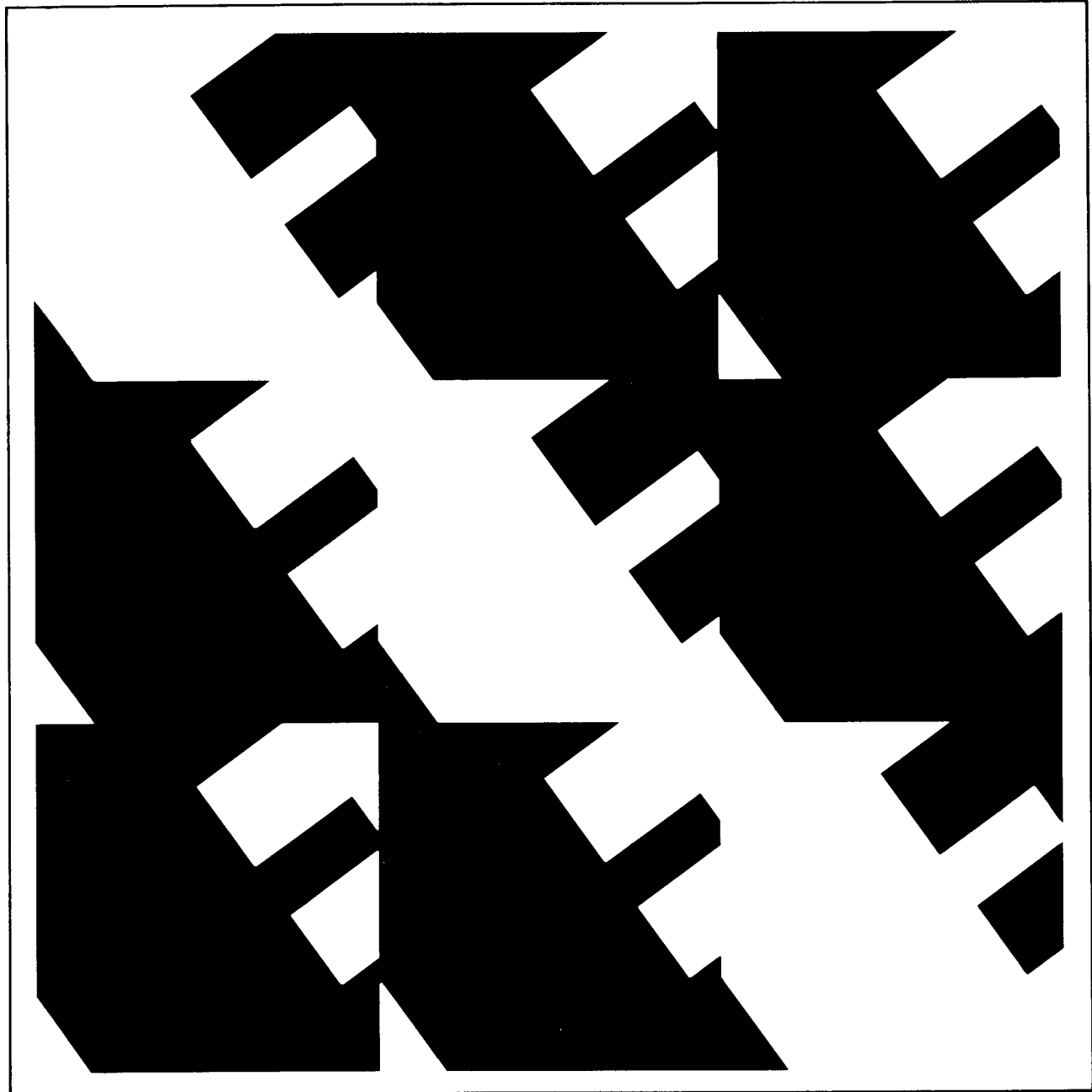


IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations



IEEE Std 603-1980



Published by The Institute of Electrical and Electronics Engineers, Inc 345 East 47th Street, New York, NY 10017, USA
November 24, 1980

SHO7849

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 safety systems for nuclear power generating stations. The criteria herein are applicable to the power, instrumentation, and control portions of the safety systems. 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 3 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 which 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 must contain all of the general elements or that a particular general element is limited to application in only one operational element.

¹See Fig 2 for IEEE Stds, ANSI/ANS 4.1-1978, ANSI N18.2-1973, ANSI N18.2a-1975, ANSI/ANS 52.1-1978, ANSI N213-1975, and ANSI N214-1976.

Figure 4 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 5 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 mitigate the consequences of design basis events. However, this standard does not apply to all of the safety-related systems, structures, and equipment required for complete plant safety, for example, fire protection systems. The electrical portion of the safety systems are classified as Class 1E.

2. Definitions

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

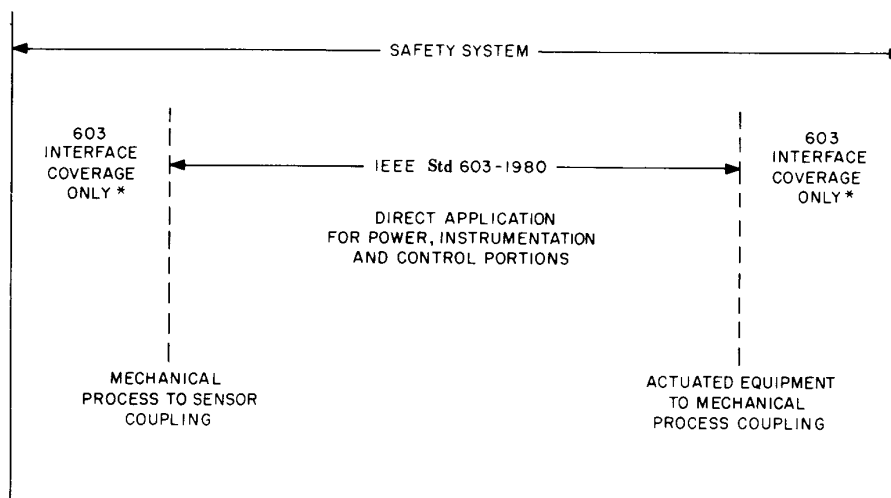
acceptable. Demonstrated to be adequate by the safety analysis of the station.

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.

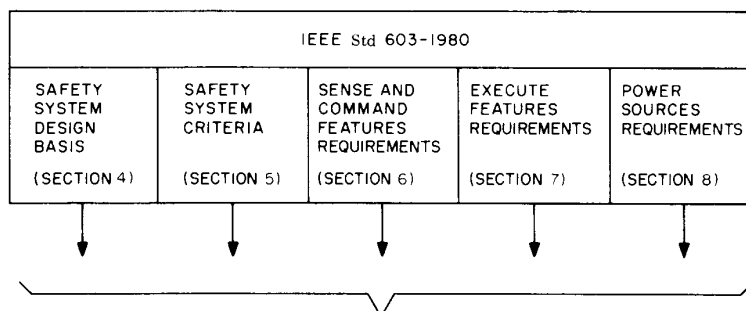
actuation device. A component or assembly of components that directly controls the motive power (electricity, compressed air, hydraulic fluid, etc) for actuated equipment.

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



*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.

Fig 1
Nonelectrical Interface
Scope Diagram



ANSI/IEEE Std 279-1971: Criteria for Protection Systems
ANSI/IEEE Std 338-1977: Periodic Testing of Class 1E Power and Protection Systems
ANSI/IEEE Std 379-1977: Application of Single Failure Criterion to Class 1E Systems
ANSI/IEEE Std 384-1977: Independence of Class 1E Equipment and Circuits
ANSI/IEEE Std 577-1976: Reliability Analyses of Safety Systems
IEEE Std 308-1980: Class 1E Power Systems
IEEE Std 323-1974: Qualifying Class 1E Equipment

Fig 2
Relationship Between IEEE Std 603-1980
and Other IEEE Standards

		GENERAL ELEMENTS OF A SAFETY SYSTEM		
		SENSE AND COMMAND FEATURES	EXECUTE FEATURES	POWER SOURCES
OPERATIONAL ELEMENTS OF A SAFETY SYSTEM	REACTOR TRIP SYSTEM AND ENGINEERED SAFETY FEATURES			
	AUXILIARY SUPPORTING FEATURES			
	OTHER AUXILIARY FEATURES			

NOTES:

(1) The *protection system* of ANSI/IEEE Std 279-1971 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 which provide similar performance characteristics (for example, sensors) for many discrete safety functions.

(4) Each operational element will contain one or more general elements. Every operational element will not necessarily contain all of the general elements.

(5) A device which serves as a general element is not necessarily limited to application in only one operational element.

Fig 3
3 × 3 Matrix Representation of
Safety System

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

auxiliary supporting features. Systems or components which provide services (such as cooling, lubrication, and energy supply) which are 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.

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.

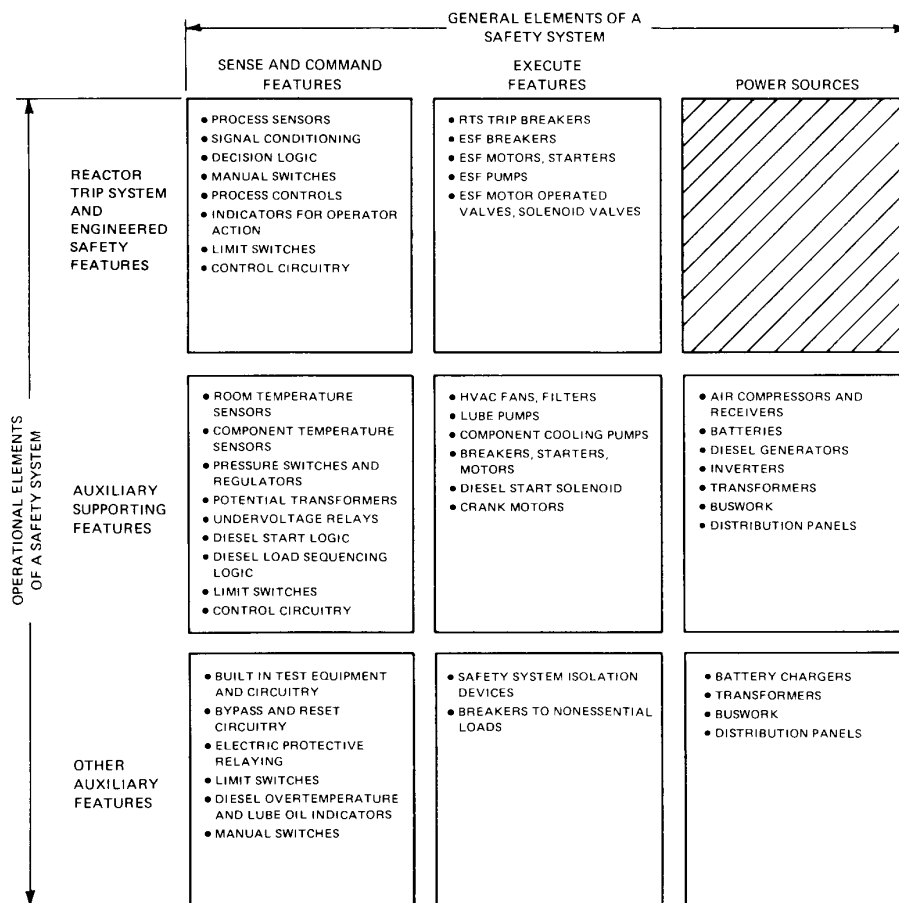
design basis events. Postulated events used in the design to establish the acceptable performance requirements for the structures, systems, and components.

detectable failures. Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures which 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 379-1977, Application of the Single-Failure Criterion to Nuclear Power Generating Station Class 1E Systems, for application guidance.

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



NOTES:

- (1) The items listed are only representative examples as to inclusion or location in the matrix.
- (2) See Fig 3 for additional notes.

Fig 4
Examples of Equipment Fitted to
Safety System Scope Diagram

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.

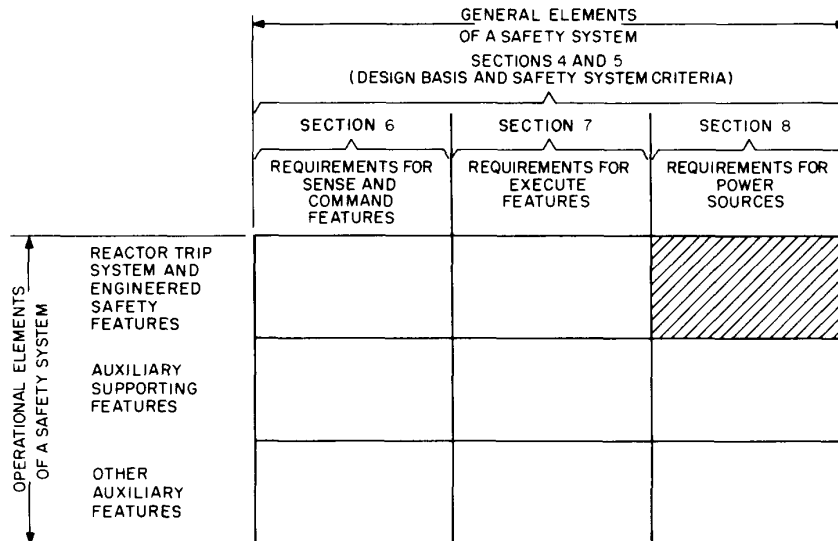
NOTE: In some instances protective actions may be performed by execute features that respond directly to the process conditions (for example, check valves, self-actuating relief valves).

maintenance bypass. Removal of the capability of a channel, component, or piece of equip-

ment 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 will not result in the loss of a safety function.

module. Any assembly of interconnected components which 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 which permit it to be



NOTE: See Fig 3 for notes.

Fig 5
Scope Diagram for IEEE Std 603-1980
Criteria for Safety Systems for Nuclear Power Generating Stations

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 safety injection 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 fea-

tures 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 intercon-

nected components, modules, and equipment that can accomplish a safety function.

NOTE: A safety group may include one or more divisions (see Appendix A for an illustrative example).

safety system. Those systems (the reactor trip system, an engineered safety feature, or both, including all their auxiliary supporting features and other auxiliary features) which provide a safety function. A safety system is comprised of more than one safety group of which any one safety group can provide the safety function.

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. That portion of a channel which responds to changes in a plant variable or condition and converts the measured process variable into an electric or pneumatic signal.

3. References

- [1] ANSI/ANS 4.1-1978, Design Basis Criteria for Safety Systems in Nuclear Power Generating Stations²
- [2] ANSI/IEEE Std 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations
- [3] ANSI/IEEE Std 338-1977, Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems
- [4] ANSI/IEEE Std 352-1975, Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems
- [5] ANSI/IEEE Std 379-1977, Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Class 1E Systems
- [6] ANSI/IEEE Std 494-1974, Standard Method for Identification of Documents Relat-

²ANSI documents are available from the American National Standards Institute, 1430 Broadway, New York, N.Y. 10018.

ed to Class 1E Equipment and Systems for Nuclear Power Generating Stations

[7] ANSI/IEEE Std 577-1976, Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations

[8] IEEE Std 308-1980, Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations

[9] IEEE Std 323-1974, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

[10] IEEE Std 384-1977, Standard Criteria for Independence of Class 1E Equipment and Circuits

[11] IEEE Std 420-1973, Trial-Use Guide for Class 1E Control Switchboards for Nuclear Power Generating Stations

[12] IEEE Std 497-1977, Trial-Use Standard Criteria for Post Accident Monitoring Instrumentation for Nuclear Power Generating Stations

4. Safety System Design Basis

A specific basis² 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 prepared in accordance with the requirements of ANSI/ANS 4.1-1978, 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.

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

4.4 The following for each of the protective actions identified in 4.2:

²See [B1], [B2], and [B8], Appendix B.