IEEE Std 603-1991
(Revision of ANSI/IEEE Std 603-1980)

IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

Sponsor
Nuclear Power Engineering Committee
of the
IEEE Power Engineering Society

Approved June 27, 1991

IEEE Standards Board

Abstract: Establishes minimum functional design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems. 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, preventive interlock features, or any other systems, structures, or equipment related to safety.
Keywords: Actuated equipment, associated circuits, Class 1E, design, failures, maintenance bypass, operating bypass, protection, 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

ISBN 1-55937-144-7

IEEE Standards documents are developed within the Technical Committees of 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 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 technical 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

Foreword

(This Foreword is not a part of IEEE Std 603-1991, 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 shall be recognized that the safety functions cannot be accomplished without mechanical, as well as electrical equipment and circuitry. Therefore, the design by other than electrical engineering disciplines, primarily mechanical and nuclear engineering, 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. 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 Fig 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 is to provide 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 52.2-1983) 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.

Evolution

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

protection system standard; IEEE Std 603-1977, a trial-use standard for safety systems; and IEEE Std 603-1980, a full safety system standard.

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.

Purpose of Revision

During the development of IEEE Std 603-1980, six future tasks were identified. Those tasks have been completed. The result is that changes to the Standard were found to be important regarding some definitions and criteria for shared systems. In addition, position papers were prepared and presented at Power Engineering Society meetings on safe shutdown (IEEE-PES-WM 1983) and automatic termination of protective action (IEEE-PES-SM 1985). A position paper on diversity has been prepared and is planned for presentation in the near future.

The American National Standards Institute endorsed IEEE Std 603-1980 in 1987. Their endorsement took the form of a published correction sheet designated ANSI/IEEE Std 603-1980. It included mostly editorial changes, some changes in references and a few text clarifications. The corrections by ANSI have been addressed in this revision.

The U.S. Nuclear Regulatory Commission endorsed IEEE Std 603-1980 with Regulatory Guide 1.153 in December 1985. R.G. 1.153 stated five modifications/supplements to IEEE Std 603-1980. Three of the USNRC items resulted in changes included in this revision. They deal with clarification of Fig 6 of this standard, clarification of the criteria for interaction between sense and command features and other systems, and a change in the language used in the definition of safety system. The definition of the term “safety system” now agrees with that used in Section 50.49 of 10 CFR 50. The two other USNRC items deal with how the NRC will use standards referenced in IEEE Std 603 and did not result in changes in the document.

The Instrument Society of America asked that the determination of setpoints be consistent with how they specify them in standard ISA S67.04. The standard has been revised to refer to the ISA document for direction.

Other changes included cover consideration of human factors, clarification of the design basis event requirements for critical points in time or the plant conditions, and update of the references.

Future Work

Definitions have been changing in the industry. It will be a future work task for the work group to review the definitions, together with ASME, ANS and the ISA, to standardize terms and maximize clarity.

This document was prepared by the Safety-Related Systems Working Group SC 6.3 of the IEEE Nuclear Power Engineering Committee. The members of the working group were:

Britton P. Grim, *Chair*

W. W. Bowers	R. Kendall	D. Sokolsky
R. L. Copyak	R. L. Olson	D. J. Zaprazny
P. M. Holzman	G. Peterson	

The following persons were on the balloting committee that approved this standard for submission to the IEEE Standards Board:

S. K. Aggarwal
R. E. Allen
J. T. Bauer
F. D. Baxter
W. W. Boweres
D. F. Brosnan
N. M. Burstein
S. P. Carfagno
R. Carruth
G. L. Doman
E. F. Dowling
R. E. Dulski
N. C. Farr
R. Fleming
J. R. Fragola
J. M. Gallagher
W. C. Gangloff
L. W. Gaussa, Sr.
L. C. Gonzalez
L. Gradin
B. P. Grim
A. R. Hall
R. E. Hall
G. K. Henry
S. Kasturi
J. T. Keiper
D. C. Lampken
J. D. LaMont
A. Marion
R. D. Miller
B. Nemroff
M. Pai
J. R. Penland
W. K. Peterson
C. A Petrizzo
N. S. Porter
W. S. Raughley
E. W. Rhoads
A. R. Roby
W. G. Schwartz
A. F. Sleva
P. B. Stevens
P. Szabados
L. D. Test
J. E. Thomas
J. T. Ullo
F. J. Volpe

When the IEEE Standards Board approved this standard on June 27, 1991, it had the following membership:

Marco W. Migliaro, *Chair*
Donald C. Loughry, *Vice Chair*
Andrew G. Salem, *Secretary*

Dennis Bodson
Paul L. Borrill
Clyde Camp
James M. Daly
Donald C. Fleckenstein
Jay Forster*
David F. Franklin
Ingrid Fromm
Thomas L. Hannan
Donald N. Heirman
Kenneth D. Hendrix
John W. Horch
Ben C. Johnson
Ivor N. Knight
Joseph L. Koepfinger*
Irving Kolodny
Michael A. Lawler
John E. May, Jr.
Lawrence V. McCall
Donald T. Michael*
Stig L. Nilsson
John L. Rankine
Ronald H. Reimer
Gary S. Robinson
Terrance R. Whittemore

Deborah A. Czyz
IEEE Standards Project Editor

*Member Emeritus

CLAUSE PAGE

CLAUSE PAGE

IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

1. Scope

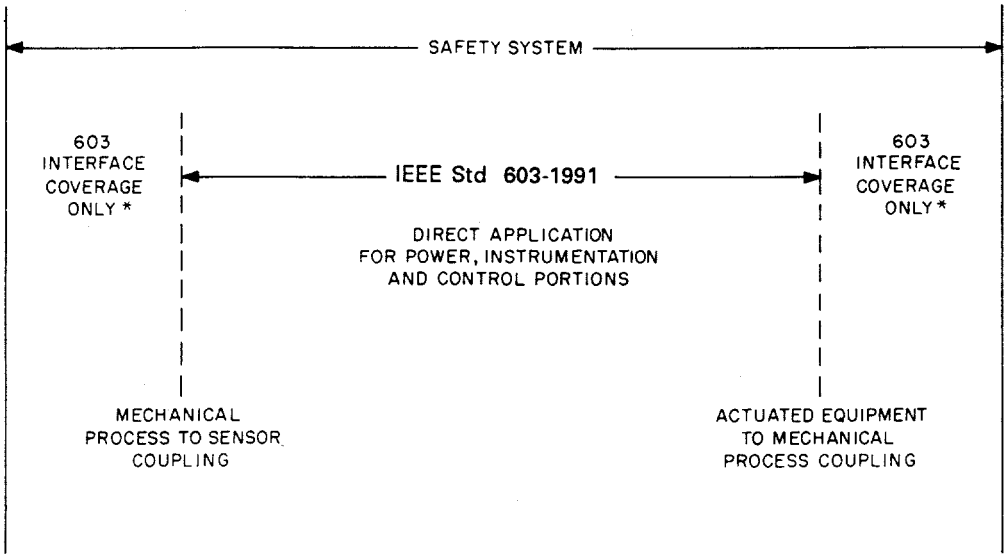
The criteria contained in this standard establish minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power generating stations. To satisfy the criteria in this standard, interface requirements may be imposed on the other portions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

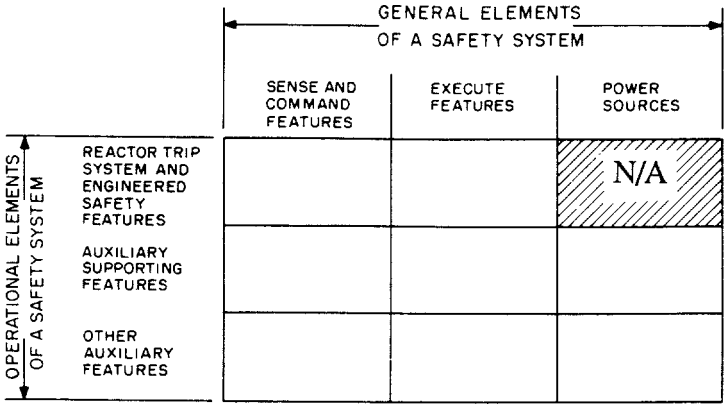
Illustrating the scope of this standard in matrix form shows that each operational element contains one or more general elements. This matrix should not be interpreted to mean that every operational element shall contain all of the general elements or that a particular general element is limited to application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

[1]See Section 3 and Appendix B for applicable standards.



*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 (withdrawn) 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 (for example, 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 devices 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

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.

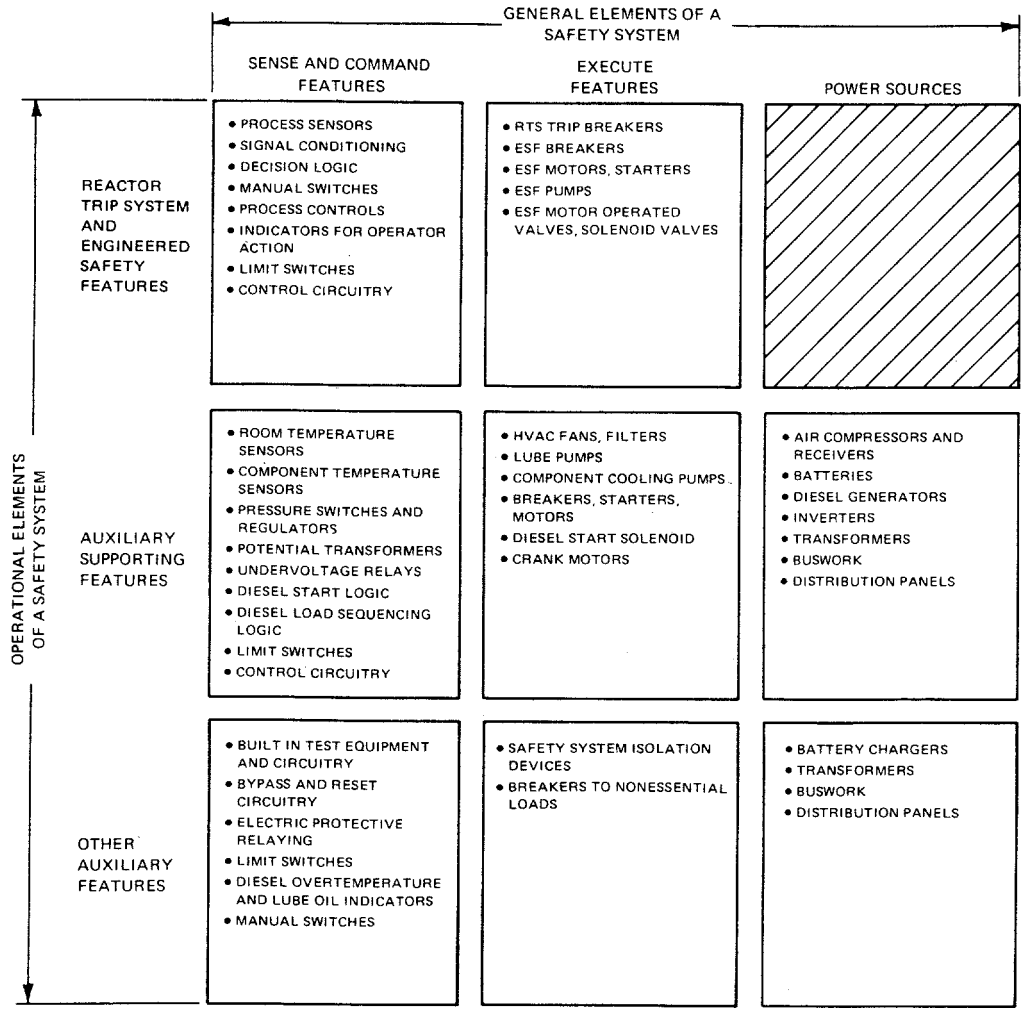
Figure 4 illustrates where criteria for each portion of the matrix can be found in this standard.

1.2 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.

Guidance on the application of these criteria for safety systems using digital programmable computers is provided in IEEE/ANS 7.4.3.2-1982 [13][2].

[2]The numbers in brackets correspond to those of the references listed in Section 3.

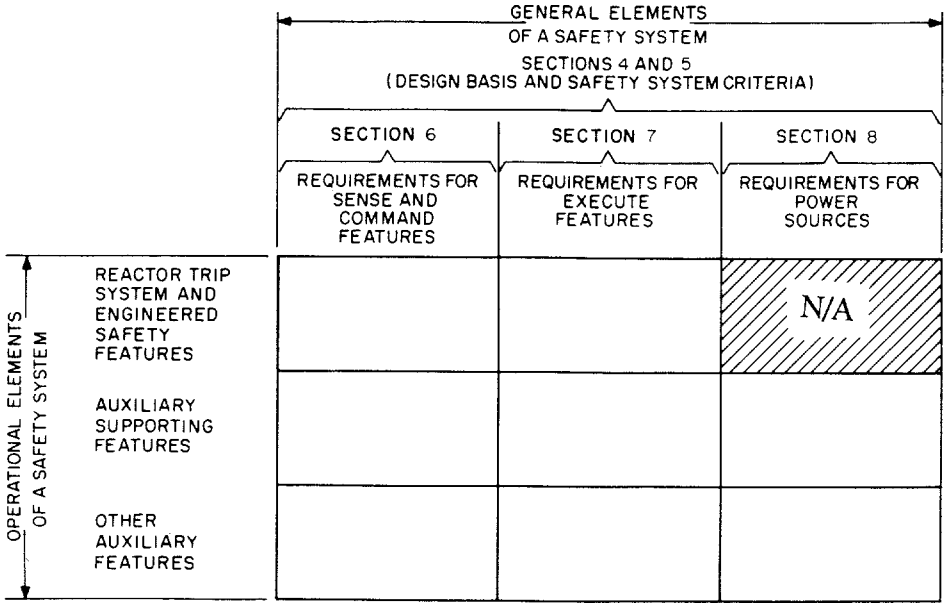


NOTES:

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

2 — See Fig 2 for additional notes.

Figure 3—Examples of Equipment Fitted to Safety System Scope Diagram



NOTE — See Fig 2 for notes.

Figure 4—Scope Diagram for IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Generating Stations

2. Definitions

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

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

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.

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

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

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

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

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.

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.

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.

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.

components: Discrete items from which a system is assembled.

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

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

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 379–1988 [5].

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.

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).

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 by pass 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.

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.

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 (for example, prevention of initiation of emergency core cooling during the cold shutdown mode).

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

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

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.

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 — Redundancy can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.

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 Appendix A for an illustrative example.)

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 Appendix A for an illustrative example).

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

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

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.

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 or pneumatic signal.

3. References

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

[1] IEEE Std 308–1980, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations (ANSI).[3]

[2] IEEE Std 323–1983, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations (ANSI).

[3] IEEE Std 338–1987, IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems (ANSI).

[4] IEEE Std 352–1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems (ANSI).

[5] IEEE Std 379–1988, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (ANSI).

[6] IEEE Std 384–1981, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (ANSI).

[7] 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.

[8] IEEE Std 494–1974 (R1990), IEEE Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations (ANSI).

[3] IEEE publication are available from the Institution of Electrical and Electronics Engineers, Inc., Service Center, 445 Hoes Lane, Piscataway, NJ 08854–1331, U.S.A.

[9] IEEE Std 497–1981, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations (ANSI).

[10] IEEE Std 577–1976 (R1986), IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations (ANSI).

[11] IEEE Std 627–1980, IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations (ANSI).

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

[13] IEEE/ANS 7.4.3.2–1982, American Nuclear Society and IEEE Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations (ANSI).

[14] ANSI/ANS 51.1–1983 (R1988), Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.[4]

[15] ANSI/ANS 52.1–1983 (R1988), Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants.

[16] ANSI/ASME NQA-1–1989, Quality Assurance Program Requirements for Nuclear Facilities.[5]

[17] Title 10, Code of Federal Regulations, Part 100, “Reactor Site Criteria.”

[18] ISA S67.04–1987, Setpoints for Nuclear Safety-Related Instrumentation.

4. Safety System Designation

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 [14] or ANSI/ANS 52.1–1983 [15] and shall document as a minimum:

4.1

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.

4.2

The safety functions and corresponding protective actions of the execute features for each design basis event.

[4]ANSI/ANS publication are available from the American National Standards Institute, Sales Department, 11 West 42nd Street, New York, NY 10036, U.S.A., or from the American Nuclear Society, 555 N. Kensington Ave., Grange Park, IL 60525, U.S.A.
[5]ANSI/ASME publications are available from the American National Standards Institute, Sales Department, 111 West 42nd Street, New York, NY 10036, U.S.A., or from the American Society of Mechanical Engineers, Order Department, 22 Law Drive, Box 2300, Fairfield, NJ 07007–2300, U.S.A.

4.3

The permissive conditions for each operating bypass capability that is to be provided.

4.4

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.

4.5

The following minimum criteria for each action identified in 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. See IEEE Std 494–1974 (R1990) [8].[6]

4.5.1

The points in time and the plant conditions during which manual control is allowed.

4.5.2

The justification for permitting initiation or control subsequent to initiation solely by manual means.

4.5.3

The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.

4.5.4

The variables in 4.4 that shall be displayed for the operator to use in taking manual action.

4.6

For those variables in 4.4 that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.

4.7

The range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform.

4.8

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 (for example, missiles, pipe breaks,

[6] See [B1] , Appendix B for additional information.

fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).

4.9

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.

4.10

The critical points in time or the plant conditions, after the onset of a design basis event, including:

4.10.1

The point in time or plant conditions for which the protective actions of the safety system shall be initiated.

4.10.2

The point in time or plant conditions that define the proper completion of the safety function.

4.10.3

The points in time or the plant conditions that require automatic control of protective actions.

4.10.4

The point in time or the plant conditions that allow returning a safety system to normal.

4.11

The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.

4.12

Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).

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 Appendix 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. (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis

event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379–1988 [5] provides guidance on the application of the single-failure criterion.[B2]

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 [B2] . The performance of a probable 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 probable 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 [4] and IEEE Std 577–1976 [10] 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 4.9 of the design basis, a probable 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 4.11 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 (ANSI/ASME NQA1–1989 [16]).

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 [2] and IEEE Std 627–1980 [11].

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.

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 to accomplish 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 to meet 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 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.

5.6.3.1 Interconnected Equipment

1) **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.
2) **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

1) **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 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 384–1981 [6] [B3] .
2) **Barriers:** 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 4.7 and 4.8 of the design basis.

5.6.3.3 Effects of a Single Random Failure

Where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) 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 379-1988 [5] for the application of this requirement.

5.6.4 Detailed Criteria

IEEE Std 384-1981 [6] provides detailed criteria for the independence of Class 1E equipment and circuits [B3] .

5.7 Capability for Test 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 [3]. 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:

1) appropriate justification shall be provided (for example, demonstration that no practical design exists),
2) acceptable reliability of equipment operation shall be otherwise demonstrated, and
3) 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 that are 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 [9]. 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.

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.

5.8.3.1

This display instrumentation need not be part of the safety systems.

5.8.3.2

This indication shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year, and (b) is expected to occur when the affected system is required to be operable.

5.8.3.3

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 effect 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:

1) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981 [6] and IEEE Std 420-1982 [7].
2) 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.
3) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).
4) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.
5) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 (R1990) [8].

5.12 Auxiliary Features

5.12.1

Auxiliary supporting features shall meet all requirements of this standard.

5.12.2

Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, 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 Fig 3 and an illustration of the application of this criteria is contained in Appendix 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 308-1980 [1]. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1988 [5].

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 [12].

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 [4] and IEEE Std 577-1976 [10] provide guidance for reliability analysis.

6. Sense and Command Features—Functional and Design Requirements

In addition to the functional and design requirements in Section 5, the following requirements 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 4.5. 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 4.5 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 4.5.

6.2 Manual Control

6.2.1

Means shall be provided in the control room to 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.

6.2.2

Means shall be provided in the control room to implement manual initiation and control of the protective actions identified in 4.5 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.

6.2.3

Means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in 4.10. 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

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:

1) 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:
   a) Channels that sense a set of variables different from the principal channels.
   b) Channels that use equipment different from that of the principal channels to sense the same variable.
   c) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.Both the principal and alternate channels shall be part of the sense and command features.
2) 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 Fig 5 for a decision chart for applying the requirements of this section.

6.3.2

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.

6.5 Capability for Testing and Calibration

6.5.1

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:

1) by perturbing the monitored variable,
2) 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
3) by cross-checking between channels that bear a known relationship to each other and that have readouts available.

6.5.2

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:

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

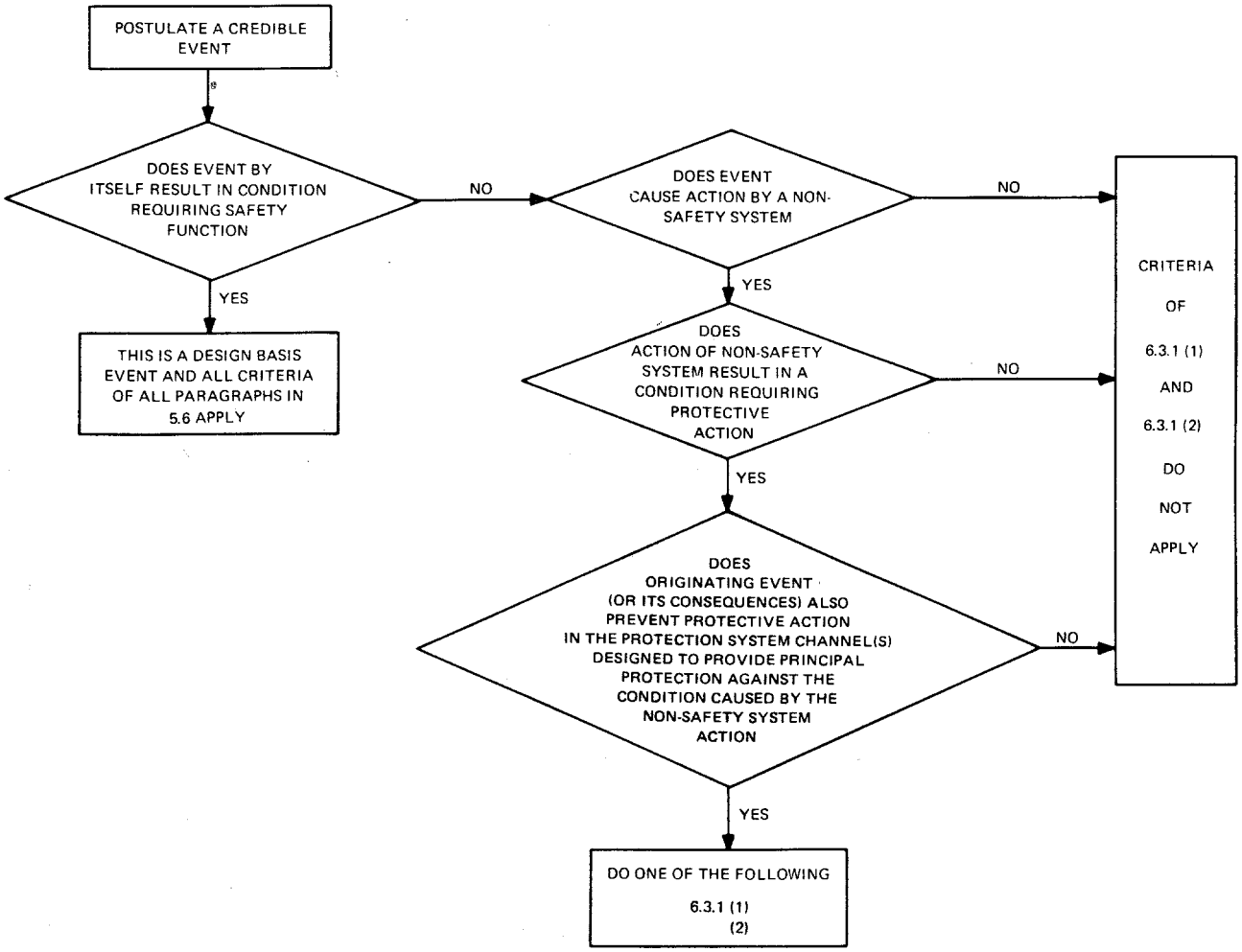


Figure 5—Interpretation of 6.31 of IEEE Std 603-1991

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:

1) Remove the appropriate active operating bypass(es).
2) Restore plant conditions so that permissive conditions once again exist.
3) 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 shall continue to meet the requirements of 5.1 and 6.3.

EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).

6.8 Setpoints

6.8.1

The allowance for uncertainties between the process analytical limit documented in Section 4.4 and the device setpoint shall be determined using a documented methodology. Refer to ISA S67.040-1987 [18].

6.8.2

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 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. Executive Features—Functional and Design Requirements

In addition to the functional and design requirements in Section 5, the following requirements 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 4.4 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 4.11 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 (that is, 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:

1) Remove the appropriate active operating bypass(es).
2) Restore plant conditions so that permissive conditions once again exist.
3) 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 (that is, reducing temporarily its degree of redundancy to zero)[7], the remaining portions provide acceptable reliability.

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 308-1980 [1].

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. [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 (that is, reducing temporarily its degree of redundancy to zero[8]), the remaining portions provide acceptable reliability.

[7]Redundancy of one: 1 out of 2; 2 out of 3; 3 out of 4; etc. Redundancy of zero: 1 out of 1; 2 out of 2; 3 out of 3; etc.
[8] Redundancy of one: 1 out of 2; 2 out of 3; 3 out of 4, etc. Redundancy of zero: 1 out of 1; 2 out of 2; 3 out of 3, etc.

Annex A Illustration of Some Basic Concepts for Developing the Scope of a Safety System

(Informative)

A1. Purpose

The purpose of this Appendix 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.

A2. 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.1 illustrates, in 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:

1) Emergency negative reactivity insertion
2) Emergency core cooling
3) Post-accident radiation removal
4) Containment isolation
5) Post-accident heat removal

A3. 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.

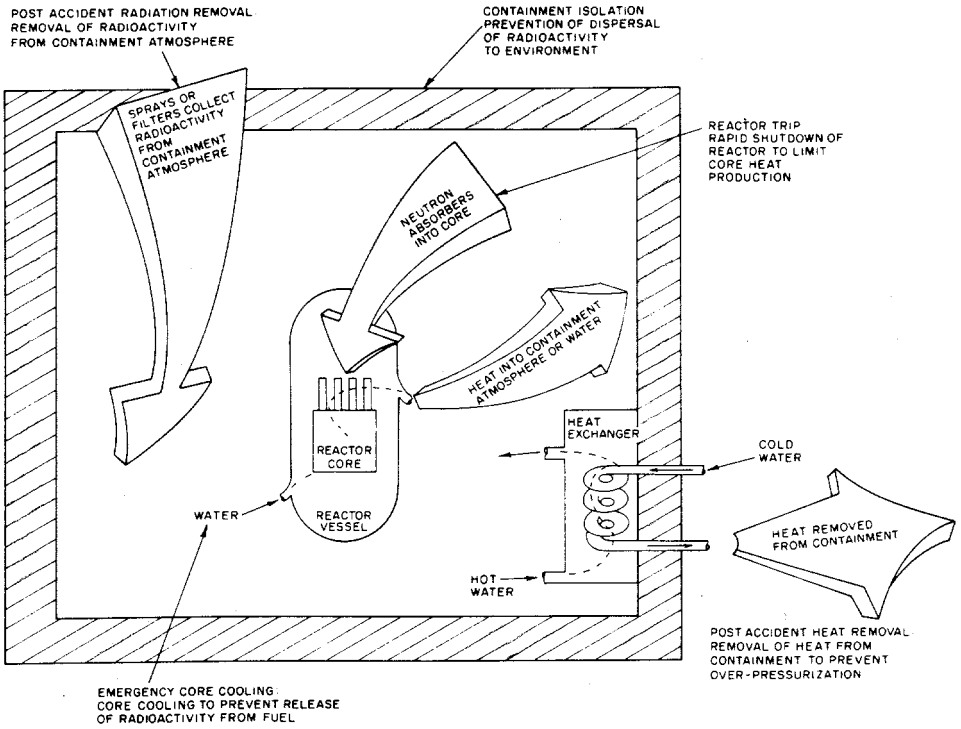


Figure A.1—Power Water Reactors Loss of Coolant Accident (LOCA) Safety Functions

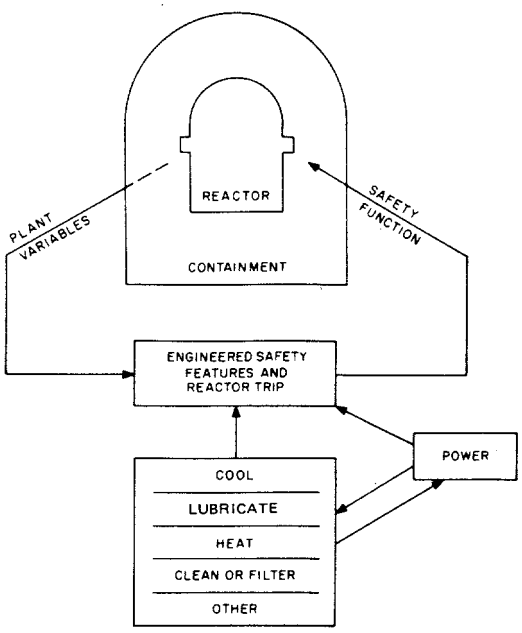


Figure A.2—Typical Safety System Block Diagram

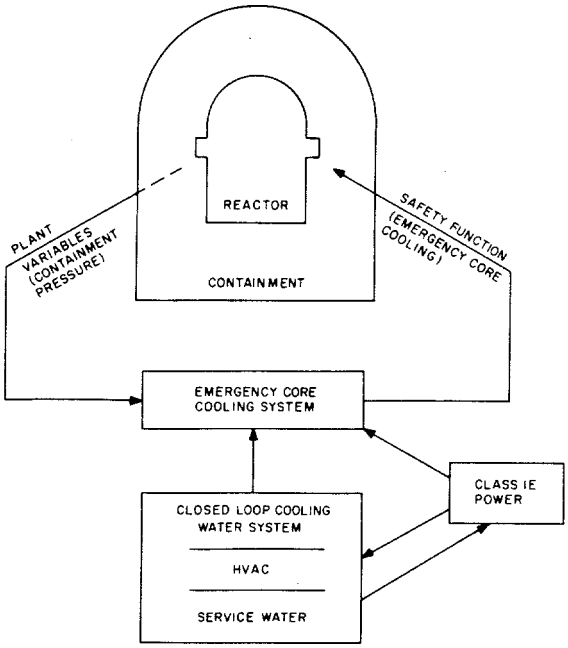


Figure A.3—Elements for Emergency Core Cooling

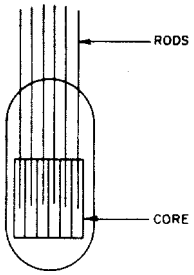


Figure A.4—Elements for Emergency Core Cooling: Reactor

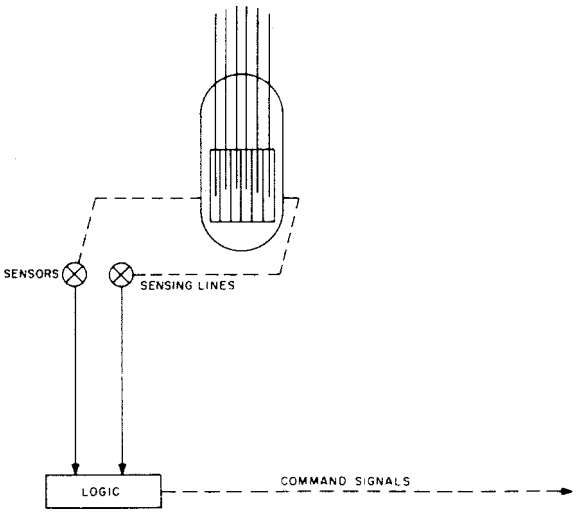


Figure A.5—Elements for Emergency Core Cooling: Addition of Sense and Command Features

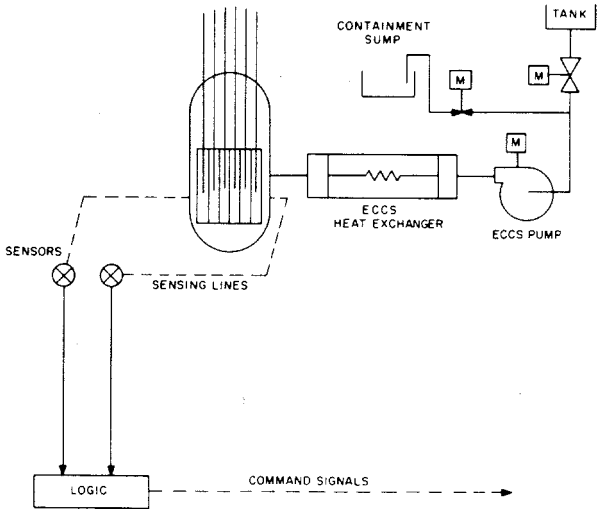


Figure A.6—Elements for Emergency Core Cooling: Addition of Execute Features

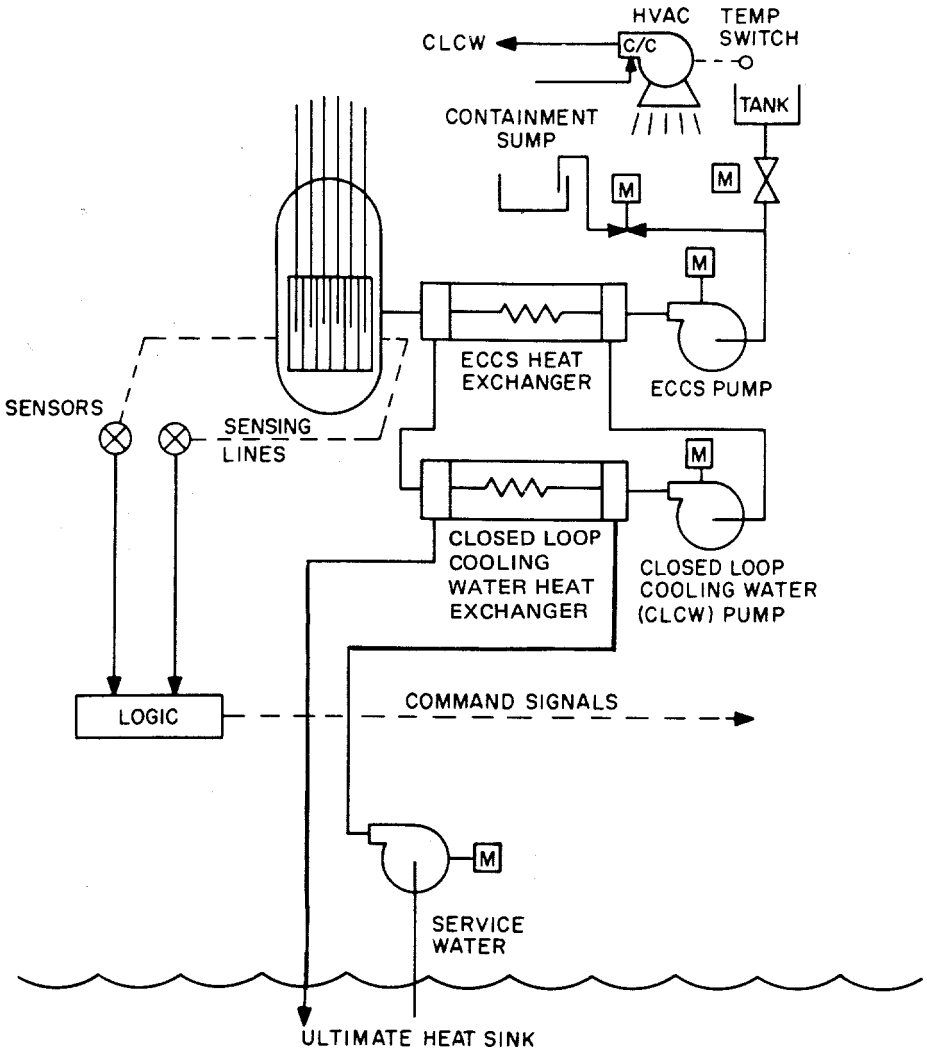


Figure A.7—Elements for Emergency Core Cooling: Addition of some Auxiliary Supporting Features

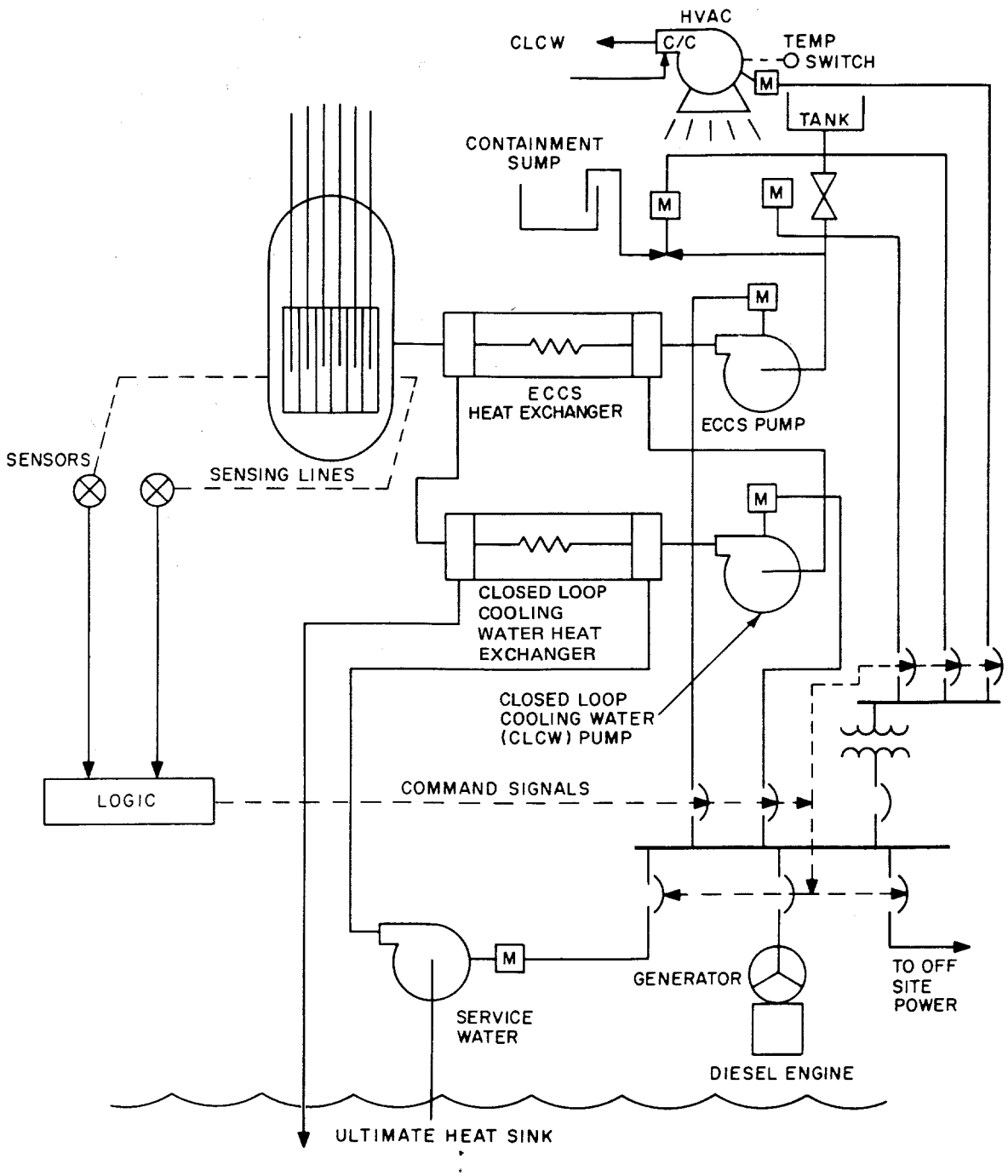


Figure A.8—Elements for Emergency Core Cooling: Addition of Class 1E Power

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 emergency core cooling system execute features. The emergency core cooling system 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.

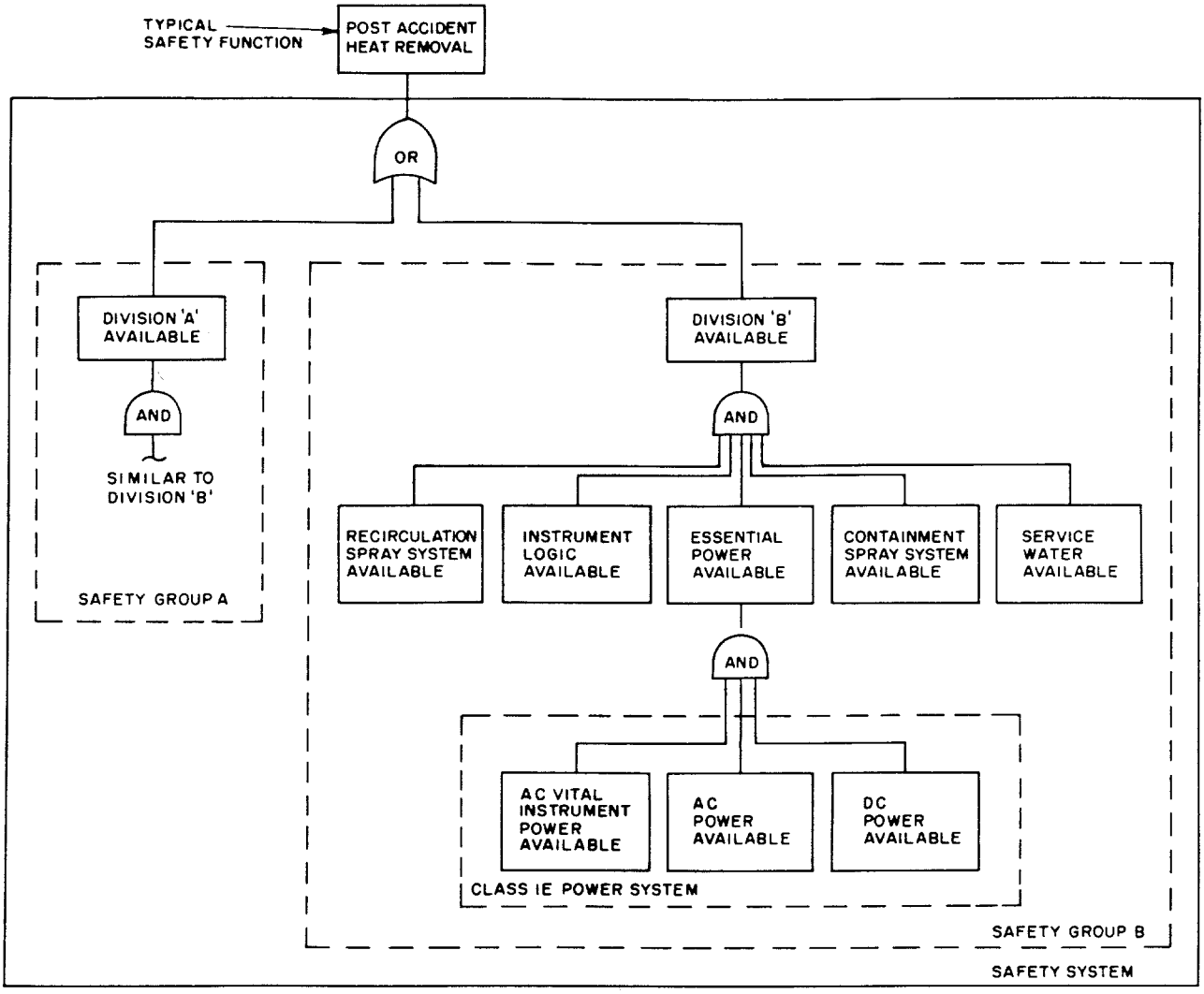
A4. Safety Group

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 Fig 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 three divisions be operating to accomplish the safety function. The safety groups would then be identified by the logic in Fig A.10. In order that the safety group status be identified, as required by 5.8, the logic shown would need to be included in the indication circuitry.

A5. Other Auxiliary Features

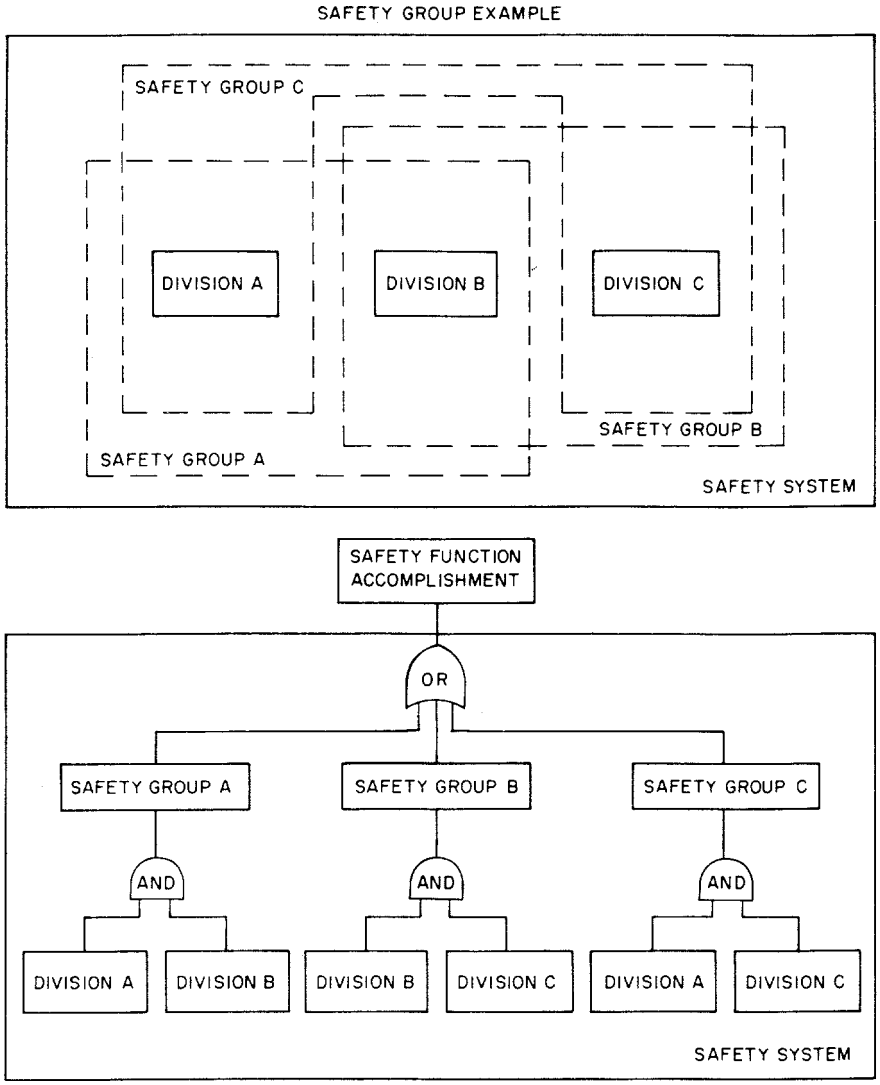
Included in the design of most safety systems are components and equipment whose primary function is to increase the availability or reliability of the safety system without directly performing a safety function. These components include, but are not limited to, equipment protection devices, built-in test equipment, isolation devices, etc., as shown in Fig 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 not cause a spurious tripping when safety system operation is required. Performance of this essential function is the one that 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 308-1980 [1].



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



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

Annex B Other Standards That Provide Additional Information That May Be Useful in Applying IEEE Std 603-1991

(Informative)

[B1] ANSI/ANS-58.8-1984, Time Response Design Criteria for Nuclear Safety-Related Operator Actions.

[B2] ANSI/ANS-58.9-1981, Single-Failure Criteria for Light Water Reactor Safety-Related Fluid Systems.

[B3] ANSI/ANS-58.3-1988, Physical Protection Criteria for Systems and Components Important to Safety.

[B4] ANSI/ANS-59.3-1984, Safety Criteria for Control Air Systems.

[B5] ANSI/ANS-59.51-1976, Fuel Oil Systems for Standby Diesel Generators.