IEEE Std 603-1998
(Revision of
IEEE Std 603-1991)

IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

Sponsor

Nuclear Power Engineering Committee
of the
IEEE Power Engineering Society

Approved 1 July 1998

IEEE-SA Standards Board

Abstract: Minimum functional and design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems are established. The criteria are to be applied to those systems required to protect the public health and safety by functioning to mitigate the consequences of design basis events. The intent is to promote safe practices for design and evaluation of safety system performance and reliability. Although the standard is limited to safety systems, many of the principles may have applicability to equipment provided for safe shutdown, post-accident monitoring display instrumentation, preventative interlock features, or any other systems, structures, or equipment related to safety.
Keywords: actuated equipment, associated circuits, Class 1E, design, failure maintenance bypass, operating bypass, safety function, sense and command features, sensor

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

Copyright © 1998 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1998. Printed in the United States of America.

ISBN 0-7381-0326-8

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) 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-SA 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; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

--`,,`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Introduction

(This introduction is not a part of IEEE Std 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.)

This standard establishes minimum functional design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems. These criteria are established to provide a means for promoting safe practices for design and evaluation of safety system performance and reliability. However, adhering to these criteria will not necessarily fully establish the adequacy of any safety system's functional performance and reliability; nonetheless, omission of any of these criteria will, in most instances, be an indication of safety system inadequacy.

Application

The criteria established by this standard apply to those systems defined as safety systems and do not necessarily apply to all of the systems, structures, and equipment required for complete plant safety. Although the scope is limited to safety systems, many of the principles may have applicability to equipment provided for safe shutdown, accident monitoring display instrumentation, preventive interlock features, or any other systems, structures, or equipment related to safety, or all of the above.

To determine those systems subject to these criteria, an analysis of the overall plant response to postulated design basis events shall be performed. Good engineering judgment should be exercised in this analysis to assure that adequate margins exist in the design to protect the health and safety of the public without imposing unduly restrictive criteria on the design.

Interdisciplinary approach

The safety system criteria herein are established using a systems approach to the design of the power, instrumentation, and control portion of the safety system, as opposed to a specific engineering discipline approach (that is, electrical, mechanical, or civil). It is recognized that the safety functions cannot be accomplished without mechanical, as well as electrical equipment and circuitry. It shall also be recognized that some safety functions may be implemented using digital computers and computer programs. Therefore, the design by other disciplines should consider these criteria. In order for the safety system to meet the requirements of this standard and the supportive standards, the aggregate design of the safety system (without regard to discipline) may be constrained. For example, the consideration of common cause failure is an item that requires an interdisciplinary review and design solution. Such constraints are themselves implicit interface requirements imposed upon the individual constituent parts to enable the entire safety system to meet these requirements. The areas where this standard interfaces with other standards are shown in Figure 1.

While this standard takes a systems approach to the design of the power, instrumentation, and control portion of the safety system, it does not attempt to establish new or different criteria for mechanical equipment or components. Such an attempt by a user is a misapplication of this standard. Nor does this standard attempt to establish the system-level requirements that may be required by mechanical or civil equipment; for example, in-service inspection of piping is intentionally excluded. This standard provides criteria for the safety system without conflicting with existing standards. This standard is not intended to duplicate or conflict with component design requirements such as the ASME Boiler and Pressure Vessel Code. Rather, this standard is to complement and interface with such documents. This standard and others (for example, ANSI/ANS 51.1-1983 and ANSI/ANS 52.1-1983) establish systems criteria while other codes and standards establish detailed design requirements necessary to ensure the functional adequacy of the individual constituent parts of the safety system.

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Evolution

This standard was evolved from IEEE Std 603-1980, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. It represents the sixth Subcommittee 6 (SC-6) publication of a systems criteria document. The series began with IEEE Std 279-1968, a trial-use standard for protection systems, followed by IEEE Std 279-1971, a standard for protection systems; IEEE Std 603-1977, a trial-use standard for safety systems; IEEE Std 603-1980 and IEEE Std 603-1991, a standard for safety systems.

Relationship to other standards

This standard establishes functional and design criteria that are general in nature. It requires supportive standards containing both general and detailed criteria to comprise a minimal set of requirements for the safety system.

Other IEEE standards prepared in support of the criteria of this standard are referenced throughout this standard. The American National Standards, in particular ANSI/ANS 51.1-1983 and ANSI/ANS 52.1-1983, also contain functional and design criteria for safety systems.

International standard IEC 60231A (1969-01) [B7][1] also contains functional and design criteria for safety systems.

The definition of the term “safety system” in Section 2 references 10 CFR Part 100. This definition is the same as used by other groups, such as, the ANS and ISA. This is per agreements made with the other organizations.

Purpose of revision

The purpose of this revision is to clarify the application of this standard to computer-based safety systems and to advanced nuclear power generating station designs. This revision provides guidance for the treatment of electromagnetic interference (EMI) and radio-frequency interference (RFI), clarifies definitions (e.g., “Class 1E”), and updates references.

IEEE Std 7-4.3.2-1993 provides additional guidance on applying the safety system criterion specified by this standard for the use of computers as components in safety systems.

Future work

In the future, consideration will be given to incorporating the requirements of IEEE Std 494-1974 [B9] into this standard.

The subcommittee recognizes that the term “Class 1E” is sometimes misapplied. A note was added in the 1991 revision of this standard to clarify the use of the term. The subcommittee will continue to review the definition of “Class 1E” to ensure clarity.

The subcommittee also recognizes the terms division, channel, and train have interchangeable definitions in different industry standards. The terms division and channel were clarified in this standard. The subcommittee will review other industry standards to ensure clarity.

Further clarification of the criteria used to determine reliability goals, as discussed in Clause 4 item i) and 5.5 of this standard, will also be considered.

---

[1]The numbers in brackets preceded by the letter B correspond to those of the bibliography in Annex C.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Consideration will be given to providing additional guidance or reference(s) to address electromagnetic interference.

The requirements for accident monitoring instrumentation, contained in ANS 4.5-1989 and IEEE Std 497-1981, are currently undergoing revision. References to IEEE Std 497-1981 are made in Clause 4 item e), and 5.8 of this standard. The criteria in ANS 4.5-1989 and in IEEE Std 497-1981 are being combined and updated in a new revision to ANS 4.5-1989. The revised ANS 4.5 standard will contain criteria that addresses the use of computerized displays and developments in human factor designs. The user is advised that updated criteria may provide useful guidance. The approved ANS 4.5 will be incorporated into the next revision of this standard.

Participants

This document was prepared by the Safety-Related Systems Working Group Subcommittee 6.3 of the IEEE Nuclear Power Engineering Committee. At the time this standard was prepared, the working group had the following membership:

David J. Zaprazny, *Chair*

Ron E. Battle	Clifford K. Doutt	Britton P. Grim
Wes W. Bowers	Edward F. Dowling	Rick Kendall
	Pat M. Duggan	

The following persons were on the balloting committee:

Satish K. Aggarwal	Rich E. Dulski	James T. Keiper
Vincent P. Bacanskas	Surinder Dureja	Alex Marion
Farouk D. Baxter	Jay Forster	John R. Matras
Wes W. Bowers	J. R. Fragola	R. B. Miller
Daniel F. Brosnan	John M. Gallagher	Burt Nemroff
Nissen M. Burstein	Wil C. Gangloff	Neil P. Smith
S. P. Carfagno	Luis C. Gonzalez	Peter B. Stevens
Robert C. Carruth	Lawrence P. Gradin	Peter Szabados
Raymond J. Christensen	John Greene	James E. Thomas
Robert L. Copyak	Britton P. Grim	Raymond Weronick
J. J. Disosway	Robert E. Hall	G. O. Wilkinson
Gary L. Doman	Joe T. Hazeltine	David J. Zaprazny
Edward F. Dowling	Gregory K. Henry	Mark S. Zar
	Sonny Kasturi	

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

The final conditions for approval of this standard were met on 1 July 1998. This standard was conditionally approved by the IEEE-SA Standards Board on 25 June 1998, with the following membership:

Richard J. Holleman, *Chair* **Donald N. Heirman,** *Vice Chair*
Judith Gorman, *Secretary*

Satish K. Aggarwal
Clyde R. Camp
James T. Carlo
Gary R. Engmann
Harold E. Epstein
Jay Forster*
Thomas F. Garrity
Ruben D. Garzon
James H. Gurney
Jim D. Isaak
Lowell G. Johnson
Robert Kennelly
E. G. "Al" Kiener
Joseph L. Koepfinger*
Stephen R. Lambert
Jim Logothetis
Donald C. Loughry
L. Bruce McClung
Louis-François Pau
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Hans E. Weinrich
Donald W. Zipse

*Member Emeritus

Catherine K.N. Berger
IEEE Standards Project Editor

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Contents

1. Scope 1

1.1 Illustration 1
1.2 Application 2

2. References 4

3. Definitions 5

4. Safety system design basis 8

5. Safety system criteria 9

5.1 Single-failure criterion 9
5.2 Completion of protective action 9
5.3 Quality 9
5.4 Equipment qualification 10
5.5 System integrity 10
5.6 Independence 10
5.7 Capability for testing and calibration 11
5.8 Information displays 11
5.9 Control of access 12
5.10 Repair 12
5.11 Identification 12
5.12 Auxiliary features 12
5.13 Multi-unit stations 13
5.14 Human factors considerations 13
5.15 Reliability 13
5.16 Common cause failure criteria 13

6. Sense and command features—functional and design requirements 13

6.1 Automatic control 13
6.2 Manual control 14
6.3 Interaction between the sense and command features and other systems 14
6.4 Derivation of system inputs 15
6.5 Capability for testing and calibration 16
6.6 Operating bypasses 16
6.7 Maintenance bypass 16
6.8 Setpoints 16

7. Execute features (functional and design requirements) 17

7.1 Automatic control 17
7.2 Manual control 17
7.3 Completion of protective action 17
7.4 Operating bypass 17
7.5 Maintenance bypass 17

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

8. Power source requirements 18

8.1 Electrical power sources 18
8.2 Non-electrical power sources 18
8.3 Maintenance bypass 18

Annex A (informative) Illustration of some basic concepts for developing the scope of a safety system 19

Annex B (informative) Electromagnetic compatibility 27

Annex C (informative) Bibliography 31

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

1. Scope

The criteria contained in this standard establish minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power generating stations. To satisfy the criteria in this standard, interface requirements may be imposed on the other portions of the safety system as shown in Figure 1. Safety system functional and design criteria are also contained in other standards.[1]

1.1 Illustration

Figure 2 illustrates the scope of this standard in the form of a 3×3 matrix. The labeling across the top of the matrix illustrates that the safety systems can be subdivided into the three general elements of sense and command features, execute features, and power sources. These general elements represent a grouping of devices that provides similar performance characteristics for many discrete safety functions. The labeling on the left side of the matrix illustrates that the safety systems can also be subdivided into the three operational elements of reactor trip system and engineering safety features, auxiliary supporting features, and other auxiliary features. When viewing an entire row of the matrix, it can be seen that an operational element may form a system.

Illustrating the scope of this standard in matrix form shows that each operational element contains one or more general elements. This matrix should not be interpreted to mean that every operational element shall contain all of the general elements or that a particular general element is limited to application in only one operational element.

Figure 3 illustrates typical equipment examples for each portion of the matrix diagram. As shown, some components can be fitted into more than one category depending on the component's use.

Figure 4 illustrates where criteria for each portion of the matrix can be found in this standard.

---

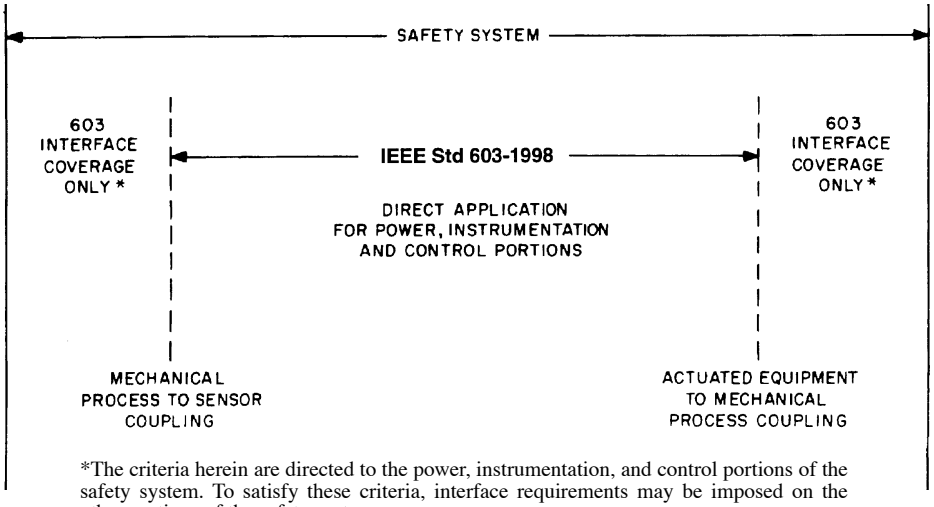
[1]See Clause 2 and Annex C for applicable standards.

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

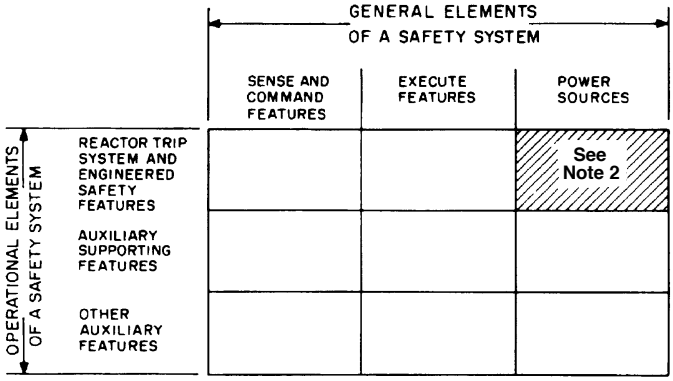
1.2 Application

The safety system criteria established herein are to be applied to those systems required to protect the public health and safety by functioning to prevent or mitigate the consequences of design basis events. However, this standard does not apply to all of the systems, structures, and equipment required for complete plant safety, for example, fire protection systems.



*The criteria herein are directed to the power, instrumentation, and control portions of the safety system. To satisfy these criteria, interface requirements may be imposed on the other portions of the safety system.

Figure 1—Nonelectrical interface scope diagram



NOTES

1—The protection system of IEEE Std 279-1971 [B8][2] and of this standard is the sense and command features for the reactor trip system and the engineered safety features.

2—Power sources, by definition, are considered auxiliary supporting features or other auxiliary features and, therefore, are not shown as part of the reactor trip system and engineered safety features.

3—When viewing an entire single row of the matrix, it can be seen that an operational element may form a system; for example, a service water system. However, when viewing an entire column, general elements represent a grouping of devices that provide similar performance characteristics (e.g., sensors) for many discrete safety functions.

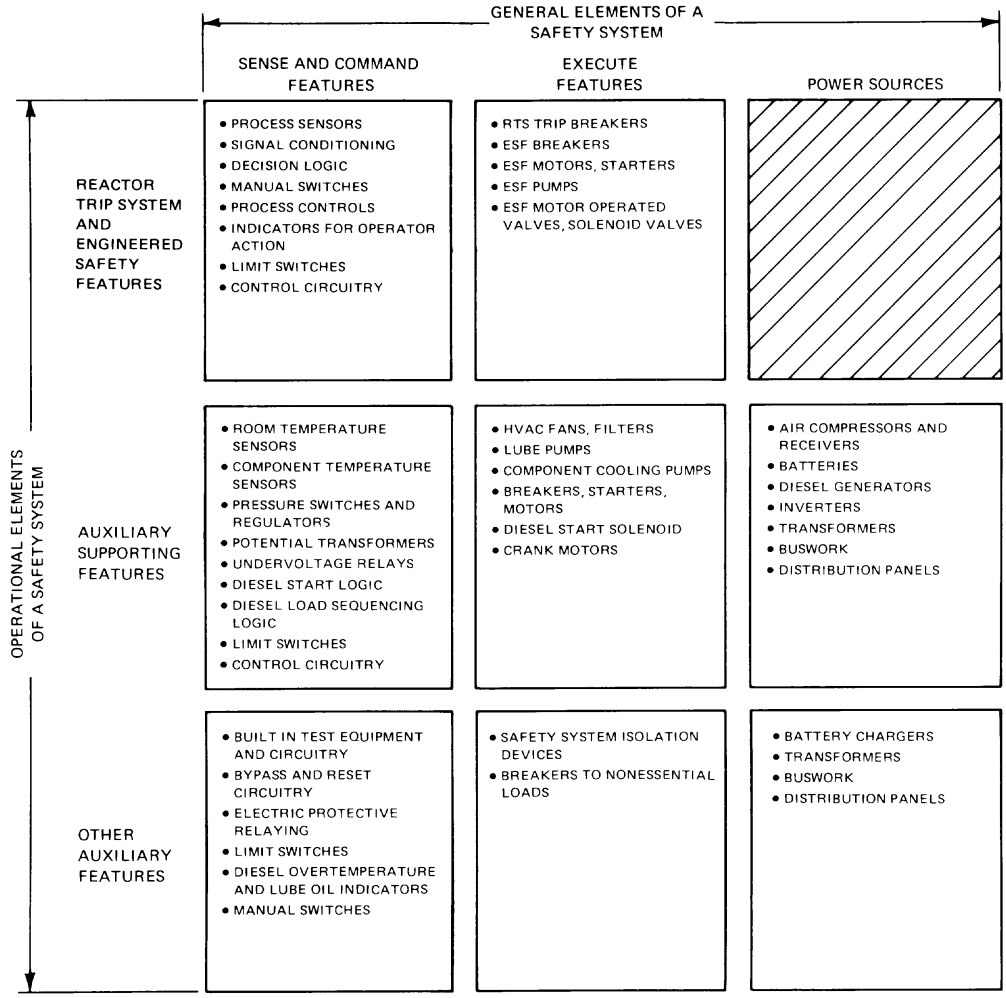
4—Each operational element contains one or more general elements. Every operational element does not necessarily contain all of the general elements.

5—A device that serves as a general element is not necessarily limited to application in only one operational element.

Figure 2—3 × 3 matrix representation of safety system

[2]The numbers in brackets preceded by the letter B correspond to those of the bibliography in Annex C.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale



NOTES

1—The items listed are only representative examples as to inclusion or location in the matrix.

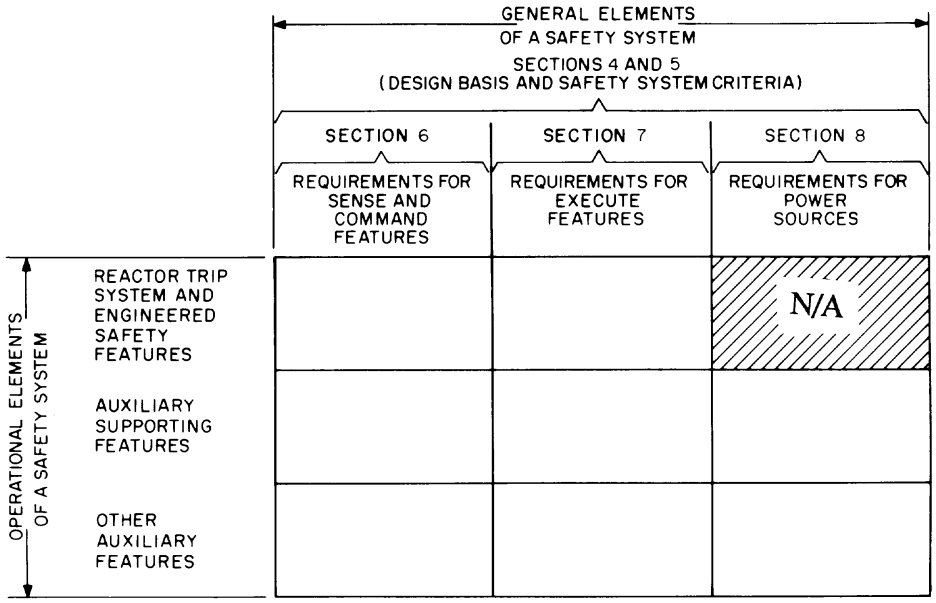
2—See Figure 2 for additional notes.

3—Computer hardware, firmware, and programs are representative examples as to inclusion or location in the matrix.

Figure 3—Examples of equipment fitted to safety system scope diagram

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale



NOTE—See Figure 2 for notes.

Figure 4—Scope diagram for IEEE Std 603-1998

2. References

This standard shall be used in conjunction with the following publications. When the following standards are superseded by an approved revision, the revision shall apply.

ANSI/ANS 51.1-1983 (Reaff l988), Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.[3]

ANSI/ANS 52.1-1983 (Reaff l988), Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants.

ANSI/ISA S67.04-1994, Setpoints for Nuclear Safety-Related Instrumentation.[4]

ASME NQA-1-1994, Quality Assurance Program Requirements for Nuclear Facilities.[5]

IEEE Std 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.[6]

IEEE Std 308-1991, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations.

[3]ANSI/ANS publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

[4]ANSI/ISA publications are available from 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709, USA or from the American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

[5]ASME publications are available from the American Society of Mechanical Engineers, 22 Law Drive, Fairfield, NJ 07007, USA.

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

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

IEEE Std 323-1983 (Reaff 1996), IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 338-1987 (Reaff 1993), IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems.

IEEE Std 352-1987 (Reaff 1993), IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.

IEEE Std 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.

IEEE Std 384-1992 (Reaff 1997), IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.

IEEE Std 420-1982, IEEE Standard for the Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations.

IEEE Std 577-1976 (Reaff l992), IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations.

IEEE Std 627-1980 (Reaff 1996), IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations.

IEEE Std 1023-1988 (Reaff 1995), IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations.

Title 10, Code of Federal Regulations, Part 100, Reactor Site Criteria.[7]

3. Definitions

The definitions in this clause establish the meaning of words in the context of their use in this standard.

3.1 acceptable. Demonstrated to be adequate by the safety analysis of the station.

3.2 actuated equipment. The assembly of prime movers and driven equipment used to accomplish a protective action.

NOTE—Examples of prime movers are: turbines, motors, and solenoids. Examples of driven equipment are: control rods, pumps, and valves.

3.3 actuation device. A component or assembly of components that directly controls the motive power (electricity, compressed air, hydraulic fluid, etc.) for actuated equipment.

NOTE—Examples of actuation devices are: circuit breakers, relays, and pilot valves.

3.4 administrative controls. Rules, orders, instructions, procedures, policies, practices, and designations of authority and responsibility.

3.5 analytical limit. Limit of a measured or calculated variable established by the safety analysis to ensure that a safety limit is not exceeded.

[7]The Code of Federal Regulations is available from the United States Government Printing Office, Washington DC 20401-4302, USA. (202) 512-1283 (http://www.access.gpo.gov/nara/cfr/cfr-table-search.html).

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

3.6 associated circuits. Non-Class 1E circuits that are not physically separated or are not electrically isolated from Class 1E circuits by acceptable separation distance, safety class structures, barriers, or isolation devices.

3.7 auxiliary supporting features. Systems or components that provide services (such as cooling, lubrication, and energy supply) required for the safety systems to accomplish their safety functions.

3.8 channel. An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined.

3.9 Class 1E. The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

NOTE— Users of this standard are advised that "Class 1E" is a functional term. Equipment and systems are to be classified Class 1E only if they fulfill the functions listed in the definition. Identification of systems or equipment as Class 1E based on anything other than their function is an improper use of the term and should be avoided.

3.10 common-cause failure. Multiple failures attributable to a common cause.

3.11 components. Discrete items from which a system is assembled.

NOTE—Examples of components are: wires, transistors, switches, motors, relays, solenoids, pipes, fittings, pumps, tanks, valves, computer programs, computer hardware, or computer firmware.

3.12 design basis events. Postulated events used in the design to establish the acceptable performance requirements for the structures, systems, and components.

3.13 detectable failures. Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures.

NOTE—Identifiable, but nondetectable, failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication. Refer to IEEE Std 379-1994.

3.14 division. The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

NOTE—A division can have one or more channels.

3.15 execute features. The electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling.

NOTE—In some instances, protective actions may be performed by execute features that respond directly to the process conditions (for example, check valves, self-actuating relief valves).

3.16 maintenance bypass. Removal of the capability of a channel, component, or piece of equipment to perform a protective action due to a requirement for replacement, repair, test, or calibration.

NOTE—A maintenance bypass is not the same as an operating bypass. A maintenance bypass may reduce the degree of redundancy of equipment, but it does not result in the loss of a safety function.

3.17 module. Any assembly of interconnected components that constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics that permit it to be tested as a unit. A module could be a card, a drawout circuit breaker, or other subassembly of a larger device, provided it meets the requirements of this definition.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

3.18 operating bypass. Inhibition of the capability to accomplish a safety function that could otherwise occur in response to a particular set of generating conditions.

NOTE—An operating bypass is not the same as a maintenance bypass. Different modes of plant operation may necessitate an automatic or manual bypass of a safety function. Operating bypasses are used to permit mode changes (e.g., prevention of initiation of emergency core cooling during the cold shutdown mode).

3.19 power sources. The electrical and mechanical equipment and their interconnections necessary to generate or convert power.

3.20 protection system. The part of the sense and command features involved in generating those signals used primarily for the reactor trip system and engineered safety features.

3.21 protective action. The initiation of a signal within the sense and command features or the operation of equipment within the execute features for the purpose of accomplishing a safety function.

3.22 redundant equipment or system. A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function, regardless of the state of operation or failure of the other.

NOTE—Duplication of essential functions can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.

3.23 safety function. One of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event.

NOTE—A safety function is achieved by the completion of all required protective actions by the reactor trip system or the engineered safety features concurrent with the completion of all required protective actions by the auxiliary supporting features, or both. (See Annex A for an illustrative example.)

3.24 safety group. A given minimal set of interconnected components, modules, and equipment that can accomplish a safety function.

NOTE—A safety group includes one or more divisions. (See Annex A for an illustrative example.)

3.25 safety system. A system that is relied upon to remain functional during and following design basis events to ensure: **(A)** the integrity of the reactor coolant pressure boundary, **(B)** the capability to shut down the reactor and maintain it in a safe shutdown condition, or **(C)** the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR Part 100 guidelines.

NOTES:

1—The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E.

2—This definition of "safety system" agrees with the definition of "safety-related systems" used by the American Nuclear Society (ANS) and IEC 60231A (1969-01) [B7].

3.26 sense and command features. The electrical and mechanical components and interconnections involved in generating those signals associated directly or indirectly with the safety functions. The scope of the sense and command features extends from the measured process variables to the execute features' input terminals.

3.27 sensor. The portion of a channel that responds to changes in a plant variable or condition and converts the measured process variable into an electric, optic, or pneumatic signal.

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

4. Safety system design basis

A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of ANSI/ANS 51.1-1983 or ANSI/ANS 52.1-1983 and shall document as a minimum:

a) The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.
b) The safety functions and corresponding protective actions of the execute features for each design basis event.
c) The permissive conditions for each operating bypass capability that is to be provided.
d) The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.
e) The protective actions identified in item b) that may be controlled by manual means initially or subsequently to initiation. See IEEE Std 497-1981 [B10]. The proactive actions are as follows:[8]
    1) The points in time and the plant conditions during which manual control is allowed.
    2) The justification for permitting initiation or control subsequent to initiation solely by manual means.
    3) The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations shall be performed.
    4) The variables in item d) that shall be displayed for the operator to use in taking manual action.
f) For those variables in item d) that have a spatial dependence (i.e., where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.
g) The range of transient and steady-state conditions of both motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference[9]) during normal, abnormal, and accident conditions throughout which the safety system shall perform.
h) The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).
i) The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design.
j) The critical points in time or the plant conditions, after the onset of a design basis event, including:
    1) The point in time or plant conditions for which the protective actions of the safety system shall be initiated.
    2) The point in time or plant conditions that define the proper completion of the safety function.
    3) The point in time or the plant conditions that require automatic control of protective actions.
    4) The point in time or the plant conditions that allow returning a safety system to normal.
k) The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.
l) Any other special design basis that may be imposed on the system design (e.g., diversity, interlocks, regulatory agency criteria).

[8]See [B1], Annex C for additional information.
[9]See Annex B for information on electromagnetic interference.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

5. Safety system criteria

The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function. (See Annex A for an illustrative example.)

5.1 Single-failure criterion

The safety systems shall perform all safety functions required for a design basis event in the presence of

a) Any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures.
b) All failures caused by the single failure.
c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1994 provides guidance on the application of the single-failure criterion. (See also [B3].) IEEE Std 7-4.3.2-1993 addresses common cause failures for digital computers.

This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion [B3]. The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.

Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in Clause 4, item i) of the design basis, a probabilistic assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.

5.2 Completion of protective action

The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.

5.3 Quality

Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (See ASME NQA-1-1994). Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

5.4 Equipment qualification

Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980. Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.

5.5 System integrity

The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Guidance on the application of this criteria for safety system equipment employing digital computers and software or firmware is found in IEEE Std 7-4.3.2-1993.

5.6 Independence

5.6.1 Between redundant portions of a safety system

Redundant portions of a safety system provided for a safety function shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design basis event requiring that safety function.

5.6.2 Between safety systems and effects of design basis event

Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability of meeting the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.

5.6.3 Between safety systems and other systems

The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4, item h) of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.

5.6.3.1 Interconnected equipment

a) *Classification*. Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.
b) *Isolation*. No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

5.6.3.2 Equipment in proximity

a) *Separation*. Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1992. (See [B1].)

b) *Barrier.* Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in Clause 4, items g) and h) of the design basis.

5.6.3.3 Effects of a single random failure

Where a single random failure in a nonsafety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1994 for the application of this requirement.

5.6.4 Detailed criteria

IEEE Std 384-1992 provides detailed criteria for the independence of Class 1E equipment and circuits [B1]. IEEE Std 7-4.3.2-1993 provides guidance on the application of this criteria for the separation and isolation of the data processing functions of interconnected computers.

5.7 Capability for testing and calibration

Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

— Appropriate justification shall be provided (e.g., demonstration that no practical design exists),
— Acceptable reliability of equipment operation shall be otherwise demonstrated, and
— The capability shall be provided while the generating station is shut down.

5.8 Information displays

5.8.1 Displays for manually controlled actions

The display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981 [B10]. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.

5.8.2 System status indication

Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

5.8.3 Indication of bypasses

If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.

a) This display instrumentation need not be part of the safety systems.
b) This indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable.
c) The capability shall exist in the control room to manually activate this display indication.

5.8.4 Location

Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to affect the actions.

5.9 Control of access

The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

5.10 Repair

The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

5.11 Identification

In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:

a) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1992 and IEEE Std 420-1982.
b) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.
c) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (e.g., identification of fire protection equipment, phase identification of power cables).
d) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.
e) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 [B9].
f) The versions of computer hardware, programs, and software shall be distinctly identified in accordance with IEEE Std 7-4.3.2-1993.

5.12 Auxiliary features

Auxiliary supporting features shall meet all requirements of this standard.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, and are part of the safety systems by association (i.e., not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criteria is contained in Annex A.

5.13 Multi-unit stations

The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1991. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1994.

5.14 Human factors considerations

Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.

5.15 Reliability

For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis. Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.

5.16 Common cause failure criteria

Plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure (See IEEE 379-1994). IEEE Std 7-4.3.2-1993 provides guidance on performing an engineering evaluation of software common cause failures, including use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the common cause failure.

6. Sense and command features—functional and design requirements

In addition to the functional and design requirements in Clause 5, the requirements listed in 6.1 through 6.8 shall apply to the sense and command features.

6.1 Automatic control

Means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4, item e). The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4, item e) following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of Clause 4, item e).

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

6.2 Manual control

Means shall be provided in the control room to

a) Implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.
b) Implement manual initiation and control of the protective actions identified in Clause 4, item e) that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.
c) Implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4, item j). The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.

6.3 Interaction between the sense and command features and other systems

6.3.1 Requirements

Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:

a) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:
   1) Channels that sense a set of variables different from the principal channels.
   2) Channels that use equipment different from that of the principal channels to sense the same variable.
   3) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.
   4) Both the principal and alternate channels shall be part of the sense and command features.
b) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system. See Figure 5 for a decision chart for applying the requirements of this clause.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

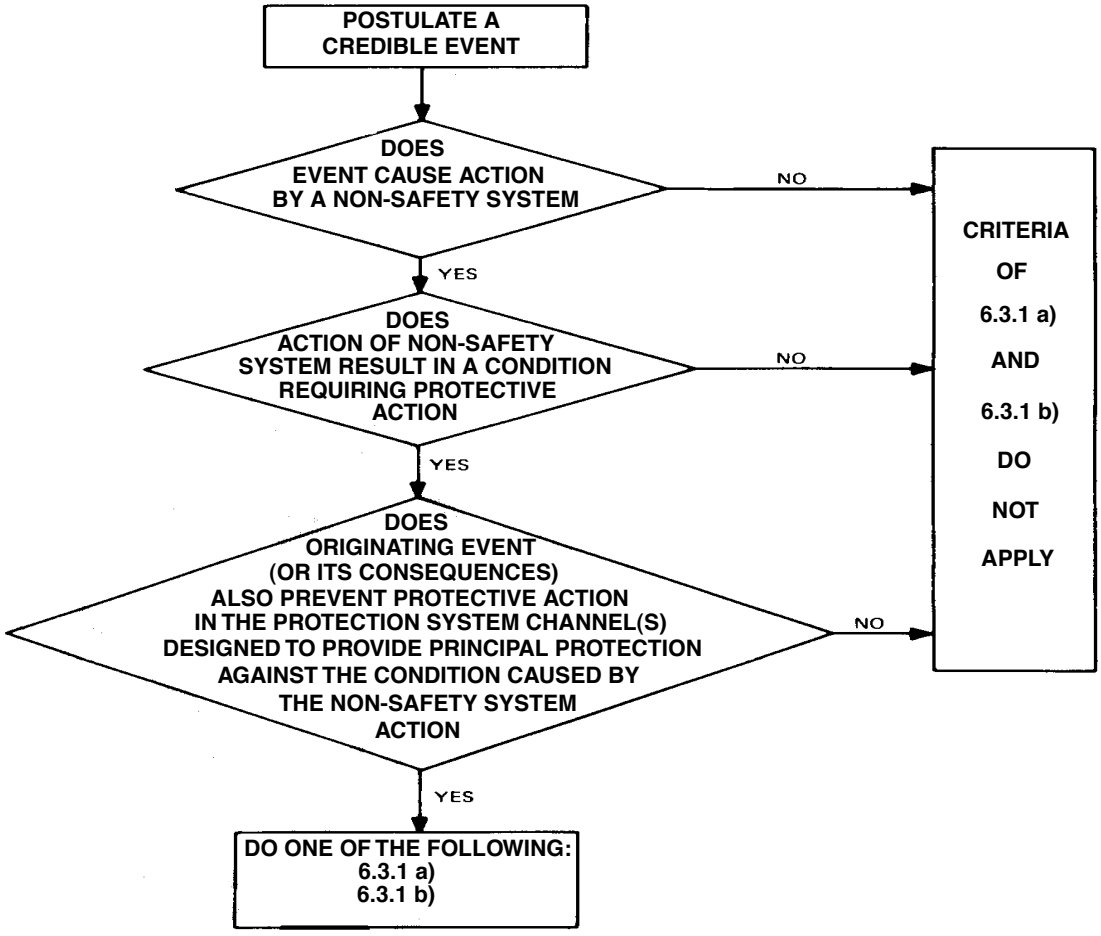


Figure 5—Interpretation of 6.3.1 of IEEE Std 603-1998

6.3.2 Provisions

Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.

6.4 Derivation of system inputs

To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

6.5 Capability for testing and calibration

6.5.1 Checking the operational availability

Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:

a) By perturbing the monitored variable,
b) Within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or
c) By cross-checking between channels that bear a known relationship to each other and that have read-outs available.

6.5.2 Assuring the operational availability

One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:

a) Checking the operational availability of sensors by use of the methods described in 6.5.1.
b) Specifying equipment that is stable and the period of time it retains its calibration during the post-accident time period.

6.6 Operating bypasses

Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:

a) Remove the appropriate active operating bypass(es).
b) Restore plant conditions so that permissive conditions once again exist.
c) Initiate the appropriate safety function(s).

6.7 Maintenance bypass

Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features should continue to meet the requirements of 5.1 and 6.3.

NOTE—For portions of the sense and command features that cannot meet the requirements of 5.1 and 6.3 when in maintenance bypass, acceptable reliability of equipment operation shall be demonstrated (e.g., that the period allowed for removal from service for maintenance bypass is sufficiently short, or additional measures are taken, or both, to ensure there is no significant detrimental effect on overall sense and command feature availability).

6.8 Setpoints

The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.

Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.

7. Execute features (functional and design requirements)

In addition to the functional and design requirements in Clause 5, the requirements listed in 7.1 through 7.5 shall apply to the execute features.

7.1 Automatic control

Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4, item d) of the design basis.

7.2 Manual control

If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.

7.3 Completion of protective action

The design of the execute features shall be such that, once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (i.e., cycling) of specific equipment to maintain completion of the safety function.

7.4 Operating bypass

Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:

a) Remove the appropriate active operating bypass(es).
b) Restore plant conditions so that permissive conditions once again exist.
c) Initiate the appropriate safety function(s).

7.5 Maintenance bypass

The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero[10]), the remaining portions provide acceptable reliability.

[10]Redundancy of one: 1 out of 2; 2 out of 3; 4 our of 4; etc. Redundancy of zero: 1 out of 1; 2 out of 2; 3 out of 3; etc.

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

8. Power source requirements

8.1 Electrical power sources

Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1991.

8.2 Non-electrical power sources

Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.[11] [B4, B5]

8.3 Maintenance bypass

The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero[12]), the remaining portions provide acceptable reliability.

[11]See [B4] and [B5], Annex C for additional information.
[12]See footnote 10.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A

(informative)

Illustration of some basic concepts for developing the scope of a safety system

A.1 Purpose

The purpose of this annex is to provide a better understanding of the intended application of this standard by utilizing some basic concepts in the development of the total scope of a safety system.

A.2 Discussion

The most fundamental and obvious starting point is to identify the concept of a safety function.

It can be seen from any typical accident analysis that more than one safety function may be required to mitigate some design basis events. Figure A.l illustrates, in a very simplistic fashion, examples of the safety functions required for one particular design basis event, a loss of coolant accident (LOCA). These safety functions include, but are not limited to

a) Emergency negative reactivity insertion
b) Emergency core cooling
c) Post-accident radiation removal
d) Containment isolation
e) Post-accident heat removal

A.3 Typical safety system scope development

By definition, a safety system shall encompass all of the elements required to achieve a safety function.

The emergency core cooling function is used to illustrate a typical safety system. Figure A.2 illustrates a typical safety system block diagram. Figure A.3 illustrates the conversion of this block diagram from a generic safety system to specific elements required to provide emergency core cooling.

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

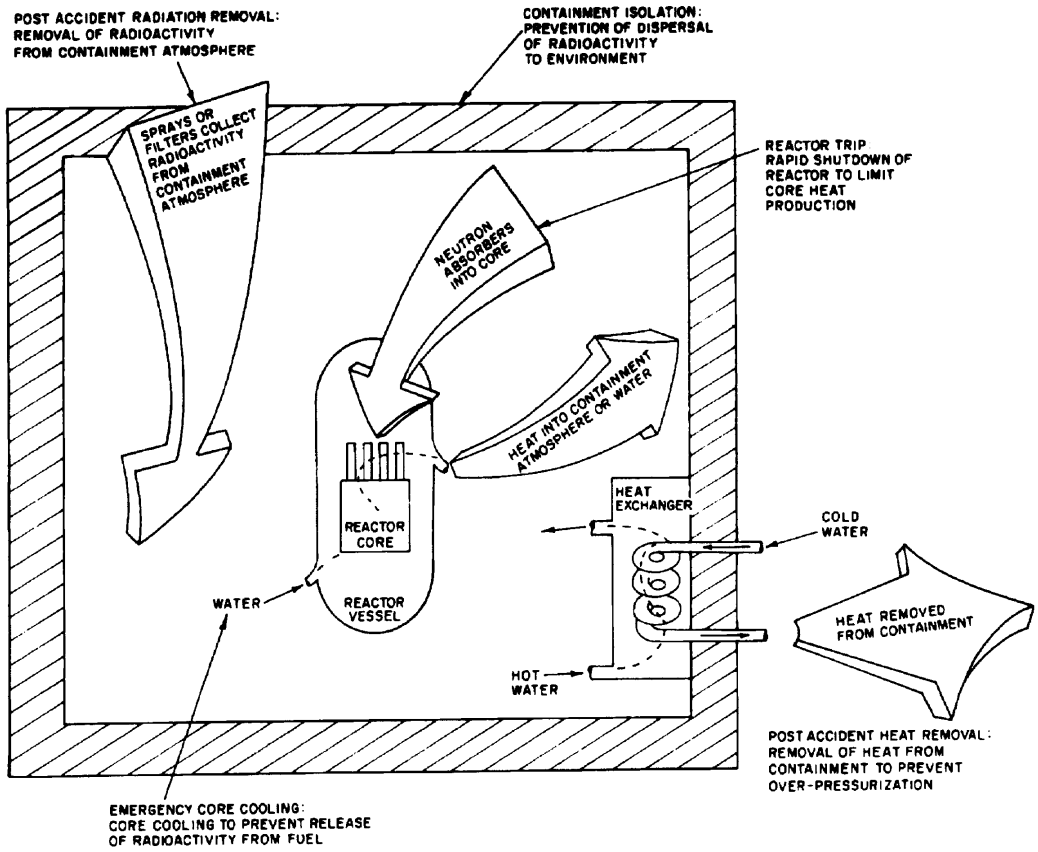


Figure A.1—Power water reactors loss of coolant accident (LOCA) safety functions

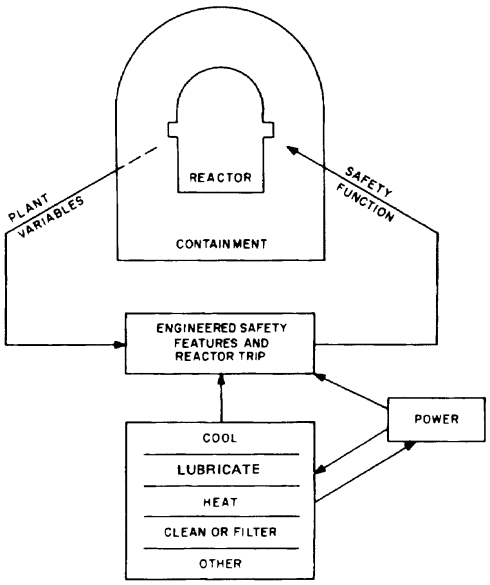


Figure A.2—Typical safety system block diagram

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale
Copyright © 1998 IEEE. All rights reserved.

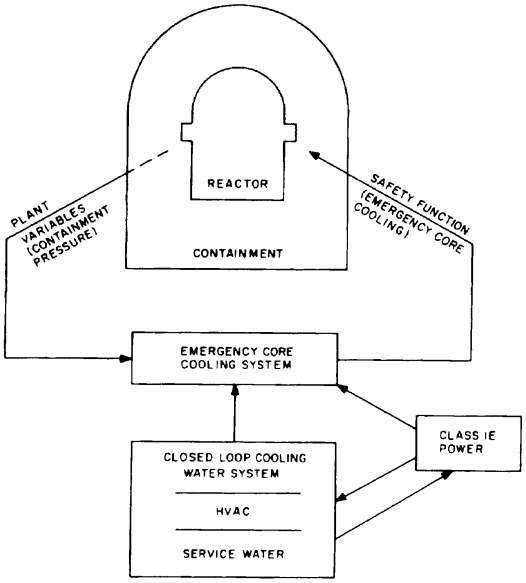


Figure A.3—Elements for emergency core cooling

Figures A.4 through A.8 illustrate, in flow diagram and one-line format for one division of a safety system, an orderly buildup of elements required to achieve emergency core cooling. Figure A.4 starts with the bare reactor. Figure A.5 adds the emergency core cooling system (ECCS) sense and command features. Figure A.6 adds the ECCS execute features. The ECCS pumps, heat exchangers, storage tanks, valves, piping, instrumentation, and controls constitute the engineering safety features portion of this safety system. Figure A.7 adds a part of the auxiliary supporting features, specifically the service water, closed loop cooling water (CLCW), and area coolers. Figure A.8 completes this division of the safety system by adding the rest of the auxiliary supporting features, specifically the Class 1E power.

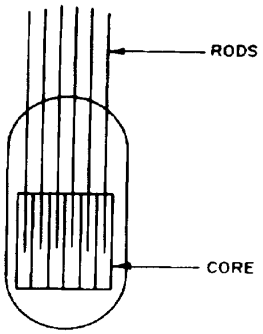


Figure A.4—Elements for emergency core cooling—Reactor

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

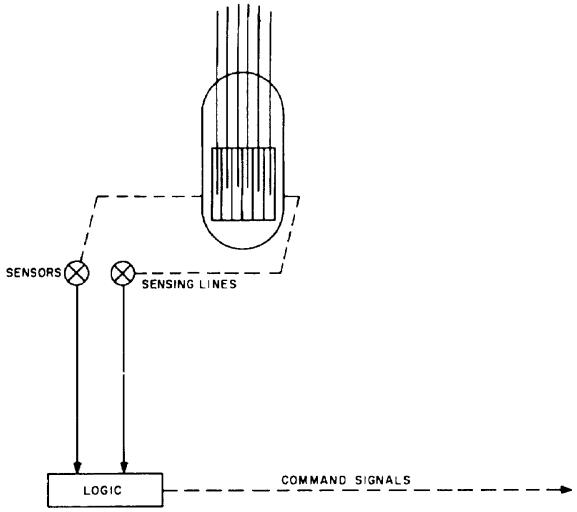


Figure A.5—Elements for emergency core cooling—Addition of sense and command features

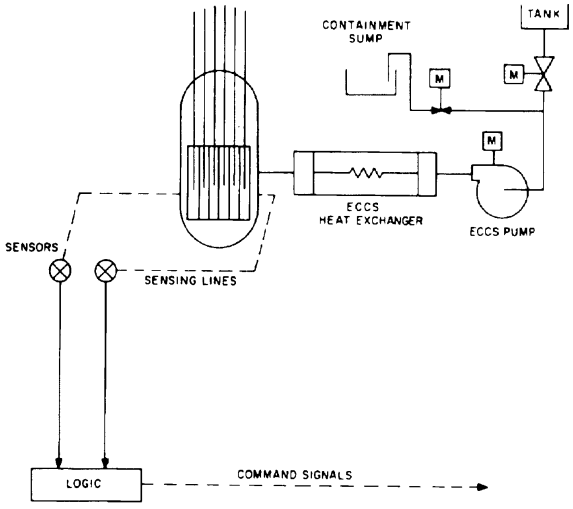


Figure A.6—Elements for emergency core cooling—Addition of execute features

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

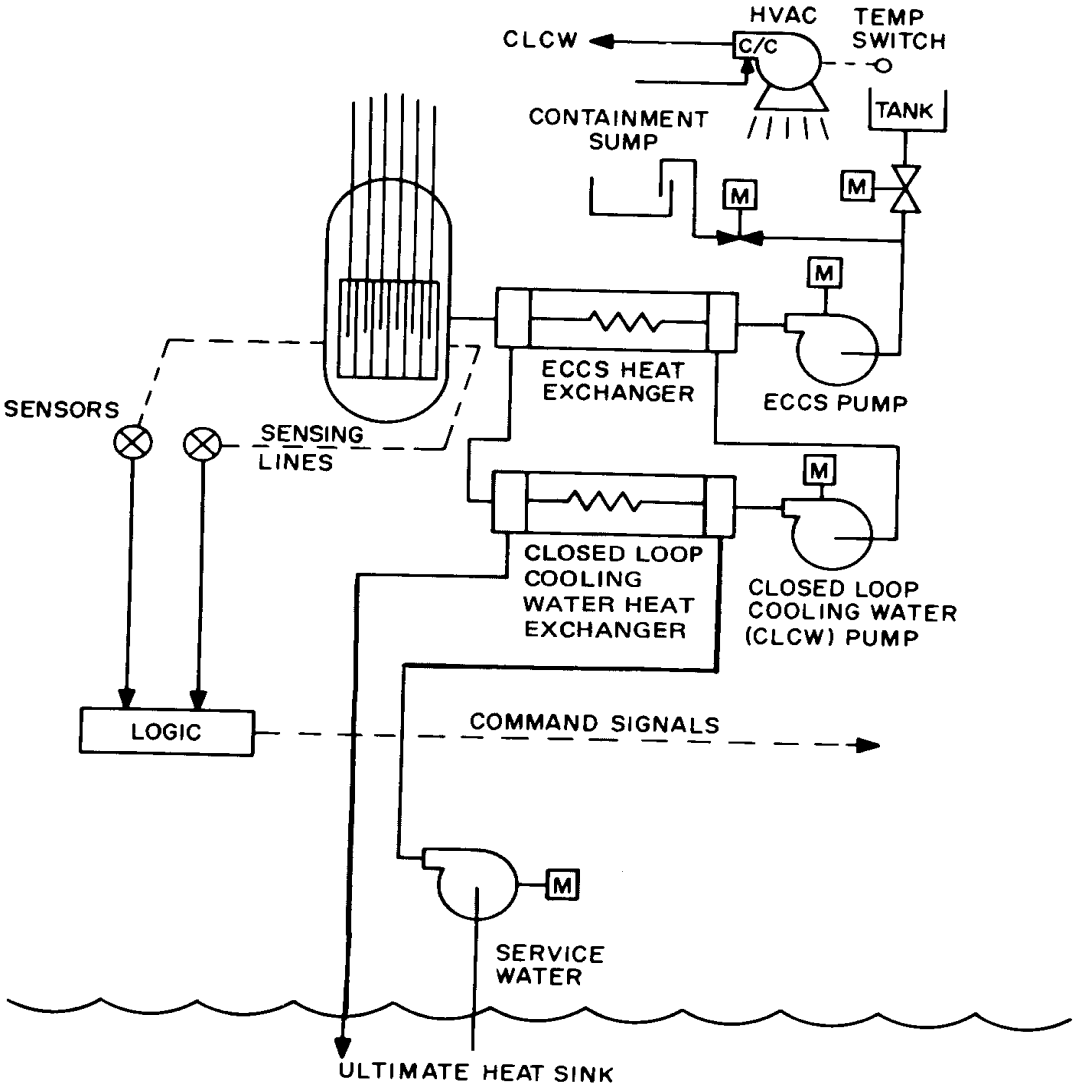


Figure A.7—Elements for emergency core cooling—Addition of some auxiliary supporting features

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

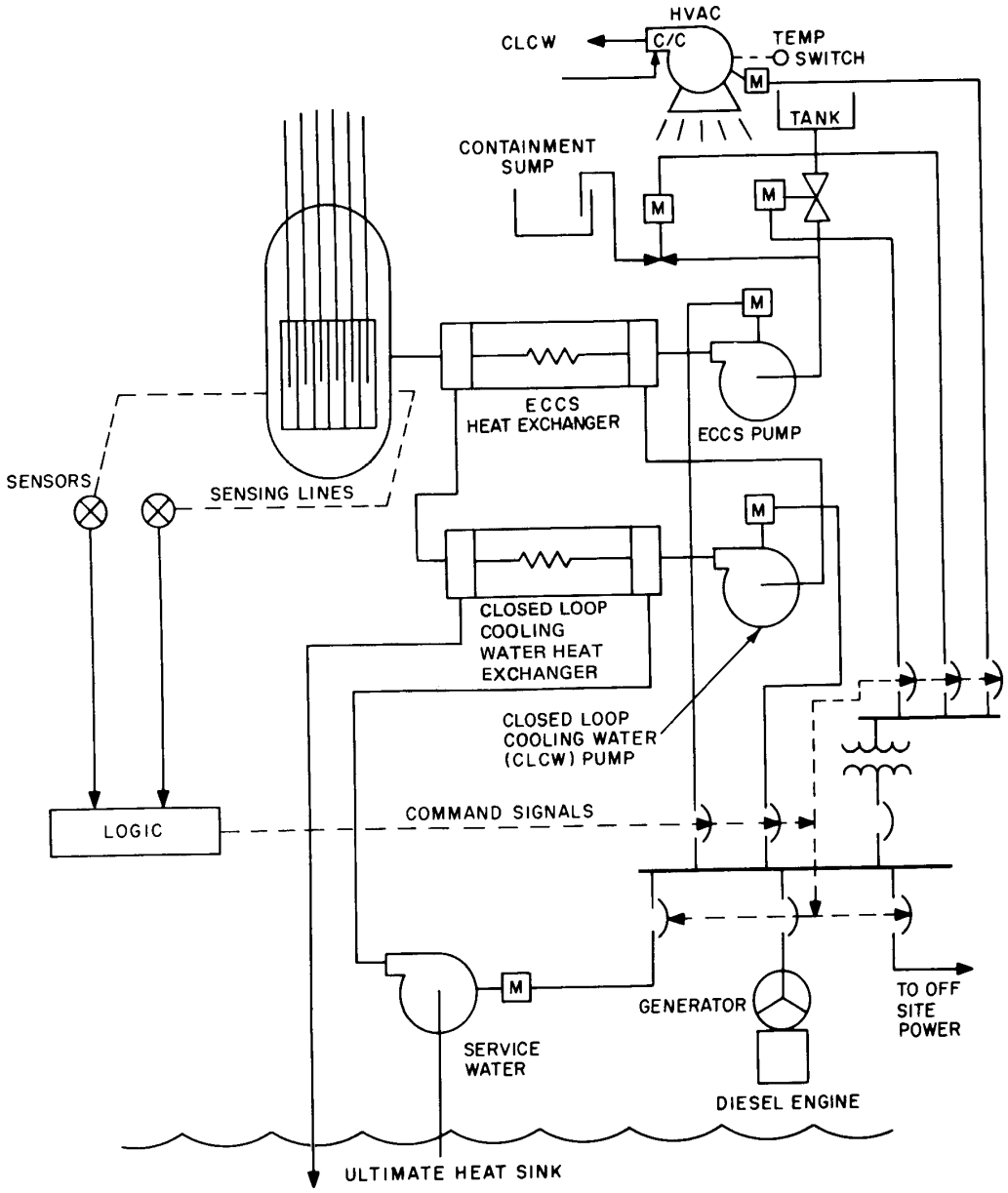


Figure A.8—Elements for emergency core cooling—Addition of Class 1E power

A.4 Safety group

A safety group is a given minimal set of interconnected components, modules, and equipment that can accomplish a safety function. In a design where each division can accomplish the safety function, each division is a safety group, as shown in Figure A.9. However, a design consisting of three 50% capacity systems separated into three divisions would have three safety groups, each safety group requiring that any two out of

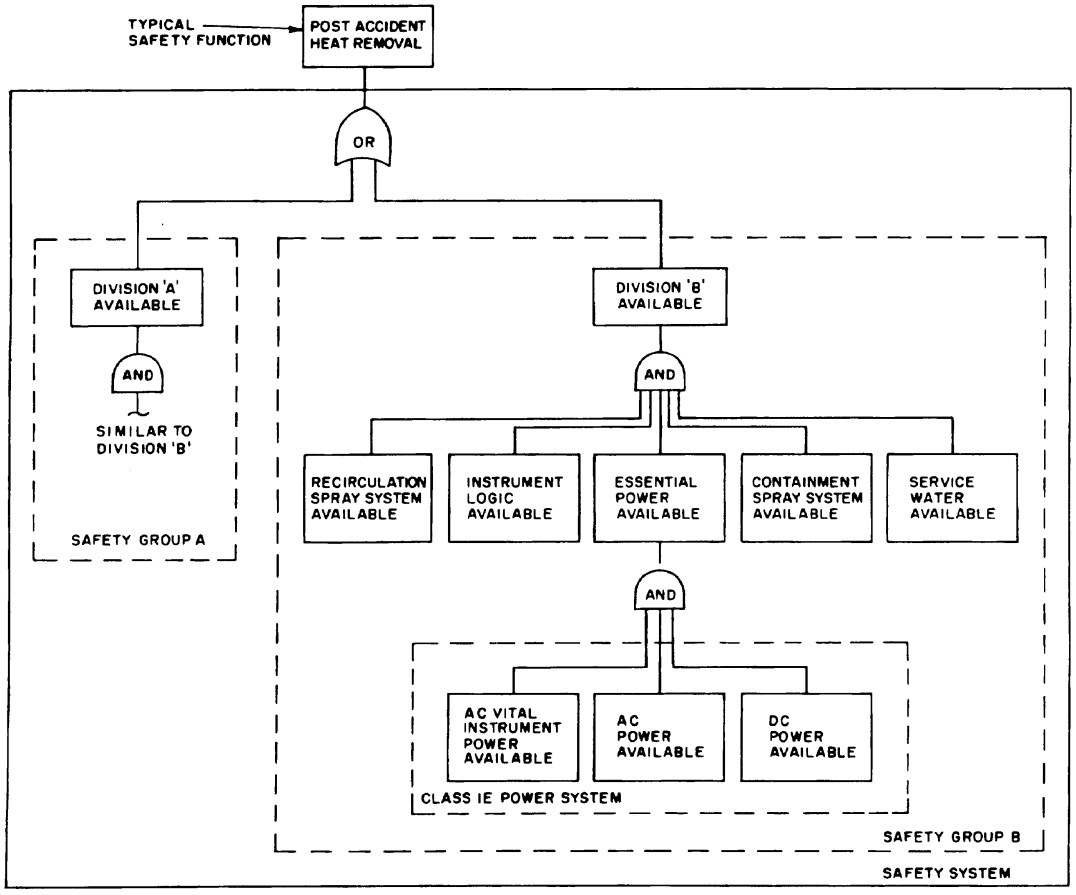
Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

three divisions be operating to accomplish the safety function. The safety groups would then be identified by the logic in Figure A.10.

A.5 Other auxiliary features

Included in the design of most safety systems are components and equipment whose primary function is to increase the availability or reliability of the safety system without directly performing a safety function. These components include, but are not limited to, equipment protection devices, built-in test equipment, isolation devices, etc., as shown in Figure 3. As described in 5.12, these portions of the safety system shall meet only those requirements in this standard required to ensure that they do not degrade the safety system below an acceptable level. Examples of safety system criteria that such portions might not have to meet are operating bypass, maintenance bypass, and bypass indication.

To illustrate the application of these criteria, protective relaying on a Class 1E bus is considered. One function of this protective relaying is to increase the availability and reliability of the Class 1E power system, but from the safety system viewpoint, the essential function is to prevent a spurious tripping when safety system operation is required. Performance of this essential function falls under the criteria of this standard; requirements for the function of increasing the availability and reliability of the Class 1E power system are contained in IEEE Std 308-1991.

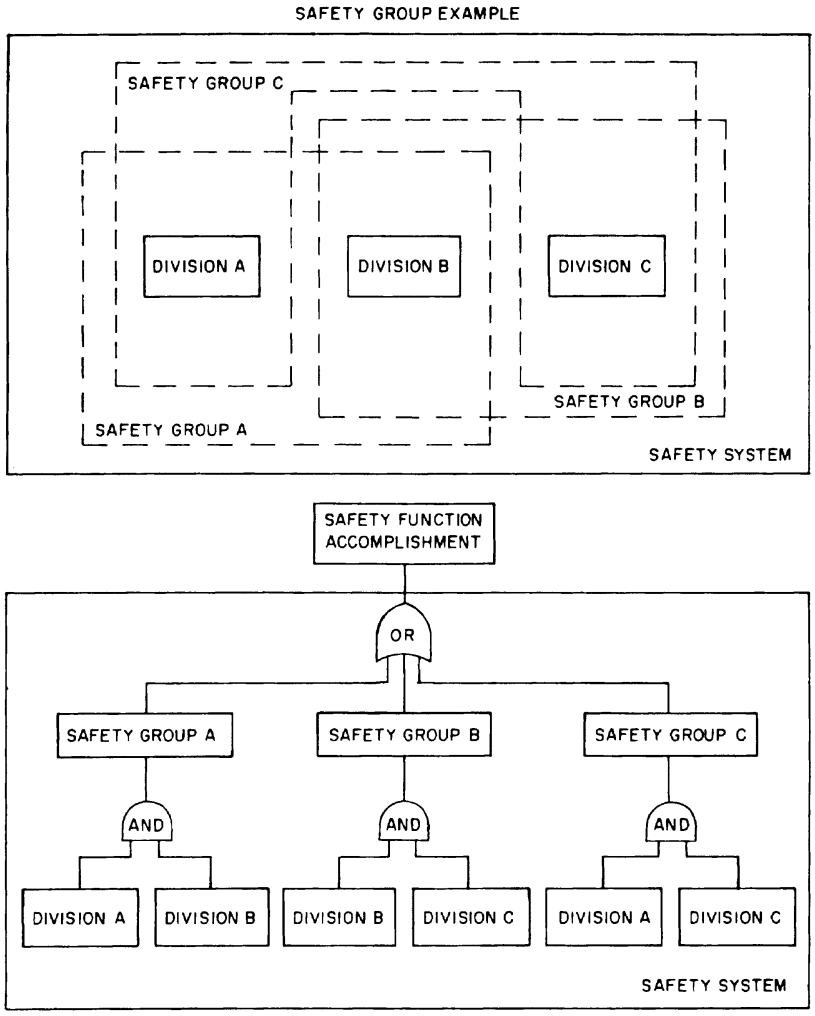


NOTE—Each division consists of a 100% capacity system. Therefore, one division is needed for each safety group to accomplish the safety function.

Figure A.9—Typical safety function

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale



NOTE—Each division consists of a 50% capacity system. Therefore, two divisions are needed for each safety group to accomplish the safety function.

Figure A.10—Safety group example

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B

(informative)

Electromagnetic compatibility

B.1 Background

The need to consider the electromagnetic environment is due to the sensitivity and vulnerability of components (analog and digital) to electromagnetic interference (EMI). This could result in the component's incorrect operation or damage.

Clause 4 item g) requires consideration of the electromagnetic environment in the definition of the safety system design basis conditions. Subclause 5.5 requires that the system be designed to perform its safety function when subjected to all conditions, external or internal, that create hazards, including EMI. This annex provides guidance for this consideration and references other documents for definition and performance.

B.2 Discussion

EMI may result from several coupling mechanisms. These coupling mechanisms should be considered in the definition of the electromagnetic environment, in the EMI testing of equipment, and in the instrumentation and control system design.

B.2.1 Definition of the electromagnetic environment

The electromagnetic environment may be determined by measurements and/or analysis. Guidance for measuring the electromagnetic environment may be found in the following standards and guides:

— IEEE Std 473-1985 (Reaff 1997), IEEE Recommended Practice for Electromagnetic Site Survey (10 kHz to 10 GHz).
— MIL-STD-462 INT Notice 5, Measurement of Electromagnetic Interference Characteristics.

B.2.2 Evaluation of the electromagnetic environment

Safety system equipment must be designed to perform its safety function when subjected to the nuclear power generating station's electromagnetic environment. This requires consideration of the following four coupling mechanisms-conductive, radiative, inductive, and capacitive, as well as electrostatic discharge (ESD).

a) *Conductive coupling*. A significant majority of all noise is conductively coupled. There are three properties with conductive coupling. They are as follows:
   1) Metallic contact is required.
   2) Noise is unaffected by people or cable movement.
   3) Noise waveform will have a non-zero average value (dc signal component).
   4) Conductive coupling can be eliminated by breaking or removing the metallic contact or by filtering out the noise.
b) *Radiative coupling*. Radiative coupling is known as electromagnetic radiation or radio frequency coupling, which occurs at distances one-sixth of a wavelength or greater. This coupling is usually

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

only a high-frequency concern where wavelengths are small enough to be coupled over short distances, such as a cable or any antennalike device. The electromagnetic field strength is inversely proportional to the distance of the source and proportional to the square root of the transmitted power. The only method for preventing radiative coupling noise is through shielding techniques, which either absorb or reflect the propagated wave. To have effective shielding, the shield shall completely encompass the conductors in order to shield against any propagating waves.

c) *Inductive coupling*. Inductive or electromagnetic coupling occurs when the noise and signal circuits or conductors experience changing currents and have mutual inductance. The energy (induced voltage) produced by this electromagnetic field is proportional to the change in current divided by the change in time (di/dt), and the length and axial displacement of the conductors.

Some identifiable properties of inductive coupling noise are as follows:
— It has high noise frequency or current (power cables)
— It has excessive wiring inductance
— It is not affected by nonconducting materials
— It provides a detectable magnetic field

Methods for eliminating inductive coupling noise include the following:
— Reduce the noise frequency or current sources
— Reduce mutual inductance (loop area and proximity of the conductors)
— Filter or shield against the noise

d) *Capacitive coupling*. Capacitive coupling is due to an electric field (changing voltage) between metal surfaces in the signal and noise circuits. Therefore, capacitive coupling is dependent on the surface area of the metals, spacing, impedance, and dielectric. Some identifying properties are as follows:
— High noise voltage relative to signal voltage
— Metal surfaces forming capacitance
— High impedance signal circuit
— Noise is affected by cable or people movement

There are several solutions for eliminating capacitive coupling noise. They are as follows:
— Attenuate the voltage or reduce the frequency of the noise source
— Reduce the coupling capacitance (surface area)
— Reduce the circuit impedance
— Use shielding

Performance may be demonstrated by a combination of testing, analysis, or documented operating experience in a similar environment. These activities need to consider the total system design, including design features that reduce equipment susceptibilities such as twisted cable, shielded cable, fiber optic communications cable and others. Test levels should be sufficient to demonstrate coverage of the expected environment and include sufficient margin for abnormal conditions and events.

Guidance for testing methods may be found in the following standards:

EPRI TR-102323, Guidance for Electromagnetic Interference testing in Power Plants, September 1994.

IEC 60255-3 (1989-06), Electrical Relays—Part 3: Single input energizing quantity measuring relays with dependent or independent time.

IEC 61000-4-1 (1992-12), Electromagnetic Compatibility (EMC)—Part 4: Testing and measurement techniques—Section 1: Overview of immunity tests.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

IEC 61000-4-2 (1995-01), Electromagnetic Compatibility (EMC)—Part 4: Testing and measurement techniques—Section 2: Electrostatic discharge immunity test.

IEC 61000-4-3 (1995-03), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 3: Radiated, radio-frequency, electromagnetic field immunity test.

IEC 61000-4-4 (1995-01), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 4: Electrical fast transient/burst immunity test.

IEC 61000-4-5 (1995-03), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 5: Surge immunity test.

IEC 61000-4-6 (1996-04), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 6: Immunity to conducted disturbances, induced by radio-frequency fields.

IEC 61000-4-7 (1991-08), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 7: General guide on harmonics and interharmonics measurements and instrumentation, for power supply systems and equipment connected thereto.

IEC 61000-4-8 (1993-06), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 8: Power frequency magnetic field immunity test.

IEC 61000-4-9 (1993-06), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 9: Pulse magnetic field immunity test.

IEC 61000-4-10 (1993-06), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 10: Damped oscillatory magnetic field immunity test.

IEC 61000-4-11 (1994-06), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 11: Voltage dips, short interruptions and voltage variations immunity tests.

IEC 61000-4-12 (1995-05), Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 12: Oscillatory waves immunity test.

IEEE Std C62.45-1992 (Reaff 1997), IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits.

MIL-STD-461C Notice 2, Electromagnetic Emission and Susceptibility Requirements for control of Electromagnetic Interference.

B.2.3 System design for electromagnetic interference

System design to provide protection from electromagnetic interference requires the application of appropriate design techniques. These techniques include the following:

a) Shielding
b) Grounding wire selection
c) Wire routing
d) Suppression
e) Filtering
f) Data quality checking
g) Software handling (e.g., software bandpass filtering)

Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Guidance for design may be found in the following standards:

IEEE Std 1050-1996, IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations.

IEEE Std 518-1982 (Reaff 1996), IEEE Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources.

Copyright © 1998 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C

(informative)

Bibliography

Other standards that provide additional information and that may be useful in applying this standard are as follows:

[B1] ANSI/ANS-58.3-1992, Physical Protection for Nuclear Safety-Related Systems and Components.

[B2] ANSI/ANS-58.8-1994, Time Response Design Criteria for Nuclear Safety-Related Operator Actions.

[B3] ANSI/ANS-58.9-1981 (Reaff 1987), Single-Failure Criteria for Light Water Reactor Safety-Related Fluid Systems.

[B4] ANSI/ANS-59.3-1992, Nuclear Safety Criteria for Control Air Systems.

[B5] ANSI/ANS-59.51-1997, Fuel-Oil Systems for Emergency Diesel Generators.

[B6] Code of Federal Regulations, CFR Publication 10 CFR 50.49 (Jan. 1994).

[B7] IEC 60231A (1969-01), First Supplement to General Principles of Nuclear Reactor Instrumentation.

[B8] IEEE Std 279-1971 (withdrawn), IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations.[13]

[B9] IEEE Std 494-1974 (withdrawn), IEEE Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations.[14]

[B10] IEEE Std 497-1981 (withdrawn), IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.[15]

[13]IEEE Std 279-1971 has been withdrawn; however, copies can be obtained from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5704, USA, tel. (303) 792-2181 (global..ihs.com/).

[14]IEEE Std 494-1974 has been withdrawn. See footnote 13.

[15]IEEE Std 497-1981 has been withdrawn. See footnote 13.

--`,,`-`-`,,`,,`,`,,`---
Copyright © 1998 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale