

IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations

Sponsor

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

Reaffirmed 22 September 2005

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

Copyright © 2005 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1997. Printed in the United States of America.

ISBN 1-55937-941-3

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

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.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (508) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

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. Gausa
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 Rüsck
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

1.	Overview.....	1
1.1	Scope.....	1
1.2	Purpose.....	1
2.	References.....	1
3.	Definitions.....	2
4.	Integrated security system.....	3
4.1	General.....	3
4.2	List of security system equipment (or subsystems)	3
4.3	Performance requirements	4
4.4	Design basis	4
4.5	Functional design verification.....	4
5.	Perimeter intrusion alarm system.....	6
5.1	General.....	6
5.2	Description.....	7
5.3	Site evaluation.....	8
5.4	Performance requirements	9
5.5	Tamper protection	10
6.	Security lighting.....	10
6.1	General.....	10
6.2	Outdoor security lighting	10
6.3	Primary portal security lighting	11
6.4	Interior security lighting	12
7.	Remote video surveillance	12
7.1	General.....	12
7.2	Performance requirements	13
7.3	Minimum equipment standards.....	15
7.4	Documentation.....	15
8.	Access control	16
8.1	General.....	16
8.2	Design basis documentation	16
8.3	Access control hardware	16
9.	Interior intrusion detection.....	18
9.1	General.....	18
9.2	Description.....	18
9.3	Site evaluation.....	18
9.4	Performance requirements	19

9.5	Tamper protection.....	19
10.	Data acquisition, processing, and display	19
10.1	General.....	19
10.2	Data acquisition	20
10.3	Signal processing	20
10.4	Data display	21
10.5	Integration with other security functions—Access control	23
11.	Voice communications—Performance requirements	24
11.1	Telephone availability.....	24
11.2	Radio availability	24
11.3	Security force communication	24
11.4	Communication protection.....	25
11.5	Antenna protection.....	25
11.6	Intelligence protection	25
11.7	Radio interference protection.....	25
11.8	Loss of communication.....	25
12.	Line supervision.....	25
12.1	General.....	25
12.2	Performance requirements	25
12.3	Implementation of performance.....	26
13.	Duress alarms.....	26
13.1	General.....	26
13.2	Duress alarm devices	26
13.3	Design basis	27
14.	Power supplies	28
14.1	General.....	28
14.2	Security system power	28
14.3	Performance requirements	30
15.	Maintenance and testing	31
15.1	Acceptance testing	31
15.2	Equipment identification.....	31
15.3	Procedures.....	31
15.4	Intervals.....	31
15.5	Records	31
15.6	Spare parts.....	32
15.7	Technical information.....	32
15.8	Training.....	32
Annex A	(informative) Bibliography	33

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).

¹IEEE 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 than 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

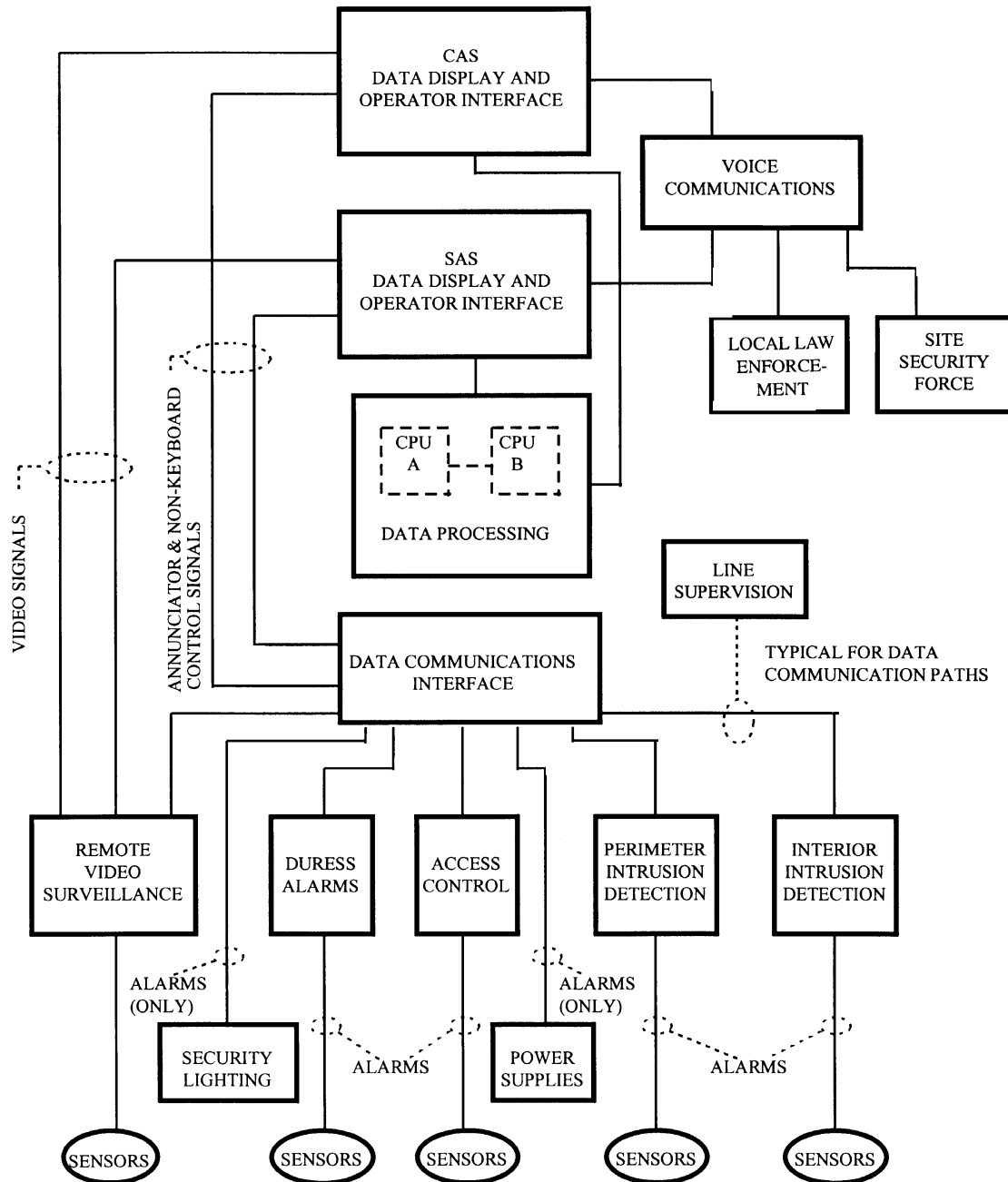


Figure 1—Integrated security system interfaces

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

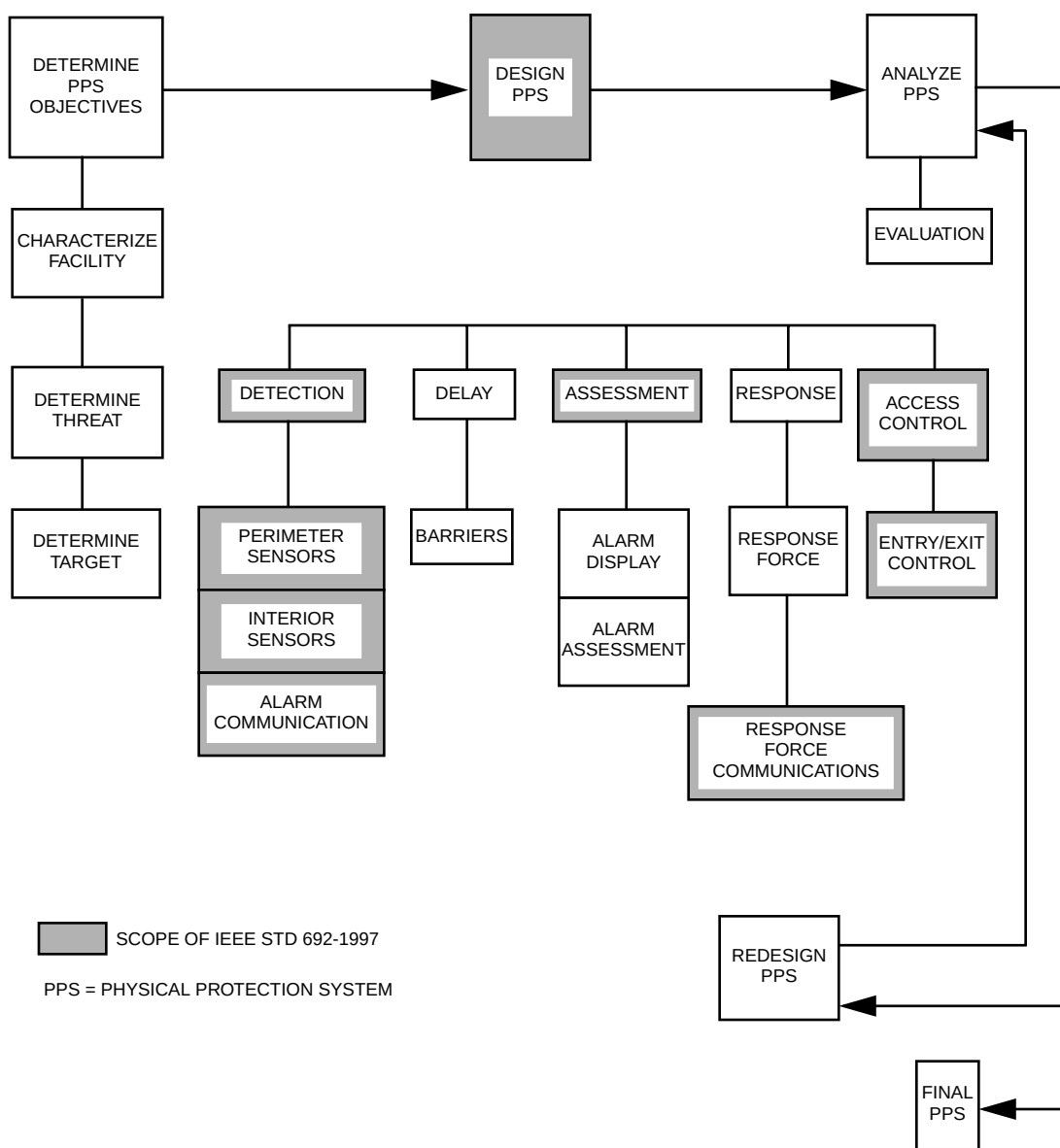


Figure 2—Physical protection elements

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.