate human engineering features that facilitate meaningful operator interaction.

10.2 Data acquisition

Rapid, reliable, and accurate transmission of information from remote devices to a central location(s) for processing is essential to the security system design.

10.2.1 Design consideration

The system designer should consider the following data acquisition design considerations:

a) *Location of remote devices.* The selection of the type and method of transmission should consider the vulnerability associated with the distribution of the remote sensors and the distance and terrain over which the transmission is to occur.

b) *Speed.* The rate at which a change of state at a remote device is transferred to the security computer system shall support the system's ability to respond to alarms in less than 1 s. The condition where all devices supported by this communication link are in alarm at the same time must be reported within 1 s.

c) *Reliability.* The method of data acquisition shall employ techniques to ensure that a proper signal is transmitted every time the remote sensor detects a condition for which it was designed to react, regardless of the length of time between activations. A single signal path or component failure (e.g., short or open circuit) shall not cause the loss of communications with more than one sensor point or signal transmission point. Dual communication circuits shall be employed for any link carrying alarm signals from more than one alarm location. Self-checking, error detecting, or error correcting techniques shall be utilized to identify errant operation or improper signals and to minimize nuisance alarms due to adverse environmental conditions.

10.3 Signal processing

Information received from remote devices shall be converted into a format that can be used by other portions of the security system and the CAS and SAS operators. The speed and reliability of this conversion shall be compatible with overall system performance requirements.

10.3.1 Design considerations

The system designer shall take into account the signal processing considerations in 10.3.1.1 through 10.3.1.6.

10.3.1.1 Speed

The internal processing times, data transfer rates, and display refresh times shall support a time from alarm signal occurrence to annunciation of 1 s or less.

10.3.1.2 Reliability/maintainability

The signal processing equipment shall employ self-checking provisions to identify errant operation. Redundant processors shall be provided to ensure reliable system operation in the event of a single failure and during maintenance efforts on one of the processor systems. Each processor system shall monitor the status of the other and report any errors detected. The automatic switchover logic shall be designed to avoid contention for master processor status. Alarm reporting terminals and printers must be automatically connected to the master processor. Signal processing equipment shall be modular in design to facilitate maintenance.

10.3.1.3 Priorities

The computer program logic or other signal processing technique used shall give highest priority to alarm signal conditions. An alarm signal that is being reported cannot be replaced by a higher priority alarm signal. Provisions for handling overflow conditions shall be included in the signal processing system.

10.3.1.4 Security

A means shall be provided to restrict access to the computer system. This includes both hardware and software. The computer system shall be located in a controlled-access area. Terminals not located in a controlled-access area shall have limited functionality consistent with the security plan. All terminals shall require, as a minimum, password log-on procedures. Additional protective features such as password entry with the command, key switch enable, dual operator verification, or similar procedures shall be considered for selected sensitive functions. All operator transactions shall be logged with the name of the person initiating the transaction. The system shall not allow this file to be edited, except in a controlled, verified manner defined in the site security plan.

10.3.1.5 Expansion

The security computer system shall have the capability to incorporate additional monitored points. The security computer system should be purchased with greater than the anticipated operational requirements. (Experience has shown that a minimum capacity of 50% greater than the anticipated operational requirements is prudent.)

10.3.1.6 Report generation

Automatic log generation capability shall be provided. The recall capability of stored data shall be flexible to permit presentation of a wide variety of information. The system shall have the capability to allow on-line design and generation of custom log summaries to meet future needs. The printing of log summaries and reports shall not be restricted to a single printer.

10.4 Data display

The first consideration for data display is to determine what information is required. Once this determination is made, the type and format of display can be selected. The CAS and SAS operators' overall work load, comprehension, and environment are human factors that influence display complexity and presentation.

10.4.1 Design considerations

The system designer shall take into account the data display considerations in 10.4.1.1 through 10.4.1.7.

10.4.1.1 Locations of local/remote devices

The type and method of data to be displayed shall be determined. A human factors review shall be performed in order to enhance operability and visibility of the data displays.

10.4.1.2 Display times

The internal processing times, data transfer rates, and data display refresh times shall support a time from alarm signal occurrence to annunciation consistent with the location of the remote display device and the overall system's ability to successfully assess and display an alarm signal and shall agree with 10.3.1.1.

10.4.1.3 Reliability

The method of data display shall employ techniques to ensure that the display is activated every time a sensor transmits the designated signal to the display device. When multiple alarms from the same point or zone occur in rapid succession with no intervening alarms, they shall activate the display as a group, rather than on an individual basis. Backup or redundant display equipment shall be provided to ensure system operation in the event of a single failure. Data display equipment shall be modular in design to facilitate maintenance.

10.4.1.4 Priorities

The data display shall give highest priority to alarm signal conditions. An alarm signal that is being reported cannot be replaced by a higher priority alarm signal. Provisions for handling overflow conditions shall be included in the data display system.

10.4.1.5 Security

A means shall be provided to restrict access to the control portions of the data display equipment (hardware and software).

10.4.1.6 Expansion

The data display equipment shall have the capability to incorporate additional display points or devices and should be purchased with greater than the anticipated operational requirements. (Experience has shown that a minimum capacity of 50% greater than the anticipated actual operational requirements is prudent.)

10.4.1.7 Display systems

Display systems shall be developed considering the human/information presentation interface such that the information is easily interpreted by the operator.

The display systems shall include at least the following data for alarm inputs:

a) Device status
b) Alarm location
c) Time of occurrence
d) Acknowledged/not acknowledged

10.4.2 Alarm reporting

10.4.2.1 General

Alarm events originate from discrete points or zones by activation of perimeter or interior intrusion detection devices, door alarms, invalid card reader transactions, or other security detection devices. Such alarms shall cause a data presentation in real-time containing the following information:

a) Point or zone identification
b) Narrative description of the point or zone location
c) Apparent reason for the sensor stimulus (e.g., intrusion)
d) Date and time to the nearest second

A listing of existing, noncleared alarms shall be available.

10.4.2.2 Equipment failure alarms

Equipment failure alarm events shall be reported in the same format as events described in 10.4.2.1.

10.4.2.3 Acknowledgment

A means shall be provided for the operator to acknowledge events in the system. The system shall provide the capability to distinguish between unacknowledged and acknowledged events. Such distinguishing can be accomplished by flashing the visual identification of an unacknowledged alarm and, when acknowledged, the visual identification would be steady. Multiple nuisance alarms from the same point or zone may be caused by contact chatter or extreme weather conditions. When multiple alarms from the same point or zone occur in rapid succession with no intervening alarms, they shall be acknowledged as a group.

Each alarm acknowledgment shall be logged for permanent recording. The permanent record shall contain the time and date of acknowledgment, the point or zone identification, and the identification of the operator who performed the function.

10.4.2.4 Alarm annotation

Every alarm that occurs shall require the operator to annotate the specific action taken. Annotation shall be of sufficient text to provide an adequate description of the action taken. When multiple alarms from a single point or zone occur in rapid succession with no intervening alarms, they shall be annotated as a group.

The text shall be logged on a permanent record that shall also include the time and date of the annotation, the point or zone identification, and the identification of the person performing the function.

10.4.2.5 Event clearing/reset

The alarm system shall be designed so that the console operator can clear alarms from the alarm listing only after the alarm has been annotated and reset. The action of clearing an event shall be logged on a permanent record that shall also contain the time of the clearing, the point or zone identification, and the identification of the person performing the function.

10.4.2.6 System status

System status of off-normal points or zones shall be immediately available. System status shall include off-normal conditions (e.g., alarm, access, and off-line).

10.4.2.7 Record keeping

All data generated as a result of alarm reporting shall be maintained as a permanent record and shall be stored on a secondary or bulk storage device in a form suitable for retrieval and reporting at a later date. These records shall be maintained for seven years unless otherwise justified.

10.5 Integration with other security functions—Access control

Integration of the access control system with the data acquisition, processing, and display system can be used to facilitate personnel access verification and documentation requirements.

Access requests transmitted to the security computer system shall include the user’s identity and the desired entry/exit location. The validity of the access control identification device used to input the access request shall first be verified, and then the identity data shall be verified against the stored information on the individual. The validity of the request shall be verified to determine if the individual is authorized access for that

time. A negative or incorrect response to any of the above shall generate an alert. The alert message shall include the date, time, and location of the unauthorized request, and the individual's identification. A means shall be provided to record all authorized and unauthorized access requests. Each transaction shall be documented as it occurs, unless a means of on-line storage is provided. The storage facility shall have provisions for generating a periodic log (usually daily) of the stored data. The record for authorized access requests shall include, as a minimum, the date, time, name and badge number of the individual, as well as the location of the requested access. The record of unauthorized access requests shall include the information contained in the original alert message and the action taken.

The format for establishing access control files shall permit expeditious and accurate inputting of data. In computerized systems, a means shall be provided to prevent loss of data in the event of a system failure. A means shall be provided to modify the access control files.

The access control system shall be integrated with the central security computer system to provide the flexibility to monitor additional parameters, such as accountability, compartmentalization, and logging of visitor access.

The access control system shall be designed to support the data acquisition, processing, and display system during execution of the plant's emergency evacuation procedures. This includes placing selected access control points into access mode and providing accountability data during and following an emergency evacuation. The accountability reporting must provide, as a minimum, a list of all personnel accounted for and a list of those unaccounted for along with their last known location.

11. Voice communications—Performance requirements

The central alarm station and the secondary alarm station shall 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 (operating to meet its intended function or functions) requirements are as indicated in 11.1 through 11.8.

11.1 Telephone availability

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

11.2 Radio availability

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

11.3 Security force communication

All members of the security force shall have the ability for continuous two-way voice communication with the CAS, the SAS, and each other.

11.3.1 Availability

Equipment for on-site, two-way voice communication shall have a 95% availability of operation.

11.3.2 Communications coverage

The on-site 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 shall be kept to a minimum. Dead zone areas shall be identified for security purposes. If a dead zone is sufficiently large, alternate communication means (telephone) shall be provided.

11.4 Communication protection

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

11.5 Antenna protection

The fixed security radio antenna or antennas shall be located within the PA.

11.6 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 network.

11.7 Radio interference protection

The security communications system shall be designed to preclude radio frequency interference from and with plant operating equipment.

11.8 Loss of communication

Upon detection of degraded communications or a loss of one of the available communication paths, repairs shall be initiated immediately to diminish the possibility that all communication paths will be out of service at the same time.

12. Line supervision

12.1 General

Line supervision is a technical means used to detect the intentional modification by an adversary of security alarm data in the communication path between the sensor and the annunciation location(s).

Line supervision applies to all sensor data communication paths. This includes all path media (e.g., wire conductor, optical fiber, atmospheric transmission) and all path types (e.g., dedicated line/star configuration, multiplexed line/loop configuration).

12.2 Performance requirements

12.2.1 Continuous detection

Line supervision shall monitor the communication path continuously, including times when the attached sensor is in the access mode.

12.2.2 Timely detection

Alarm data modification shall be detected and annunciated in 1 s or less.

12.2.3 Protection-in-depth

Each segment of the data communication path from the sensor to the annunciator shall have equivalent protection.

12.2.4 Balanced protection

Each security alarm communication path shall have equivalent protection.

12.3 Implementation of performance

12.3.1 Line protection

Line supervision is required for data communication paths. DC line supervision (i.e., Ohm's Law type) provides acceptable protection for nuclear assets at nuclear power stations. Digital polling techniques (interrogation and response) shall be considered when enhanced security is required. The enhanced features of digital polling shall include random polling sequence and/or frequency, data authentication, or word encryption.

12.3.2 Enclosure protection

Access cover position tamper switches shall be used. Other tamper sensors, such as penetration sensors/continuity grids and optical sensors/light level shall be considered where enhanced security is required. Tamper protection shall use tamper-resistant hardware, tamper-indicating materials (visual/physical inspection), and real-time tamper alarms.

13. Duress alarms

13.1 General

Duress alarms shall be located in the CAS and SAS and shall be considered for other critical locations. Such signaling could be the result of hostile activity being observed within the facility, such as a threatened security force member, an employee under duress, or other emergency situations.

13.2 Duress alarm devices

Different types of duress alarm devices that can be used to suit the various operations for which the device is installed are described in 13.2.1 through 13.2.5.

13.2.1 Button alarm

Manual button alarms can be hold-type hand buttons or distinctively colored (usually blue) wall-mounted emergency stations, which require overt action to operate. Hidden buttons are also used.

13.2.2 Foot-operated alarm

Foot-operated alarms are of the holdup foot-rail type, which require semi-overt action to operate. If a user is seated at a desk and the alarm is mounted on the floor under the desk, the alarm can be operated surreptitiously.

13.2.3 Desk drawer alarm

Desk drawer alarms are of the holdup money clip (bill trap) type for covert operation. The user simply removes a certain sheet of paper from a desk drawer, which allows an electrical contact to be made, and a duress alarm is sent.

13.2.4 Wireless signaling device

Limited-range wireless signaling devices can consist of a self-contained hand-operated transmitter similar in size and range to a garage-door-opener transmitter. It sends a signal to a nearby receiver which, in turn, signals over an alarm circuit (hardwired or multiplexed) to the CAS and SAS. The general location of the duress situation is thus established since it is known which receiver has operated.

13.2.5 Wireless feature

Manual, foot-operated, or covert duress signaling devices can be made wireless by associating a transmitter with them.

13.3 Design basis

Duress signaling devices shall be provided at all locations within the plant where they are deemed necessary to fill the requirements of the security design plan. Duress signaling devices shall be considered for, but not be limited to, the following:

a) Entry portals (search areas)
b) Control room
c) PA entry

13.3.1 Operation

Activation of any duress alarm initiating device shall result in a distinctive signal at the CAS and SAS. In the case of hardwired systems, the signal shall be audible and visual and shall indicate by a console display (e.g., lamp annunciation or CRT display) and not at the location from which the signal originated. This alarm shall contain only duress signaling devices and no other intrusion detection or security equipment.

13.3.2 Multiplexing considerations

In multiplex systems, the duress alarm shall be displayed on the system readout (printer, CRT, annunciator, graphic) along with an audible signal. The readout shall clearly indicate the location of the duress signaling device. This alarm shall contain only duress initiating devices.

13.3.3 Annunciation exclusion

Duress signals shall not annunciate at the point of origination.

13.3.4 Wireless considerations

Wireless systems shall signal to a receiver located within the range of the single-purpose RF transmitter carried by security force members and other personnel needing duress signaling indication.

13.3.5 Other duress alarm techniques

Entrances to vital areas can be controlled by card readers with a digital keypad. The insertion of a coded card into the reader and the insertion of a correct number into the keypad will allow the door to be opened. To send a duress signal, the code number entered is a predefined number for duress.

13.3.6 Hand-held transceiver considerations

Some manufacturers of walkie-talkie systems provide a feature on the hand-held transceivers that causes an automatic duress signal to be sent if the transceiver is dropped or if the security force member carrying the transceiver assumes a prone position.

14. Power supplies

14.1 General

The design and installation of the security system power is critical to the availability of the security system at all times.

14.2 Security system power

The security power system shall supply ac 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: PA lighting; uninterruptible power supply (UPS) system battery charger; interior emergency lighting; critical heating, ventilation, and air-conditioning (HVAC) equipment; and data processing equipment not required for continuous monitoring. Backup power for lighting of the isolation zone during power interruptions shall be considered where enhanced security is required. A typical security power system consists of an ac generator set, automatic transfer equipment, a maintenance bypass switch, and a normal ac power supply (see Figure 4). The generator set shall be either a dedicated generator or another plant power supply that meets the requirements of this clause. The ac generator set will provide power to the supporting equipment whose failure could be tolerated for a period of time following the loss of normal ac power.

14.2.1 Uninterruptible power supply (UPS) system

The UPS system shall supply power to all equipment required to maintain continuously monitored parameters. These include such items as central processing units (CPUs), cathode ray tubes (CRTs), printers, annunciators, multiplexers, CCTV equipments, perimeter intrusion detection equipment, door controls (card readers, push-buttons, etc.), turnstiles, devices requiring calibration upon the loss of ac power (explosive detectors), and communications equipment. A typical UPS system consists principally of a normal ac power supply, a static inverter, a static transfer switch, a maintenance bypass switch, a battery charger, a battery, and an alternate ac power supply. Backup power for lighting the isolation zones during power interruptions shall be considered where enhanced security is required.

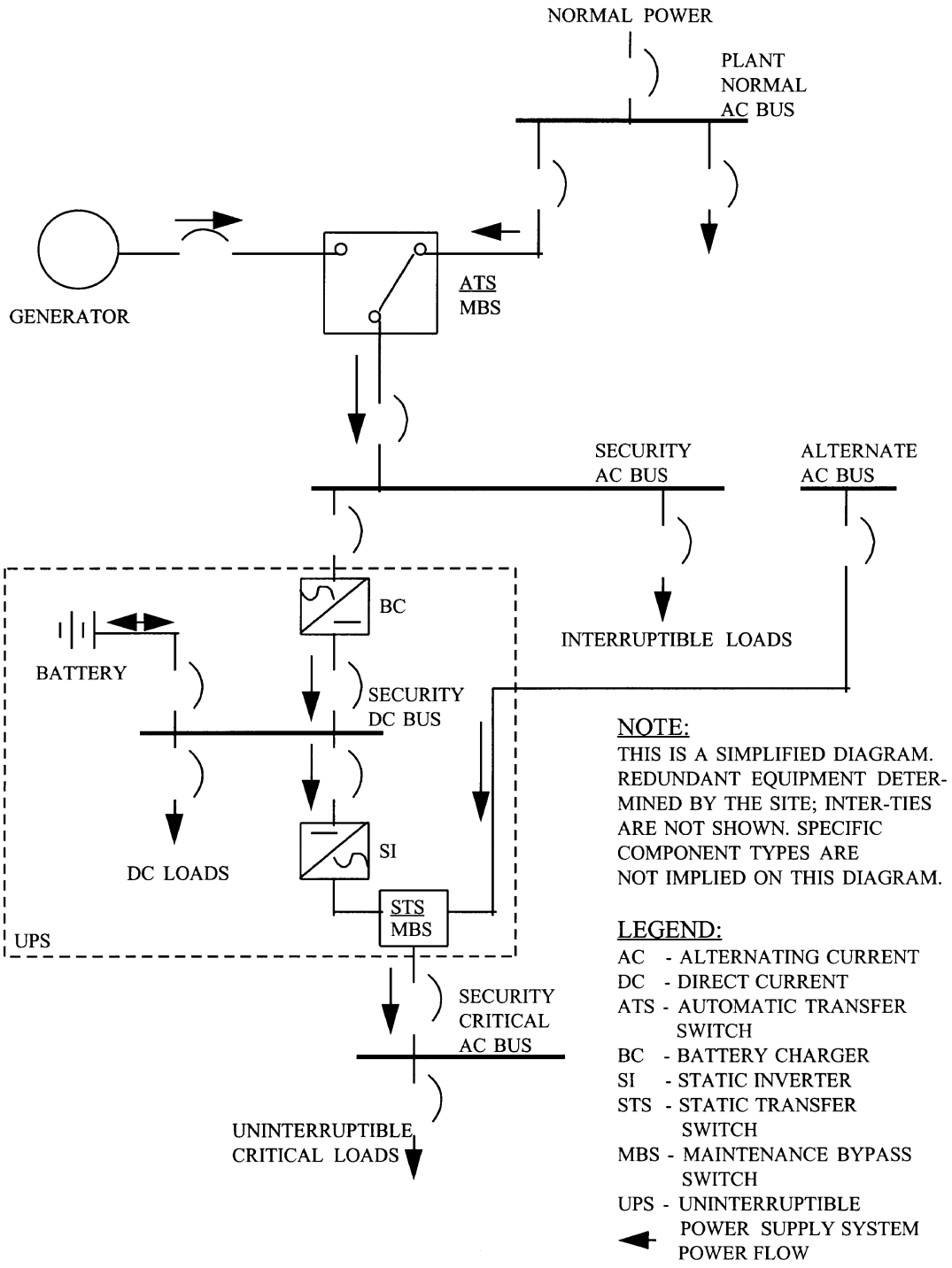

Figure 4—Single-line typical power supply

14.2.2 Plant bus

The UPS system's alternate ac power supply and normal ac power supply shall be from separate plant ac buses. The plant ac buses can be supplied from off-site or on-site sources.

14.2.3 Battery packs

Interior emergency lighting and equipment, when located such that providing power from the uninterruptible or security ac (see Figure 4) 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. The duration of operation on a battery pack is determined by the site-specific power outage coping duration.

14.3 Performance requirements

14.3.1 Location

All power supply equipment shall be installed within the PA, 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. Alarming shall be provided to indicate tampering or unauthorized access to the area containing the power supply equipment. Emergency generator fuel supply shall also be in the controlled access area and access to the fuel fill pipe shall be controlled.

14.3.2 Availability

Automatic switching or transfer of the UPS system shall not affect continuously monitored parameters. Upon loss of the battery charger, the UPS system shall be capable of sustaining operation without replacing or recharging batteries. Upon loss of the normal supply, an emergency supply shall be capable of sustaining operation. The duration of battery operation or emergency supply is determined by the site-specific power outage coping duration. Maximum availability of the supply of power to the security system shall be a design goal.

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

14.3.3 Annunciation

Degradation of the emergency power source or UPS system shall be annunciated as equipment failure alarms.

14.3.4 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 should be purchased with a minimum capacity 25% greater than the anticipated operational load to allow for future system growth.

15. Maintenance and testing

A documented maintenance and testing program shall be established and maintained for the life of the security system. This program shall address, as a minimum, factory and site acceptance testing; equipment identification; procedures for periodic testing, calibration, and other maintenance; intervals for testing and preventive maintenance; spare parts; technical information control; and training.

15.1 Acceptance testing

A program shall be established to implement acceptance testing of components, system segments, and systems at the factory prior to shipment. As a minimum, installed system acceptance tests at the plant site shall be performed before the system is placed into active service.

15.2 Equipment identification

A listing of all equipment in the security system shall be prepared that properly identifies each item. Each item or component shall be assigned an identifying number which is affixed to or inscribed on that item. Records shall include both model and serial numbers when available.

15.3 Procedures

Written procedures shall be available for each maintenance function by equipment type. As a minimum, documented procedures shall be prepared and used when performing testing and calibration. Procedures shall include the following basic information:

a) Identification of item to be tested/calibrated
b) Description of test equipment to be used including last calibration date and tolerances
c) Description of test or calibration and applicable tolerances
d) Sequence of test or calibration
e) Special instructions, if required
f) Frequency of test or calibration by calendar or running time

Procedures to be used could be those recommended by the equipment manufacturer or prepared by plant personnel.

15.4 Intervals

Intervals of testing and preventive maintenance shall be established from records of inherent reliability of equipment, downtime required for testing, historical records for similar equipment, and regulatory requirements.

15.5 Records

Records shall be maintained for the life of the equipment system or subsystem for all initial testing, unless otherwise justified. Calibration, preventive or corrective maintenance, or replacement records for security equipment shall be maintained for a period of three years. Records shall identify equipment by number, nature of work performed, procedure and test equipment used (if applicable), date, and person performing the work.

15.6 Spare parts

A spare parts procurement and stocking system shall be established to maintain an acceptable level of system performance. Equipment supplier recommendations and equipment failure experience may be used to establish a proper level of spare parts stock on hand.

15.7 Technical information

Technical information, such as maintenance manuals, blueprints, and schematic drawings, including detailed circuit drawings of all printed circuit boards, shall be obtained prior to equipment installation and maintained for the life of the equipment or system. Technical information and drawings shall be updated as needed whenever modifications are made to the system or individual items of equipment.

15.8 Training

A documented program of training for maintenance personnel shall be initiated prior to installation of the security systems. Records of security systems maintenance training shall be maintained for the duration of active maintenance employment of maintenance personnel.

Annex A

(informative)

Bibliography

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

[B1] ANSI/IES RP7-1990, Practice for Industrial Lighting.

[B2] ASTM F967-95, Practice for Security Engineering Symbols.

[B3] ASTM F1029-86 (Reaff 1991), Guide for Selection of Physical Security Measures for a Facility.

[B4] NRC 10 CFR 73, Physical Protection of Plants and Materials.

[B5] NRC Regulatory Guide 5.7, Entry/ Exit Control for Protected Areas, Vital Areas, and Material Access Areas, Rev. 1, 5/80.

[B6] NRC Regulatory Guide 5.12, General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials, Nov. 1973.

[B7] NRC Regulatory Guide 5.44, Perimeter Intrusion Alarm Systems, Rev. 2, 5/80.

[B8] NUREG 0181, Barrier Penetration Database, 7/78.

[B9] NUREG 0219, Nuclear Security Personnel for Power Plants, 7/78.

[B10] NUREG 0220, Interim Acceptance Criteria for a Physical Security Plan for Nuclear Power Plants, 3/77.

[B11] NUREG 0271, Physical Protection Equipment Study, 1/78.

[B12] NUREG 0273, Guide for the Evaluation of Physical Protection; Equipment (Book 1, vol. I-III), 1/78.

[B13] NUREG 0669, Fixed Site Physical Protection Upgrade Rule Compendium, 6/89.

[B14] NUREG 0703, Potential Threat to Licensed Nuclear Activities from Insiders (Insider Study), 7/80.

[B15] NUREG 0794, Protection of Unclassified Safeguards Information; Criteria and Guidance, 10/81.

[B16] NUREG 0908, Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans, 8/82.

[B17] NUREG 0992, Report of the Committee to Review Safeguards Requirements at Power Reactors, 5/83.

[B18] NUREG 1045, Guidance on the Application of Compensatory Measures for Power Reactor Licensees, 1/84.

[B19] NUREG-CR-1327, Security Lighting Planning Document for Nuclear Fixed Site Facilities, 4/80.

[B20] NUREG-CR-2462, Capacity of Nuclear Power Plant Structures to Resist Blast Loading, 9/83.

[B21] NUREG-CR-2546, Reactor Safeguards Against Insider Sabotage, 3/82.

[B22] NUREG-CR-2551, Rank Ordering of Vital Areas Within Power Plants, 4/82.

[B23] NUREG-CR-2585, Nuclear Power Plant Damage Control Measures and Design Changes for Sabotage Protection, 5/82.

[B24] NUREG-CR-2643, A Review of Selected Methods for Protecting Against Sabotage by an Insider, 8/82.

[B25] NUREG-CR-4250, Vehicles Barriers: Emphasis on Natural Features Sandia Lab Documents, 7/85.

[B26] NUREG-CR-5721, Video Systems for Alarm Assessment, 9/91.

[B27] NUREG-CR-5722, Interior Intrusion Detection Systems, 10/91.

[B28] NUREG-CR-5723 Security System Signal Supervision, 9/91.

[B29] SAND 88-1715C, Selection and Evaluation of Video Tape Records for Surveillance Applications, 1988.

[B30] Title 10 Code of Federal Regulations, Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.”

[B31] UL 187-1993, X-Ray Equipment.

[B32] W-A-0450B (GSA-FSS), (Interim Federal Specification) Security Components for Interior Alarm Systems, 2/16/73.