

680 20

ANSI/ANS-51.1-1983(W2000)

American Nuclear Society

nuclear safety criteria for the design of stationary pressurized water reactor plants



Documents
Document Sharing Hub

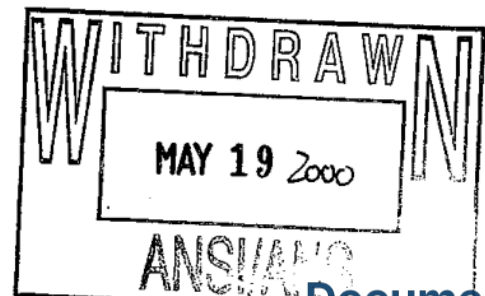
**American National Standard
Nuclear Safety Criteria for the Design of
Stationary Pressurized Water Reactor Plants**

**Secretariat
American Nuclear Society**

**Prepared by the
American Nuclear Society
Standards Committee
Working Group ANS-51.1**

**Published by the
American Nuclear Society
555 North Kensington Avenue
La Grange Park, Illinois 60525 USA**

**Approved April 29, 1983; Reaffirmed September 26, 1988
by the
American National Standards Institute, Inc.**



Documents

Document Sharing Hub

American National Standard

An American National Standard implies a consensus of those substantially concerned with its scope and provisions. An American National Standard is intended as a guide to aid the manufacturer, the consumer, and the general public. The existence of an American National Standard does not in any respect preclude anyone, whether he has approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. American National Standards are subject to periodic review and users are cautioned to obtain the latest editions.

CAUTION NOTICE: This American National Standard may be reviewed or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of publication. Purchasers of this standard may receive current information, including interpretation, on all standards published by the American Nuclear Society by calling or writing to the Society.

Published by

American Nuclear Society
555 North Kensington Avenue, La Grange Park, Illinois 60525 USA

Copyright © 1983 by American Nuclear Society.

Any part of this standard may be quoted. Credit lines should read "Extracted from American National Standard ANSI/ANS-51.1-1983(R1988) with permission of the publisher, the American Nuclear Society." Reproduction prohibited under copyright convention unless written permission is granted by the American Nuclear Society.

Printed in the United States of America

Foreword

(This Foreword is not a part of American National Standards Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants, ANSI/ANS-51.1-1983(R1988).)

This standard is a complete revision and combination of N18.2-1973/ANS-51.1 and N18.2a-1975/ANS-51.8. It has been prepared by Subcommittee ANS-51, Pressurized Water Reactor Criteria, to incorporate additional requirements for the design of pressurized water reactor (PWR) nuclear power plants and to address three major areas:

1. Safety Classes

The results of the ANS Nuclear Power Plant Standards Committee (NUPPSCO) Ad Hoc Committee and NUPPSCO Coordinating Working Group 3 on Equipment Classification are incorporated. These results define Safety Classes and specify requirements for all equipment and structures in a stationary nuclear power plant having a nuclear safety function. A methodology is given to classify all equipment into one of three Safety Classes according to its importance to nuclear safety and its capability for maintenance, surveillance testing, and inspection, or into a Non-Nuclear Safety Class. In addition, classification interface criteria are defined.

2. Plant Conditions

The results of the NUPPSCO Coordinating Working Group 2 have been incorporated. The concept of Plant Conditions is developed that includes individual process conditions, combinations of process conditions, and the combinations of process conditions and external hazards that could result in simultaneous effects on plant equipment. Probability of occurrence is the unifying basis for the categorization of Plant Conditions.

3. Design Requirements

This standard provides a set of design requirements for all Safety Classes and Non-Nuclear Safety Class in terms of industry codes and standards for each category of Plant Conditions. The design requirements reference specific standards and ensure substantial interrelationship with other codes and standards.

The content of this standard reflects an attempt to achieve the following objectives:

- a. To establish a consistent set of requirements for light water reactor nuclear power plants;
- b. To establish a disciplined, systematic method for defining nuclear safety requirements for nuclear power plants;
- c. To establish and delineate the functional nuclear safety requirements for the design of nuclear power plants;
- d. To be responsive to both the regulatory requirements of the Nuclear Regulatory Commission and the design and technical requirements of industry codes and standards;
- e. To provide a framework for augmenting these criteria as additional standards are developed within the nuclear industry; and
- f. To provide a uniform basis for design safety requirements which may be reflected in regulatory documents.

The existence of unique plant or site characteristics might require the consideration of alternate design concepts. This standard has been developed along functional lines to permit this flexibility. The standard has, however, cited many standards, some of which were still in draft form at the time this document was published. Provisions



Documents

Document Sharing Hub

Contents

Section	Page
1. Introduction	1
1.1 Scope	1
1.2 Purpose	1
2. Definitions	2
3. General Safety Criteria	5
3.1 General Approach	5
3.2 Plant Conditions and Plant Nuclear Safety Criteria	6
3.2.1 Application of the Single Failure Criterion	7
3.2.2 Coincident Occurrences	8
3.2.3 Optional Approach	9
3.2.4 Plant Condition Application Examples	9
3.2.5 Multiple Failures in Nuclear Safety-Related Equipment and Common Cause Failures	10
3.2.6 Operator Action and Human Error	10
3.2.7 Site Conditions	10
3.2.8 Natural and Man-Made Hazards	10
3.3 Equipment Classification	11
3.3.1 Safety Classes	11
3.3.2 Safety Class Interfaces	13
3.3.3 Safety Class Requirements Correlations	16
3.4 Industry Codes and Standards	16
3.4.1 Safety Class 1, 2, and 3 Mechanical Equipment	16
3.4.2 Safety Class 3 Electrical Equipment	17
3.4.3 Safety Class 2 and 3 Structures	17
3.4.4 Non-Nuclear Safety Equipment	17
3.4.5 Quality Assurance	17
3.5 Safety Analyses	18
3.5.1 General Requirements	18
3.5.2 Requirements for Plant Condition 1	18
3.5.3 Requirements for Other Plant Conditions	18
4. Design Criteria*	32
4.1 Reactor Core and Internals	32
4.2 Reactivity Control Systems	33
4.3 Protection System	34
4.4 Reactor Coolant System	34
4.5 Shutdown Heat Removal Systems	36
4.6 Reactor Coolant Auxiliary Systems	37
4.7 Cooling Water Systems	38
4.8 Emergency Core Cooling Systems	39
4.9 Primary Containment	40
4.10 Emergency Secondary Heat Removal Systems	41
4.11 Containment Auxiliary Systems	43
4.12 Safety-Related Area Cooling Systems	43
4.13 Fuel Storage and Handling	44
4.14 Electrical Power Systems	44
4.15 Fire Protection Systems	45
4.16 Control Complex	45



Documents

Document Sharing Hub

4.17	Radioactive Waste Processing Systems	46
4.18	Other Structures	47
4.19	Power Conversion System	47
4.20	Multi-Unit Stations	48

*Each subsection of Section 4 adheres to the following outline:

4.X Title

4.X.1	Function
4.X.2	Definition
4.X.3	Performance Criteria
4.X.4	Safety Class
4.X.5	Design Criteria
4.X.5.1	Nuclear Design Criteria
4.X.5.2	Systems Design Criteria
4.X.5.3	Mechanical Design Criteria
4.X.5.4	Electrical Design Criteria
4.X.5.5	Instrumentation and Control Design Criteria
4.X.5.6	Structural Design Criteria
4.X.5.7	Testing and Inspection Criteria
4.X.5.8	Layout Criteria

5.	References	51
----	------------------	----

Appendices

Appendix A	Classification Application	55
Appendix B	Basis for Plant Condition Criteria in Subsection 3.2	77
Appendix C	Historical Background and Rationale for Equipment Classification in Subsection 3.3	86
Appendix D	Basis for Mechanical Design Criteria in Subsection 3.4.1	91

Tables

Table 3-1	Offsite Radiological Dose Criteria for Plant Conditions	20
Table 3-2	Plant Nuclear Safety Criteria	21
Table 3-3	Example of a Set of Limiting Normal Operations and Limiting Events	22
Table 3-4	Methodology for Determining the Plant Condition of an Event	24
Table 3-5	Basic Requirements for Equipment by Safety Class	25
Table 3-6	ASME Boiler and Pressure Vessel Code, Section III Service Limits for Various Plant Conditions and Nuclear Safety Functions	26
Table 3-7	Standards for Safety Class 3 Electrical Equipment (Class 1E)	27
Table 3-8	Codes and Standards for Safety Class 2 and 3 Structures	28
Table 4-1	System Functional Design Criteria Interfaces	30

Table A-1 Equipment Classification	56
Table A-2 Examples of Typical Classification of Components Comprising Complex Principal Equipment	71
Figures	
Fig. 3-1 Fluid-System Safety Class Interfaces	29
Fig. B-1 Event Categorization	83
Fig. B-2 Dose Limit Line for Whole-Body Dose at Site Boundary	84
Fig. B-3 Dose Limit Line for Thyroid Dose at Site Boundary	84
Fig. B-4 Whole-Body Dose Limit Line Based on 10 CFR 50 Appendix I Guideline	85
Fig. B-5 Thyroid Dose Limit Line Based on 10 CFR 50 Appendix I Guideline	85

Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants

1. Introduction

1.1 Scope. This standard establishes the nuclear safety criteria and functional design requirements of structures, systems, and components of stationary pressurized water reactor (PWR) power plants. Operations, maintenance, and testing requirements are covered only to the extent that they affect design provisions.

A methodology is given for classifying all equipment into one of three Safety Classes according to its importance to nuclear safety or into a Non-Nuclear Safety Class. Another methodology is given for identifying and categorizing into one of five Plant Conditions the normal operations and events for which the plant shall be designed. Acceptance criteria are given for each Plant Condition.

Specific design requirements are given for each major system in a typical plant. These requirements are related to other, more specific design standards and are intended to amplify the criteria given in the Code of Federal Regulations, Title 10, "Energy," Part 50, "Licensing of Production and Utilization Facilities," Appendix A, "General Design Criteria for Nuclear Power Plants" [1].¹

1.2 Purpose. Incorporating the requirements of this standard provides a degree of assurance that, in their entirety, plants are designed and constructed so that they can be operated without undue risk to the health and safety of the public. It is intended that this standard lead to attainment of this objective by defining existing practices that are consistent with the licensing requirements of the U.S. Nuclear Regulatory Commission (NRC), appropriate industry codes, and good engineering practice. References to regulations, codes, and other standards are included where appropriate.

A designer of a plant has a responsibility, even at the design stage, going beyond conformance to the criteria defined in this standard. In addition to considering this standard, the NRC regulations, and other published guidance, the designer must ensure that the design bases and expected operational characteristics are supported, to the extent practical, by design analyses, experimental verifications, and comparisons to accepted designs or experience gained from similar designs.

Consideration of alternate or additional criteria and requirements may be necessary to accommodate unique site characteristics.

This standard is written specifically for a PWR nuclear power plant. A PWR plant is based on closed-cycle circuits, utilizing two separate fluid systems that interface at two or more heat exchangers called steam generators. These circuits are known as the reactor coolant (or primary) system and the power conversion (or secondary) system. The reactor coolant system contains the reactor core, a water-cooled and water-moderated nuclear assembly that utilizes fissionable fuel. Heat is transferred by the reactor coolant system from the reactor core to the power conversion system at the steam generators. The power conversion system converts thermal energy into electrical energy by means of a turbine generator. Both the reactor coolant system and the power conversion system are provided with a number of auxiliary systems that supply, service, and control circulated fluids, processes and environmental conditions, and remove undesirable by-products, distribute power, and ensure safe conditions, during normal or accident conditions. A number of structures are provided to house, contain, protect, and shield both equipment and personnel. For the purpose of this standard, a PWR plant has the following characteristics:

- a. Solid ceramic fuel enclosed in metallic cladding,
- b. Fixed geometry for the fuel and coolant (which acts as the moderator),

¹Numbers in brackets refer to corresponding numbers in Section 5, References.

c. Core and core coolant enclosed in an envelope of high integrity, and

d. Core and core coolant envelope enclosed in a primary containment barrier of high integrity.

2. Definitions

This section defines terms applicable to this standard.

active component. A component in which mechanical movement must occur to accomplish the nuclear safety function of the component.

active failure. A malfunction, excluding passive failures, of a component that relies on mechanical movement to complete its intended nuclear safety function upon demand.

Examples of active failures include the failure of a valve or check valve to move to its correct position, or the failure of a pump, fan, or diesel generator to start.

Spurious action of a powered component originating within its actuation or control system shall be regarded as an active failure unless specific design features or operating restrictions preclude such spurious action. An example is the unintended energization of a powered valve to open or close.

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

best-estimate value. The mean value of the probability density function for the random variable of interest. Where the probability density function is not known, the mean value shall be estimated based on engineering judgment.

cold shutdown. The condition in which the reactor is subcritical and the reactor coolant system average temperature is below the required temperature to permit major maintenance, consistent with technical specification operational limits.

common cause failure. Multiple failures of structures, systems, or components as a result of a single phenomenon.

controlled shutdown and cooldown. A shutdown and cooldown in which the fuel and reactor coolant pressure boundary conditions may exceed technical specification limits and implementation of plant emergency procedures may be required.

departure from nucleate boiling (DNB). The onset of the transition from nucleate to film boiling.

departure from nucleate boiling ratio (DNBR). The ratio of the heat flux required to cause departure from nucleate boiling (DNB) to the actual channel heat flux for given conditions.

equipment. A constituent of a component, a component, an assemblage of components, a system, or a structure having at least one function.

engineered safety feature. A nuclear safety-related structure, system, or component that serves to control and limit the consequences of releases of energy or radioactivity if an event were to occur to the extent that the public health and safety might be impaired if these energy or radioactivity releases were not additionally restrained.

event. A condition that deviates from normal operation, i.e., an initiating occurrence or an initiating occurrence plus single failure or coincident occurrence combination.

fission product barriers. The fuel cladding, reactor coolant pressure boundary, and primary containment.

fuel cladding damage. Perforation or excessive distortion or rupture of fuel rod cladding which would permit the release of fission products to the reactor coolant.

hot shutdown. In the PWR, the condition in which the reactor is subcritical and the reactor coolant system average temperature is below the required temperature to permit operation of the low pressure residual heat removal system, consistent with technical specification operational limits.

hot standby. In the PWR, the condition in which the reactor is subcritical and the reactor coolant system average temperature is above the required

temperature to permit operation of the low pressure residual heat removal system, consistent with technical specification operational limits.

human error. A mistake, blunder, condition, or act deviating from normal or expected behavior committed unintentionally or through ignorance that fails to achieve what should be accomplished or performed.

initiating occurrence. A single occurrence and its consequential effects that place the plant or some portion of the plant in an off-normal condition. An initiating occurrence is not the single failure defined elsewhere herein. An initiating occurrence can be an equipment failure, a human error, a natural hazard, or a man-made hazard.

long term. In the context of the single failure criterion, that period of system operation, following the short term, during which the nuclear safety function is required.

(The concept of short term and long term does not apply to electrical components.)

loss-of-coolant accident (LOCA). The loss of reactor coolant at a rate in excess of the reactor coolant normal makeup rate, from breaks or openings in the reactor coolant pressure boundary inside primary containment up to, and including, a break equivalent in size to the largest justified pipe rupture (or in the absence of justification, a double-ended rupture of the largest pipe) in the reactor coolant pressure boundary.

man-made hazard. A condition involving vehicles, equipment, material, or structures created by man that occurs outside of a unit and has the potential for causing damage to nuclear safety-related structures, systems, or components of the unit.

missile. A mass that has kinetic energy and is unrestrained.

natural hazard. A natural phenomenon that has the potential for causing damage to the nuclear safety-related structures, systems, or components of a unit.

natural phenomena. Those conditions of the environment external to the unit that are not man-made. (The natural phenomena considered

in nuclear power plant design criteria are termed natural hazards.)

no loss of nuclear safety function. The capability of unit structures, systems, and components to accomplish nuclear safety functions required to accommodate normal operation or a specified event within applicable nuclear safety criteria.

Non-Nuclear Safety (NNS). Classification of structures, systems, or components that are not in Safety Class 1, 2, or 3.

normal shutdown and cooldown. A shutdown and cooldown in which normal operational systems can be used, the fuel and reactor coolant pressure boundary conditions are within technical specification operational limits, and no automatic actuation of any engineered safety feature is required.

nuclear safety function. Any function that is necessary 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 Plant Conditions that could result in potential offsite exposures that are comparable to the guideline exposures of the Code of Federal Regulations, Title 10, "Energy," Part 100, "Reactor Site Criteria" [2].

nuclear safety-related. Of significance or importance because it applies to:

- a. Structures, systems, or components designed to perform a nuclear safety function,
- b. Drawings, specifications or procedures, analyses, and other documents used to determine or describe parameters affecting structures, systems, or components that are designed to perform a nuclear safety function, or
- c. Services to design, purchase, fabricate, handle, ship, store, clean, erect, install, test, operate, maintain, repair, refuel, and modify structures, systems, or components that are designed to perform a nuclear safety function.

operating. Performing an intended action in the required manner.

operating basis earthquake (OBE). The earthquake that, considering the regional and local

geology and seismology, and specific characteristic of local subsurface material, could reasonably be expected to affect the plant site during the operating life of the plant. It is that earthquake which produces the vibratory ground motion for which those nuclear safety-related features of the plant necessary for subsequent operation without undue risk to the health and safety of the public are designed to remain functional.

operator error. In the context of the single failure criterion, a single incorrect or omitted action by a human operator attempting to perform a nuclear safety-related manipulation in response to an initiating occurrence.

orderly shutdown and cooldown. A shutdown and cooldown in which the fuel and reactor coolant pressure boundary conditions are within technical specification operational limits. Automatic actuation of an engineered safety feature may be required.

passive component. A component that is not an active component.

passive failure. The blockage of a process flow path or failure of a component to maintain its structural integrity or stability, such that it cannot provide its intended nuclear safety function upon demand.

Plant Condition (PC). Categorization of normal operations and events in terms of their likelihood of occurrence for the purpose of establishing nuclear safety criteria.

primary containment. The principal structure of a unit that acts as the barrier, after the fuel cladding and reactor coolant pressure boundary, to control the release of radioactive material. It includes (1) the containment structure and its access openings, penetrations, and appurtenances, (2) those valves, pipes, closed systems, and other components used to effect isolation of the containment atmosphere from the environment, and (3) those systems or portions of systems that, by their system functions, extend the containment structure boundary (e.g., the connecting steam and feedwater piping) and provide effective isolation.

primary reactor containment. (See primary containment; the preferred term is primary containment.)

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

reactor containment. (See primary containment; the preferred term is primary containment.)

reactor coolant normal makeup. Makeup to the reactor coolant pressure boundary by the system(s) relied upon to maintain reactor coolant inventory during normal operation.

reactor coolant pressure boundary (RCPB). All those pressure-containing components, such as pressure vessels, piping, pumps, and valves that are:

- a. Part of the reactor coolant system, or
- b. Connected to the reactor coolant system up to and including any or all of the following:
 - (1) The outermost primary containment isolation valve in system piping that penetrates the primary containment,
 - (2) The second of two valves normally closed during normal reactor operation in system piping that does not penetrate primary containment, or
 - (3) The reactor coolant system safety and relief valves.

reactor-year. One calendar year per nuclear power reactor unit.

redundant component, system, or subsystem. A component, system, or subsystem that independently duplicates the functions of another component, system, or subsystem.

refueling shutdown. The cold shutdown condition in which the reactor coolant system is depressurized for the purpose of replacing fuel.

safe shutdown. A shutdown with (1) the reactivity of the reactor kept to a margin below criticality consistent with technical specifications, (2) the core decay heat being removed at a controlled rate sufficient to prevent core or reactor coolant system thermal design limits from being exceeded, (3) components and systems necessary to maintain these conditions operating.

their design limits, and (4) components and systems necessary to keep doses within prescribed limits operating properly.

safe shutdown earthquake (SSE). The earthquake that is based upon evaluation of the maximum earthquake potential considering regional and local geology and seismology, and specific characteristics of local subsurface material. It is the earthquake that produces the maximum vibratory ground motion for which nuclear safety-related structures, systems, and components are designed to perform their nuclear safety function.

Safety Class (SC). Classification of structures, systems, or components based on their nuclear safety functions.

secondary containment. The structure surrounding the primary containment that acts as a further barrier to control the release of radioactive material.

secondary reactor containment. (See secondary containment; the preferred term is secondary containment.)

seismic category I. The category of nuclear safety-related structures, systems, and components that are required to perform their nuclear safety function during or after an SSE as necessary to accommodate any event involving an SSE.

shall, should, and may. The word "shall" is used to denote a requirement; the word "should" is used to denote a recommendation; and the word "may" is used to denote permission, neither a requirement nor a recommendation.

short term. In the context of the single failure criterion, that period of operation up to 24 hours following the initiating event, but for purposes of design of the emergency core cooling and containment spray systems, the short term shall be considered to terminate upon transfer of these systems to the long-term cooling mode.

(The concept of short term and long term does not apply to electrical components.)

shutdown. The procedure of making a nuclear reactor subcritical (shutdown) or the state of a nuclear reactor after being made subcritical (shutdown).

single failure. A random failure and its consequential effects, in addition to an initiating occurrence, that result in the loss of capability of a component to perform its intended nuclear safety function(s).

Fluid and electrical systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly), nor (2) a single failure of any passive component (assuming active components function properly) results in a loss of the capability of the system to perform its nuclear safety function.

station (nuclear). A facility wherein electric energy is produced from nuclear energy by means of suitable apparatus. The station may consist of one or more units located on an adjacent or contiguous site.

ultimate heat sink. The nuclear safety-related means of heat dissipation from the unit to the environment, including the necessary retaining structures (e.g., a dammed lake or a cooling tower) and any connecting canals or conduits.

unit. One nuclear power reactor and associated equipment necessary for electrical power generation, including those structures, systems, and components required to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

3. General Safety Criteria

3.1 General Approach. The design of a nuclear power unit requires the integration of a number of interdisciplinary considerations to ensure that nuclear safety criteria are adequately identified and implemented. The information contained in this section develops these criteria by considering the following:

a. Identification of Plant Conditions (PCs) that are used to classify the normal operations and events the plant must be designed to accommodate. Five PCs are defined that allow categorization of the normal operations and events in terms of likelihood of occurrence during the plant life. Plant nuclear safety criteria are established.

lished for each PC with the objective that the more likely the event, the smaller the potential consequences. Rules governing the application of single failure or coincident occurrences in combination with initiating occurrences, and the accommodation of natural and man-made hazards are also provided.

b. Identification of a set of equipment Safety Classes (SCs) that correlate the stringency of design requirements to which structural, mechanical, and electrical equipment are assigned to ensure performance of nuclear safety functions.

c. Identification of major applicable industry codes and standards for design of structures, systems, and components.

d. Identification of criteria that are applicable to several or all plant systems (e.g., single failure criterion, and credit for operator action).

e. Identification of those nuclear safety-related structures, systems, or components for which a quality assurance program must be established in accordance with industry requirements.

3.2 Plant Conditions and Plant Nuclear Safety Criteria. The spectrum of normal operations and events shall be identified in accordance with their best-estimate frequency of occurrence² and divided into five categories as follows:

Plant Condition (PC)	Best-Estimate Frequency Of Occurrence (F), per Reactor Year ³
1	Normal Operations
2	$F \geq 10^{-1}$
3	$10^{-1} > F \geq 10^{-2}$
4	$10^{-2} > F \geq 10^{-4}$
5	$10^{-4} > F \geq 10^{-6}$

As noted in 3.2.3, events with a best-estimate frequency of occurrence of $<10^{-6}$ /reactor year need not be considered for design.⁴ The offsite

²See Appendix B for guidance in determining best-estimate frequency of occurrence.

³Analyses by industry have shown that some events have occurrence frequencies which would place them in PC categories that are different from those in which they have been placed during past licensing considerations. In some of these cases, regulatory authorities may require that the events continue to be treated in the previously established manner. An example may be design basis fire.

⁴Some events, even though their frequencies of occurrence are $<10^{-6}$ /reactor year, have been and may continue to be required to be accommodated within PC-5 nuclear safety criteria by regulatory authorities. An example is LOCA + loss of offsite power + single failure.

radiological dose criterion for each PC is presented in Table 3-1. The plant nuclear safety criteria for each PC are presented in Table 3-2.

The best-estimate frequency of occurrence of an event (e.g., estimated system or component failure rate) shall be determined and the appropriate PC assigned. The consequences of the event shall be determined to be within the nuclear safety criteria specified in Table 3-2 for that PC. The nuclear safety criteria of Table 3-2 have been established on the premise that:

a. Those situations in the plant that are assessed as having a high frequency of occurrence shall have a small consequence to the public, and

b. Those extreme situations having the potential for the greatest consequence to the public shall be those having a very low frequency of occurrence.

A set of limiting normal operations for PC-1 and limiting events for each PC other than PC-1 shall be comprehensively and systematically identified for detailed analysis. The limiting set of normal operations consist of those normal operating modes that cause the most extreme values of basic plant parameters (e.g., system pressures, system flow rates, radiation levels or component stresses). The limiting set of events shall be determined as follows:

a. Consider events that can result in the basic parameter changes listed below and identify potential limiting events:

- Increase of core reactivity,
- Changes of reactor coolant flow,
- Changes of reactor coolant pressure,
- Changes of reactor coolant temperature,
- Changes of reactor coolant inventory,
- Changes in energy supplies to the plant,
- Changes in coolant supplies to the plant,
- Changes in the nuclear safety-related equipment status,

- Changes in core power distribution,
- Changes in radioactive releases, or
- Changes of any other variable that has a limiting value.

b. Evaluate whether the integrated response of the plant to each potential limiting event without any preventive or mitigating nuclear safety function can cause parameter changes that will result in the violation of any plant nuclear safety criteria, as identified in Table 3-2. The evaluation shall include the

sequences of the event, such as the effects of the event on plant equipment.

c. For each event that could violate plant nuclear safety criteria, identify its initial conditions, its best-estimate frequency of occurrence, and its consequences including its effect on basic parameters, taking into account preventive or mitigating nuclear safety functions.

d. Categorize each event as PC-2, -3, -4, or -5 according to its best-estimate frequency of occurrence. Those events that cause a limiting parameter change in their PC shall be identified as the limiting set of events.

Experience may show a need to add to the limiting set after its initial identification. A qualitative comparison of similar events may be sufficient to identify the specific event that leads to the most limiting consequences. Only that event shall then be analyzed in detail. The intent is to minimize the number of events that need to be quantitatively analyzed. It should be noted, however, that different events in the same PC may be limiting when the multiplicity of consequences is considered. For example, within a given PC, one event might result in the highest system pressure, while another event might lead to minimum core thermal-hydraulic margin or maximum offsite dose consequences. An example of a limiting set of normal operations and events is given in Table 3-3.

Subsections 3.2.1, 3.2.2, and 3.2.3 describe treatment of single failure and coincident occurrences. Use of these subsections might allow re-categorization of some events downward one or two PC categories (i.e., from PC-3 to PC-4 or PC-5). However, if the PC categorization is shifted by use of 3.2.1, 3.2.2, and 3.2.3, such shift shall not eliminate the need to evaluate the basic initiating occurrence (e.g., without single failure or coincident occurrence or both) in the more probable PC, if it is a limiting event for that PC. If the frequency of occurrence of an initiating occurrence, or initiating occurrence plus single failure or coincident occurrences, is shown to be $<10^{-6}$ /reactor year on a best-estimate basis per 3.2.3, this event shall not be considered for design.⁵ Subsection 3.2.4 and Table 3-4 illustrate the use of 3.2.1, 3.2.2, and 3.2.3.

⁵Some events, even though their frequencies of occurrence are $<10^{-6}$ /reactor year, have been and may continue to be required to be accommodated within PC-5 nuclear safety criteria by regulatory authorities.

3.2.1 Application of the Single Failure Criterion.

The single failure criterion requires that the plant be capable of achieving (1) emergency core reactivity control, (2) emergency core and containment heat removal, and (3) containment isolation, integrity, and atmosphere cleanup⁶ given an initiating occurrence plus an independent single failure of a nuclear safety-related component⁷ in any one of the systems required to support directly or indirectly these three nuclear safety functions (i.e., only one single failure need be assumed in the plant nuclear safety-related equipment for any initiating occurrence).

The specific rules governing the application of single failures in combination with initiating occurrences are as follows:

a. Location of Single Failure

The single failure shall be assumed only in the nuclear safety-related components that are needed to respond to the initiating occurrence in order to achieve the three nuclear safety functions stated above.

b. Electrical Equipment

Except as noted in d. through f. as follows, the electrical nuclear safety-related equipment that is required to support, directly or indirectly, the three nuclear safety functions stated previously shall conform to the single failure criterion as provided in American National Standards Criteria for Protection Systems for Nuclear Power Generating Stations, ANSI/IEEE 279-1971 [3], and Application of the Single-Failure Criterion to Nuclear Power Generating Station Class 1E Systems, ANSI/IEEE 379-1977 [4].⁸

c. Fluid Systems

Except as noted in d. through f. as follows, fluid systems required to support, directly or indirectly, the three nuclear safety functions stated above shall be capable of performing their nuclear

⁶Containment cleanup means removing the fission products from the containment atmosphere as required to meet applicable dose criteria following a LOCA.

⁷Complex principle equipment such as diesels are systems and the single failure criterion is applied to their constituent components.

⁸For additional guidance, see IEEE 308-1980, "Criteria for Class 1E Power Systems for Nuclear Power Generating Stations," and IEEE 603-1980, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," available from the Institute of Electrical and Electronics Engineers, Inc., 345 E. 47th St., New York, N.Y. 10017.

safety functions as provided in American National Standard Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems, ANSI/ANS-58.9-1981 [5].

d. Dual Purpose Nuclear Safety-Related Systems

Where the initiating occurrence is the postulated failure of one of two or more redundant trains of a dual purpose nuclear safety-related system, i.e., one required to operate during normal operations as well as to shut down the reactor and mitigate the consequences of the initiating occurrence, a single failure in the remaining train, or trains, of that system shall not be assumed, provided the system is designed to seismic category I standards, is capable of being powered from either offsite or onsite sources, and is constructed, operated, and inspected to quality assurance, testing, and inservice inspection standards appropriate for equipment Safety Classes 1, 2, or 3. Under these circumstances continued operation of the plant following the initiating occurrence is controlled by the plant technical specifications in American National Standard Criteria for the Technical Specifications for Nuclear Power Stations, ANSI/ANS-58.4-1979 [6].

e. Nuclear Safety-Related Systems Not Normally Operating, Case 1

Where the initiating occurrence is the postulated failure of one of two or more redundant trains of a nuclear safety-related system that is not required to operate during normal operations, a single failure shall not be assumed if the initiating occurrence does not require a reactor trip to mitigate the consequences of the initiating occurrence. Under these circumstances, continued operation of the plant is controlled by the plant technical specifications (See Reference [6].)

f. Nuclear Safety-Related Systems Not Normally Operating, Case 2

Where the initiating occurrence is the postulated failure of one of two or more redundant trains of a nuclear safety-related system that is not required to operate during normal operations but whose failure requires a reactor trip to mitigate the consequences, a single failure shall be assumed. However, if the single failure is assumed to occur in another train of that system, all available systems, including those that are not nuclear safety-related and those that are actuated by operator actions, may be employed to mitigate the consequences of the initiating occurrence plus single failure. In judging the availability of

systems, if a reactor trip or turbine trip is a direct consequence of the initiating occurrence, the continued availability of electric power shall be evaluated. The feasibility of carrying out operator actions shall be judged on the basis of adequate indication, enough time being available for the proposed actions, and adequate access to the equipment utilized.⁹

g. Plant Condition Determination

Except as noted in 3.2.3, when a single failure is imposed on a PC-2, -3, or -4 initiating occurrence or initiating occurrence plus coincident occurrence, PC-3, -4, or -5 nuclear safety criteria respectively shall apply. When a single failure is imposed on a PC-5 initiating occurrence or initiating occurrence plus coincident occurrence, the PC-5 nuclear safety criteria shall apply except as noted in 3.2.3.

h. Allowable Outage Intervals

During allowable outage intervals of one of two or more redundant trains of nuclear safety-related equipment permitted by plant technical specifications, the application of the single failure criterion to another train of that equipment is not required.

3.2.2 Coincident Occurrences. Some events may include simultaneous independent, or low probability dependent, occurrences other than single failure of nuclear safety-related equipment, common cause failures, and multiple failures in nuclear safety-related equipment. (Single failure criteria for nuclear safety-related systems are specified in 3.2.1; multiple failures in nuclear safety-related equipment and common cause failures are addressed in 3.2.5.) The plant shall be capable of accommodating credible coincident occurrences. Except as noted in 3.2.3, when any coincident occurrence or combination of coincident occurrences, whose probability of occurrence coincident with the initiating occurrences is $\leq 10^{-2}$ /initiating occurrence, is combined with a PC-2, -3, or -4 initiating occurrence or initiating occurrence plus single failure, PC-3, -4, or -5 nuclear safety criteria respectively shall apply. When any coincident occurrence, or combination of coincident occurrences, is imposed on a PC-5 initiating occurrence plus single failure, PC-5 nuclear safety criteria shall apply except as noted in 3.2.3. Examples of coincident occurrences include:

⁹For additional guidance see proposed American National Standard for Light Water Reactor Operator Actions, ANS-58.8; assigned correspondent: R.R. Mills, Combustion Engineering, 1000 Prospect Hill Road, Windsor, Conn. 06095.

- a. Loss of offsite power,
- b. Stuck control assembly,
- c. Reactor coolant system iodine concentration spike, or
- d. Failure of a normal plant control system.

3.2.3 Optional Approach. As an option to 3.2.1.g and 3.2.2, a probabilistic assessment may be performed to determine the likelihood of the combination of the initiating occurrence plus a single failure or coincident occurrences, or both. Best-estimate values shall be the basis for compliance with this alternative.

This event shall then be categorized as a PC in accordance with the frequency ranges defined in Table 3-1, and the corresponding nuclear safety criteria shall apply. If the frequency of occurrence of an event is shown to be $<10^{-6}$ /reactor year on a best-estimate basis, this event shall not be considered for design.¹⁰ If this optional approach is used, the designer shall indicate this in any statement regarding compliance with this standard.

3.2.4 Plant Condition Application Examples. A general application of the criteria in 3.2, 3.2.1.g, 3.2.2, and 3.2.3 is illustrated in Table 3-4. A typical application of these criteria based on typical best-estimate frequencies follows:

a. If the initiating occurrence is a generator trip and if the best-estimate frequency of occurrence is 1.2×10^{-1} /reactor year, then referring to 3.2, this event would be a PC-2.

b. Referring to 3.2.1, a single active failure combined with the generator trip must also be considered. When a generator trip occurs, the turbine trips, the turbine stop valves close, the steam pressure increases, and the main steam-line relief valves open. As a single active failure, a relief valve may fail to reclose when the steam pressure decreased. The criteria found in subsection 3.2.1.g. may be applied. Referring to 3.2, this event combination would be a PC-3.

Alternately, 3.2.3 may be applied. Assuming the best-estimate frequency of occurrence for a relief valve failing to reclose is 0.9×10^{-2} /demand, then the best-estimate frequency of occurrence for the combination of a generator trip and a relief

valve failing to reclose is 1.1×10^{-3} /initiating occurrence. Referring to 3.2, this event combination would be a PC-4. This alternate would typically be used only if it were more economic.

c. Referring to 3.2.2, coincident occurrence combinations with a generator trip must also be considered. A coincident occurrence that might occur in combination with the generator trip is a failure of the turbine bypass valves to open. Subsection 3.2.2 may be applied assuming the frequency of occurrence for the turbine bypass valves failing to open on demand is $<10^{-2}$ /initiating occurrence. This event combination would be designated a PC-3.

Alternately, 3.2.3 may be applied. Assuming the best-estimate frequency of occurrence for the bypass valves failing to open on demand is 6×10^{-3} /initiating occurrence, then the best-estimate frequency of occurrence for the combination of a generator trip with failure of the turbine bypass valves to open is 7.2×10^{-4} /reactor year. Referring to 3.2, this event combination would be a PC-4. Again, this alternate would typically be used only if it were more economic.

d. Both the failure of the turbine bypass valves to open and the single failure of a relief valve to reclose could occur in combination with the turbine trip. Both 3.2.1.g. and 3.2.2 may be applied (see preceding items b. and c.), and this event combination would be designated a PC-4.

Alternately, 3.2.3 may be applied. The best-estimate frequency of occurrence of this event combination is 6.5×10^{-6} /reactor year. Referring to 3.2, this event combination would be a PC-5. As in the preceding Items b. and c., this alternate would typically be used only if more economic.

e. A second coincident occurrence, such as the feedwater controller failure demanding maximum feedwater flow, might occur in combination with the generator trip, the relief valve failing to reclose, and the turbine bypass valves failing to open. The best-estimate frequency of occurrence for the feedwater controller failure occurring coincident with the generator trip is $\leq 10^{-2}$ /initiating occurrence. Applying 3.2.1.g. once and 3.2.2 twice, the event combination would be a PC-5.

Alternately applying 3.2.3, the best-estimate frequency of occurrence for this event combination is $\leq 0.6 \times 10^{-8}$ /reactor year. Referring

¹⁰Some events, even though their frequencies of occurrence are $<10^{-6}$ /reactor year, have been and may continue to be required to be accommodated within PC-5 nuclear safety criteria by regulatory authorities.

to 3.2.3, the event combination does not need to be considered in the design since the best-estimate frequency of occurrence is $\leq 10^{-6}$ /reactor year.

3.2.5 Multiple Failures in Nuclear Safety-Related Equipment and Common Cause Failures. The criteria and requirements of this standard are based on the deterministic approach for safety evaluation. This approach does not include explicit consideration of multiple failures in nuclear safety-related equipment and common cause failures. Thus, the criteria and requirements of this standard do not apply to and cannot be used to determine the acceptability of consequences due to events that include such failures. However, the designer shall recognize that multiple failures in nuclear safety-related equipment (other than an initiating occurrence and a single failure) could occur. In addition to the requirements of 3.2, 3.2.1, 3.2.2, and 3.2.3, the designer shall recognize that redundant or diverse trains do not necessarily have independent failure modes and failures originating from a common cause could occur.

Design analyses or provisions beyond those required to satisfy this standard may be necessary to ensure that the probability of identifiable multiple failures in nuclear safety-related equipment or common cause failures are acceptably low.¹¹ The designer shall not introduce additional equipment or encumber the design with complexity without reasonable assurance that such additions are beneficial in terms of increased nuclear safety.

3.2.6 Operator Action and Human Error.⁹ Credit for operator action to prevent or mitigate the consequences of events shall be assumed only if suitable time and means for detection and diagnosis of abnormalities are provided.

Conversely, the potential for human error and its related consequences shall be considered in the design. Human error may be an initiating occurrence, a single failure, or a common cause failure.

3.2.7 Site Conditions. The range of conditions that might prevail in the vicinity of the site during the plant lifetime shall be evaluated to

establish the design requirements for the plant (e.g., meteorology, hydrology, or demography). Site conditions can be initiating or coincident occurrences. For guidance, see the following American National Standards: Criteria and Guidelines for Assessing Capability for Surface Faulting at Nuclear Power Sites, ANSI/ANS-2.7-1982 [7]; Determining Design Basis Flooding at Power Reactor Sites, ANSI/ANS-2.8-1981 (Revision of N170-1976) [8]; Evaluation of Ground Water Supply for Nuclear Power Sites, ANSI/ANS-2.9-1980 [9]; Guidelines for Evaluating Site-Related Geotechnical Parameters at Power Reactor Sites, ANSI/ANS-2.11-1978 [10]; Evaluation of Surface-Water Supplies for Nuclear Power Sites, ANSI/ANS-2.13-1979 [11].¹²

3.2.8 Natural and Man-Made Hazards. The range of external phenomena that might prevail in the vicinity of the site shall be evaluated to establish the design requirements for the plant. The range of conditions shall be established on the basis of suitable historical data, sampling and exploration of the external phenomena at and in the vicinity of the site. For guidance, see American National Standard Guidelines for Retrieval, Review, Processing, and Evaluation of Records Obtained from Seismic Instrumentation, ANSI/ANS-2.10-1979 [12]. Natural and man-made hazards and combinations of natural and man-made hazards shall be identified and considered in the design of the plant. For guidance, see American National Standard Guidelines for Combining Natural and External Man-Made Hazards at Power Reactor Sites, ANSI/ANS-2.12-1978 [13]. Natural and man-made hazards can be initiating occurrences or coincident occurrences.

¹¹ This standard does not specify acceptance criteria for the consequences due to multiple failures in nuclear safety-related equipment or common cause failures. One method of analyzing such failures is probabilistic risk analysis.

¹² For additional guidance, see the following proposed American National Standards: Guidelines for Determining Tornado, Hurricane, and other Extreme Wind Parameters at Power Reactor Sites, ANS-2.3, assigned correspondent: G. W. Nicholas, Dames & Moore, 1550 Northwest Highway, Park Ridge, Ill. 60068; Guidelines for Determining Tsunami Criteria for Power Reactor Sites, ANS-2.4, assigned correspondent: R. W. Whalin, Waterways Experiment Stat., P.O. Bx. 631, Vicksburg, Miss. 39180; Guidelines for Determining Meteorological Information Appropriate for a Power Reactor Site, ANS-2.5, assigned correspondent: I. J. Spickler, U.S. NRC, Washington, D.C. 20555; Guidelines for Determining Future and Present Population Distribution at Power Reactor Sites, ANS-2.6, assigned correspondent: A. Brearley, Sargent & Lundy, 55 E. Monroe St., Chicago, Ill. 60603.

3.3 Equipment Classification. The classification system established herein provides a rational basis of determining relative stringency of design requirements applicable to equipment.

Original and replacement equipment shall be assigned to one of the four classes (identified as SC-1, -2, -3, or NNS) in accordance with definitions provided herein. Assignments shall be made for all equipment of the nuclear power plant. Classification shall be done on the basis of definitions contained in 3.3.1 and the interface requirements of 3.3.2. If the interface requirements are not met, the equipment shall be assigned to the more stringent Safety Class corresponding to functions of the connected equipment.¹³ The classification definitions and interface requirements are intended to be independent of other portions and requirements of this standard.

3.3.1 Safety Classes. Equipment shall be assigned to one of the four classes in accordance with 3.3.1.1 through 3.3.1.4. The equipment assigned to SC-1, -2, or -3 is that relied upon in the plant design to accomplish nuclear safety functions.¹⁴

Where more than one system is capable of accomplishing a nuclear safety function and one system, on its own, satisfies all nuclear safety-related systems requirements (e.g., redundancy, diversity, capacity), the designer shall classify the latter to the corresponding Safety Class and the other as NNS.

Equipment assigned to the different classes shall meet minimum requirements as prescribed in 3.3.3. The designer may impose more stringent design requirements than those corresponding to the applicable class. If this option is elected, the designer shall retain the original class designation.

Where a single item of equipment, or a portion thereof, provides two or more functions of dif-

ferent classes, it shall be classified to the more stringent class. Different portions of the same equipment (e.g., the tube side versus the shell side of a heat exchanger) may perform different functions and be assigned to different classes if the equipment contains a suitable interface boundary meeting the requirements of 3.3.2.

The designer may optionally provide two or more pieces of equipment, where one would suffice, to separately meet multiple environmental qualification requirements of SC-2 or -3 equipment for events where such separated qualification requirements are not simultaneously necessary, provided the design is consistent with ANSI/ANS-2.12-1978 [13]. For example, two ultimate heat sinks may be provided: one tornado-proof, but not seismically qualified; and the other not tornado-proof, but seismically designed. Because the simultaneous occurrence of the tornado and seismic event is $<10^{-6}$ occurrences/reactor year, these qualification requirements may be divided between two pieces of equipment, each of which shall be SC-3 and shall meet all other requirements for SC-3 equipment.

A support shall be classified to the more stringent class corresponding to the function provided either: (a) by the supported equipment, unless failure of the support could not jeopardize the function of the supported equipment; or (b) directly by the support itself. Exceptions may be made for intermediate elements (e.g., load-bearing housings of electric motors, valve operators, heat exchangers, or diesel engines) and access structures, whether of concrete or structural steel, outside the jurisdiction of supports covered by Subsection NF of Section III of the ASME Boiler and Pressure Vessel Code [14], that carry the weight of, or provide structural stability to SC-1, -2, or -3 equipment, either directly or through NF supports. Such intermediate elements shall be classified as SC-3 or NNS in accordance with either 3.3.1.3h. or 3.3.1.4f., as applicable.

3.3.1.1 Safety Class 1. Safety Class 1 (SC-1) shall apply to pressure-retaining portions and supports of mechanical equipment that form part of the RCPB whose failure could cause a loss of reactor coolant in excess of the reactor coolant normal makeup capability and whose requirements are within the scope of the ASME

¹³ Example classification of plant equipment utilizing the equipment classification criteria is given in Appendix A.

¹⁴ A single item of SC-1, SC-2, or SC-3 equipment and a "Basic Component" as defined in the Code of Federal Regulations, Part 21, "Reporting of Defects and Non-compliance," are equivalent.

Boiler and Pressure Vessel Code, Section III [14].¹⁵

3.3.1.2 Safety Class 2. Safety Class 2 (SC-2) shall apply to pressure-retaining portions and supports of primary containment and other mechanical equipment, requirements for which are within the scope of the ASME Boiler and Pressure Vessel Code, Section III [14], that is not included in SC-1 and is designed and relied upon to accomplish the following nuclear safety functions:

- a. Provide fission product barrier or primary containment radioactive material holdup or isolation,
- b. Provide emergency heat removal for the primary containment atmosphere to an intermediate heat sink, or emergency removal of radioactive material from the primary containment atmosphere (e.g., containment spray),
- c. Introduce emergency negative reactivity to make the reactor subcritical (e.g., boron injection system), or restrict the addition of positive reactivity via pressure boundary equipment,
- d. Ensure emergency core cooling where the equipment provides coolant directly to the core (e.g., residual heat removal and emergency core cooling), or

- e. Provide or maintain sufficient reactor coolant inventory for emergency core cooling (e.g., refueling water storage tank).

3.3.1.3 Safety Class 3. Safety Class 3 (SC-3) shall apply to equipment, not included in SC-1 or -2, that is designed and relied upon to accomplish the following nuclear safety functions:

- a. Provide for functions defined in SC-2 where equipment, or portions thereof, is not within the scope of the ASME Boiler and Pressure Vessel Code, Section III [14],
- b. Provide secondary containment radioactive material holdup, isolation, or heat removal,
- c. Except for primary containment boundary extension function, ensure hydrogen concentration control of the primary containment atmosphere to acceptable limits,
- d. Remove radioactive material from the atmosphere of confined spaces outside primary containment (e.g., control room or fuel building) containing SC-1, -2, or -3 equipment,

- e. Introduce negative reactivity to achieve or maintain subcritical reactor conditions (e.g., boron makeup),

- f. Provide or maintain sufficient reactor coolant inventory for core cooling (e.g., reactor coolant normal makeup system),

- g. Maintain geometry within the reactor to ensure core reactivity control or core cooling capability (e.g., core support structures),

- h. Structurally load-bear or protect SC-1, -2, or -3 equipment,¹⁶

- i. Provide radiation shielding for the control room or offsite personnel,

- j. Ensure required cooling for liquid-cooled stored fuel (e.g., spent fuel storage pool and cooling system),

- k. Ensure nuclear safety functions provided by SC-1, -2, or -3 equipment (e.g., provide heat removal for SC-1, -2, or -3 heat exchangers, provide lubrication of SC-2 or -3 pumps, provide fuel oil to the emergency diesel engine),

- l. Provide actuation or motive power for SC-1, -2, or -3 equipment,

- m. Provide information or controls to ensure capability for manual or automatic actuation of nuclear safety functions required of SC-1, -2, or -3 equipment,

- n. Supply or process signals or supply power required for SC-1, -2, or -3 equipment to perform their required nuclear safety functions,

- o. Provide a manual or automatic interlock function to ensure or maintain proper performance of nuclear safety functions required of SC-1, -2, or -3 equipment, or

- p. Provide an acceptable environment for SC-1, -2, or -3 equipment and operating personnel.

3.3.1.4 Non-Nuclear Safety. Non-Nuclear Safety (NNS) shall apply to equipment that is not included in SC-1, -2, or -3. This equipment is not relied upon to perform a nuclear safety function.

Some NNS equipment has one or more selected, but limited, requirements that are specified to ensure acceptable performance of specific NNS functions. The selected requirements are established on a case-by-case basis commensurate

¹⁵ Remaining portions of the RCPB shall be classified in accordance with 3.3.1.2 through 3.3.1.4 consistent with the interface requirements of 3.3.2. SC-1 requirements are intended to be equivalent to those of 10 CFR 50.55a.

¹⁶ This applies to concrete or steel structures that are not within the scope of ASME Boiler and Pressure Vessel Code.

with the specific NNS function performed.¹⁷ The functions performed by this subset of NNS equipment are:

- a. Process, extract, encase, or store radioactive waste,
- b. Provide cleanup of radioactive material from the reactor coolant system or the fuel storage cooling system for normal operations,
- c. Extract radioactive waste from, store, or transport for reuse irradiated neutron absorbing materials (e.g., boron compounds),
- d. Monitor radioactive effluents to ensure that release rates or total releases are within limits established for normal operations and transient events,
- e. Resist failure that could prevent any SC-1, -2, or -3 equipment from performing its nuclear safety function,¹⁸
- f. Structurally load-bear or protect NNS equipment providing any of the functions listed in 3.3.1.4,
- g. Provide permanent shielding for protection of SC-1, -2, or -3 equipment or of onsite personnel,
- h. Provide operational, maintenance or post-accident recovery functions involving radioactive materials without undue risk to the health and safety of the public,
- i. Following a control room evacuation, provide an acceptable environment for SC-1, -2, or -3 equipment required to achieve or maintain a safe shutdown condition,
- j. Handle spent fuel, the failure of which could result in fuel damage such that significant quantities of radioactive material could be released from the fuel,
- k. Ensure reactivity control of stored fuel,
- l. Protect SC-2 or -3 equipment necessary to attain or maintain safe shutdown following fire, or
- m. Monitor variables to:
 - (1) Verify that plant operating conditions are within technical specification limits (e.g., re-fueling water storage tank level, safety-related cooling water temperature),
 - (2) Indicate the status of protection system bypasses that are not automatically

removed as a part of the protection system operation,

(3) Indicate status of SC-1, -2, or -3 equipment, or

(4) Aid in determining the cause or consequences of events for post-accident investigation.

3.3.2 Safety Class Interfaces. If failure of Safety Class or NNS equipment connected to other Safety Class equipment could prevent the latter equipment from accomplishing its nuclear safety function, an interface barrier or isolation device shall be provided to protect the latter equipment.

3.3.2.1 Safety Class Interfaces for Pressure Integrity of Fluid Systems. A membrane (e.g., heat exchanger tube, bellows, piston, o-ring, or blind flange) that provides pressure boundary separation of equipment classes serves as the required barrier between any two classes, and shall be categorized to the more stringent class. Otherwise, the interface shall be in accordance with the following criteria.

Interface barriers or isolation devices connecting Safety Class or NNS fluid system equipment to other Safety Class equipment shall be capable of limiting the loss of fluid from the latter equipment if the former were to fail. The fluid loss shall be limited such that (1) if the fluid contains radioactivity, the applicable dose criteria¹⁹ are met and (2) if the fluid performs a nuclear safety function (e.g., heat transfer) sufficient inventory and pressure are maintained to perform that function. The closure time of open valves, the leak tightness of closed valves, and the limitation of losses due to flow restrictions shall be evaluated when determining the loss of fluid. The loss of fluid shall be assessed for the full duration of the event. The loss of fluid limitation shall be met applying the single failure criterion to the actuation of the interface barriers or isolation devices.²⁰

The following cases are examples of fluid systems Safety Class interfaces that satisfy the preceding criteria. These arrangements are only examples, and other arrangements satisfying the criteria of 3.3.2.1 shall be acceptable. Where equipment of differing classes is interconnected,

¹⁷ Refer to Table 3-5 and Section 4, Design Criteria, for these selected requirements and Appendix A for additional guidance.

¹⁸ See Table 3-5, Note 4.

¹⁹ See Table 3-1.

²⁰ See 3.2.1.



the more stringent class extends to and includes the cited barriers. Combinations of the following cases are acceptable if the requirements for each arrangement are satisfied (e.g., Cases 2e and 4b are joined to form Case 3d).

Where a valve serves, in whole or part, as an interface barrier, the designation of valve type in individual criteria given as follows signifies the lowest permissible valve type of the valve hierarchy acceptable. Inherent in each criterion is permission to substitute any other valve higher in the ranking. Starting with the lowest ranked valve, the ranking follows: normally open local manual valve, normally open remote manual valve, normally open automatic valve, and administratively closed valve.

Illustrations of the fluid system Safety Class interfaces are shown schematically in Figure 3-1.

Case 1

From SC-1, -2, or -3 piping²¹ to any less stringently classified piping the interface is at the pressure boundary of one safety or relief valve or one vacuum breaker.

Case 2

SC-1 or -2 piping of the RCPB that does not penetrate primary containment:

a. From SC-1 to SC-2, the interface is at a flow restriction secured by an SC-1 reactor coolant system nozzle weld,

b. From SC-1 to SC-2, the interface is at the outlet of one passive or the outermost of two active flow restricting devices,

c. From SC-1 or -2 to NNS, the interface is at the outermost of two passive flow restricting devices, between the flow restricting devices, SC-2 may apply,

d. From SC-1 to NNS, the interface is at the outermost connection of two valves administratively closed during reactor operation,

e. From SC-2 to NNS, the interface is at the outermost connection of two valves, each of which is capable of automatic closure, meeting the closure time requirements of 3.3.2.1.2,

f. From SC-1 to SC-3, the interface is at the outermost connection of two valves, each of which is capable of automatic closure, meeting the closure time requirements of 3.3.2.1.2,

g. From SC-1 to SC-2, the interface is at the outermost connection of two check valves, where the flow path is into the reactor coolant system, but only when the SC-2 equipment performs an emergency core cooling function,²²

h. From an SC-2 sensing line to SC-3 or NNS, the interface is at the outermost connection of a single local manual valve. The NNS equipment shall be seismic category I, or

i. From SC-1 to SC-3 or NNS, the interface is at the outermost connection of a single local manual valve located beyond two SC-1 check valves, where the flow path is into the reactor coolant system.

Where flow restrictors provide the means for obtaining an interface between Safety Classes (i.e., Cases 2a, 2b, and 2c), it shall be demonstrated that, upon failure of the SC-2 equipment during reactor operation, the reactor can be shut down and cooled down in an orderly manner, assuming reactor coolant normal makeup only. A controlled leakage shaft seal system (having both the controlled leakage and another seal) may qualify as Case 2c, provided it meets this criterion. Orifices, or connected small equipment may serve as the passive flow restricting device allowed in Cases 2b and 2c.

An excess flow check valve that includes a restricting bypass or a fail closed self-actuated pressure regulating valve may serve as the active flow restricting device allowed in Case 2b.

For the aforementioned Cases 2e and 2f, a check valve may be used as one of the valves capable of automatic closure only where the flow path is into the reactor coolant system. If two valves are required for a Case 2 interface, only one may be a check valve with the exception of Case 2g.

Case 3

SC-1 or -2 piping of the RCPB penetrating primary containment:

a. From SC-1 to SC-2, the interface is at the outermost connection of two valves, each of which is capable of automatic closure; from SC-2 to any less stringent class, the interface is at the outermost connection of a third remote manual valve. Closure time requirements of interface valves shall meet the requirements of 3.3.2.1.2,

²¹In the context of the criteria of 3.3.2.1, piping includes ducting.

²²When the case is used, provisions for periodic testing of each check valve for leak tightness shall be included.

b. From SC-2 to NNS, the interface is at the outermost connection of two valves, each of which is capable of automatic closure, meeting the closure time requirements of 3.3.2.1.2,

c. From SC-1 to SC-2, the interface is at the outermost connection of two check valves, both of which are inside primary containment, where the flow path is into the reactor coolant system only; from SC-2 to SC-3, the interface is at the outermost connection of one automatic valve located outside primary containment, meeting the closure time requirements of 3.3.2.1.2,

d. From SC-2 to NNS, the interface is inside primary containment at the outermost connection of two valves, each of which is capable of automatic closure, meeting the closure time requirements of 3.3.2.1.2; and from SC-2 to NNS, the interface is at both the innermost and outermost connection of two valves located on either side of the primary containment, each of which is capable of automatic closure, meeting the closure time requirements of 3.3.2.1.2, or

e. From SC-1 to NNS piping less than or equal to six inches in diameter, the interface is at the outermost connection of two valves, each of which is capable of automatic closure, meeting the closure time requirements of 3.3.2.1.2.

For the aforementioned Cases 3a, 3b, and 3d, a check valve may be used as one of the valves capable of automatic closure only where the flow path is into the reactor coolant system.

Case 4

SC-2 or low energy SC-3 closed piping²³ penetrating primary containment, or SC-2, -3, or NNS open piping penetrating primary containment:

a. From SC-2 or low energy SC-3 closed piping to any less stringent class through an SC-2 primary containment penetration, the interface is at the outermost connection of a SC-2 single valve located outside primary containment, which is capable of remote manual

²³ "Closed piping" refers to piping so arranged that it and connecting pressure boundary equipment located inside the primary containment provide a continuous extension of the primary containment capable of withstanding, in a leak-proof condition, primary containment design pressure when internally subjected to atmospheric pressure conditions and is capable of maintaining its integrity throughout the event for which primary containment integrity is required (e.g., protected from missiles or pipe whip if such hazards are part of the event).

closure, meeting the closure time requirements of 3.3.2.1.2, or

b. From SC-2, SC-3, or NNS open piping, the interface is at both the innermost and outermost connection of two valves located on either side of primary containment, each of which is capable of automatic closure, meeting the closure time requirements of 3.3.2.1.2. A check valve may be used as one of the valves capable of automatic closure only where the flow path is into the primary containment.

Case 5

Instrument piping penetrating primary containment (see case 2h of Figure 3-1 for instrument piping not penetrating primary containment):²⁴

a. From an SC-2 sensing line, whether connected to the RCPB or not, to SC-3 (for protection system application) or NNS outside primary containment, the interface is at the outermost connection of a local manual valve, located outside primary containment, meeting the closure time requirements of 3.3.2.1.2. The NNS equipment shall be seismic category I, or

b. From an SC-2 protection system closed sensing line penetrating the primary containment connected to an SC-2 protection system closed instrument line, neither an interface nor valve is required.

Case 6

From SC-2 or -3 piping totally inside or outside the primary containment and not connected to the RCPB to any less stringent class, the interface is at:

a. The less stringent class connection to one administratively closed valve,

b. The less stringent class connection to two valves, each of which is capable of remote manual closure, meeting the closure time requirements of 3.3.2.1.2,

c. The less stringent class connection to one passive or two active flow restricting devices, provided that the flow is so limited that failure of the less stringent class equipment does not result in: (1) loss of nuclear safety function of the more stringent class equipment; or (2) an accident, or

²⁴ Sensing lines for instruments that are not part of the Protection System may utilize these criteria provided the provisions of Regulatory Guide 1.11, "Instrument Lines Penetrating Primary Reactor Containment" are satisfied. Available from U.S. Nuclear Regulatory Commission, Washington, D.C. 20555.

d. The connection of the less stringent class equipment to the more stringent class equipment if failure of the less stringent class equipment does not result in: (1) loss of the nuclear safety function of the more stringent class equipment; or (2) an accident (e.g., an NNS vent line of an SC-3 atmospheric storage tank whose failure would not result in loss of fluid from the tank, or a pressure sensing NNS instrument branch connection off an SC-3 piping system where failure of the branch connection would neither affect the nuclear safety function of the system nor cause unacceptable flooding; in such a case, the interface boundary of the SC-3 piping is the controlling restriction).

3.3.2.1.1 Primary Containment Penetration Interface. Detailed requirements for primary containment isolation are provided in American National Standard Containment Isolation Provisions for Fluid Systems, N271-1976/ANS-56.2 [15]. Any fluid system penetration through the primary containment and its corresponding primary containment isolation devices, whether inside or outside, shall be no less than SC-2. Where system piping that penetrates the primary containment boundary is assigned a less stringent Safety Class than SC-2 (on either side of the penetration), then the interface to SC-2 shall be at its connection to a primary containment isolation valve or a primary containment penetration assembly.

3.3.2.1.2 Special Barrier Valve Requirements. Closure time (including detection and actuation time) for each normally open valve shall be such that for any credible failure, all nuclear safety functions are ensured and the requirements of N271-1976/ANS-56.2 [15] are met.^{25,9}

3.3.2.1.3 Testability. There shall be provisions for periodic functional testing of any valve or active flow-restricting device for which credit is taken as an interface barrier. Additional requirements for periodic functional testing are provided in ASME Boiler and Pressure Vessel Code, Section XI [16].

3.3.2.2 Safety Class Interfaces for Electrical Systems. Safety Class interfaces for electrical equipment shall be in accordance with accepted criteria.²⁵

²⁵For guidance, see Section 6 of IEEE 384-1981, "Criteria for Independence of Class 1E Equipment and Circuits." (See footnote 8 for the availability of IEEE standards.)

3.3.2.3 Safety Class Interfaces for Other Equipment. The classification requirements for supports and mechanical movers or links shall be as required in 3.3.1. No interface barrier is required when interconnected mechanical equipment consists of differing Safety Classes, mechanical equipment connected to structures or electrical equipment, or electrical equipment connected to structures.

3.3.3 Safety Class Requirements Correlations. Basic requirements associated with each equipment class are specified in Section 3, General Safety Criteria, and listed in Table 3-5. More detailed requirements for particular structures, systems, and components are specified in Section 4, Design Criteria, or in ancillary standards cited in 4. Section 4 identifies and defines the normally operating and mitigating plant systems and states their nuclear safety functions, Safety Class requirements, performance criteria, and design criteria.

3.4 Industry Codes and Standards. Industry codes and standards shall be utilized in the design, fabrication, and installation of structures, systems, and components where such codes and standards are available and applicable.

For equipment and design conditions that are not covered by the applicable codes, appropriate criteria for stress, deformation, fatigue and other limits shall be established and utilized by the designer for each event, if needed. The criteria may be based on the criteria established in applicable industry codes or standards for similar equipment, may be derived from manufacturer's standards, or may be derived from empirical methods based upon field experience and testing. Such derived requirements shall, to the extent practicable, reflect consistency with similar requirements for other equipment in the same class.

3.4.1 Safety Class 1, 2, and 3 Mechanical Equipment. In order to meet the nuclear safety criteria of Table 3-2, the normally operating systems and mitigating systems for various events shall be designed to appropriately conservative limits. Safety Classes are established for components of these systems based on their importance in meeting the nuclear safety criteria in Table 3-2 for the spectrum of events.

ASME Boiler and Pressure Vessel Code, Section III, Division 1 (ASME III) [14] Classes for pres-

sure retaining components provide different quality levels of construction.²⁶ Different allowable stress levels (different service limits) for pressure-retaining components provide different margins to failure and hence different reliability levels for the pressure-retaining function.

The following general criteria shall be used by the designer:

a. Correlation of Safety Class with ASME III Class:

(1) ASME III Class 1 design rules shall apply to Safety Class 1 components.

(2) ASME III Class 2 design rules shall apply to Safety Class 2 components.

(3) ASME III Class 3 design rules shall apply to Safety Class 3 components.

b. Design Loadings

Design loadings shall be established in the design specification. The design limits of the appropriate subsection of ASME III shall not be exceeded for the design loadings specified.

c. Operating Basis Earthquake (OBE)

The magnitude of the OBE shall be determined based on the considerations in 10 CFR 100, Appendix A [2]. At the designer's option the magnitude of the OBE may be determined by a probability analysis based on a best-estimate probability of occurrence of 1×10^{-2} /reactor year at the plant site.²⁷ The inertial portion of the OBE load shall be included in the PC-3 transient loads (L_3).²⁸

d. Safe Shutdown Earthquake (SSE)

The magnitude of the SSE shall be determined based on the considerations in 10 CFR 100, Appendix A [2]. The inertial portion of the SSE load shall be included in the PC-5 transient loads (L_5).

e. Application of ASME III Service Limits

The correlation between PC categories, nuclear safety functions, and ASME III Service Limits shown in Table 3-6 shall be used.

²⁶ Refer to ASME Boiler and Pressure Vessel Code, Section III, Division 1 for definition of "construction."

²⁷ Where the OBE magnitude is determined to be less than one-half the SSE magnitude, supporting data should be presented in accordance with 10 CFR 100, Appendix A, Section II. Methods for determining the probability of an earthquake of a certain magnitude are under development by the American Nuclear Society.

²⁸ ASME III currently considers the OBE as a "design mechanical load," which would require its consideration as a design load, not a service condition "B" load.

3.4.2 Safety Class 3 Electrical Equipment. The design of SC-3 electrical equipment (IEEE Class 1E equipment) shall meet the requirements of the industry codes and standards listed in Table 3-7.

3.4.3 Safety Class 2 and 3 Structures. The design of SC-2 and -3 structures shall meet the requirements of the industry codes and standards listed in Table 3-8.

3.4.4 Non-Nuclear Safety Equipment. The design of Non-Nuclear Safety mechanical equipment, electrical equipment, and structures shall meet the requirements of the industry codes and standards specified in Section 4, Design Criteria.

3.4.5 Quality Assurance. All equipment designated SC-1, -2, -3 or NNS that provide the functions listed in 3.3.1.1 through 3.3.1.4 shall have quality assurance programs devised and implemented to ensure an acceptable level of confidence that the included structures, systems, and components can perform their functions.

3.4.5.1 Safety Class 1, 2, and 3. The quality assurance program implemented for SC-1, -2, and -3 equipment shall apply those pertinent requirements and applicable elements of American National Standard Quality Assurance Program Requirements for Nuclear Power Plants, ANSI/ASME NQA-1-1979 [17].²⁹ These requirements shall be applied wholly or in part depending on the nature and scope of the work to be performed and the relative importance to safety of the item or service produced. The organization applying these requirements shall be responsible for specifying the degree of applicability of ANSI/ASME NQA-1-1979 [17] requirements. Further, that responsible organization shall appropriately relate the specified quality requirements to specific items or services furnished.

The application of quality assurance program requirements, or portions thereof, shall be specified by the responsible organization in written contracts, policies, procedures or instructions.

3.4.5.2 Non-Nuclear Safety. The quality assurance program implemented for this equipment having the functions listed in 3.3.1.4 shall be sufficient to ensure that the functions of the equipment shall be achieved. Selected requirements from ANSI/ASME NQA-1-1979 [17]²⁹

²⁹ Further guidance is provided in NRC regulation 10 CFR 50, Appendix B, and in "Quality Assurance Program Requirements for Nuclear Power Plants," ANSI/ASME N45.2-1977, and applicable daughter standards.

shall be applied to the aforementioned equipment to provide adequate certification or other records to ensure that items or services as furnished and installed meet specified requirements.

No formalized quality assurance program is required for other NNS equipment.

3.5 Safety Analyses. The General Design Criteria, Appendix A to 10 CFR 50, [1] require that a nuclear unit be able to survive an initiating occurrence without causing undue risk to the health and safety of the public. These criteria recognize that a nuclear unit is subject to failures that differ in severity, and hence require different levels of protection.

The criteria established in 3.2 require a set of limiting normal operations for PC-1 and limiting events for each PC other than PC-1 to be identified based on their best-estimate frequency of occurrence. A detailed safety analysis shall be performed based on this limiting set. This safety analysis shall constitute the technical basis to demonstrate that the nuclear unit can be operated without undue radiological risk to the health and safety of the public.

3.5.1 General Requirements. Systematic analyses shall be made of the capabilities of the plant structures, systems, and components to perform intended nuclear safety functions. These analyses shall show that the limiting set of normal operations and events considered in design are accommodated within the plant nuclear safety criteria stipulated in Table 3-2.

To implement these analyses, the following shall be considered for all normal operations and events identified in 3.2:

- a. Identify nuclear safety-related structures, systems, and components to be utilized for the normal operations or events to be analyzed,
- b. Identify and establish nuclear safety requirements for the SC-1, -2, and -3 structures, systems, and components,
- c. Identify and establish requirements for NNS structures, systems, and components,
- d. Identify nuclear safety-related actions to be taken by operators and their associated times. Consider equipment status to be controlled to accomplish the nuclear safety functions.

e. Ascertain that the nuclear safety functions are accomplished within the restrictions imposed by the criteria of Section 4, and

f. Establish the operating limits or restrictions to be imposed on the structures, systems, and components, including surveillance and testing.

3.5.2 Requirements for Plant Condition-1. Analyses shall be made to determine the control requirements and administrative restrictions necessary to ensure that nuclear safety-related actions are not required during normal operations. These analyses shall include evaluation of the following to the extent that they are pertinent:

- a. Radioactive material release control,
- b. Reactor coolant flow rate control,
- c. Core power level control,
- d. Core power distribution control,
- e. Reactor coolant system inventory control,
- f. Reactor coolant system pressure control,
- g. Reactor coolant system temperature control,
- h. Reactor coolant system water quality control,
- i. Reactor coolant system leakage control,
- j. Core reactivity control,
- k. Control rod assembly worth,
- l. Primary containment pressure and temperature control,
- m. Shielding, cooling, and reactivity control of stored fuel,
- n. Refueling restrictions,
- o. Environmental conditions,
- p. Electrical power supply, and
- q. Engineered safety features status.

3.5.3 Requirements for Other Plant Conditions. Analyses shall be made to determine nuclear safety-related action requirements, administrative restrictions, or control requirements during the limiting set of events for each PC other than PC-1. For each event considered, the analyses shall account for parameters and variations listed below, to the extent that they are pertinent:

a. Initial conditions at the time of event initiation including, but not restricted to, the effects of:

- (1) Reactor power, reactor coolant temperatures and pressure, margin to departure from nucleate boiling ratio safety limit, and other applicable conditions taking into account control system response and instrument accuracies,
- (2) The full range of expected normal operating conditions, including:

- (a) Operating modes, and
- (b) Systems under manual control considering alarm points, manual action requirements, and protective overrides,
- (3) Variations in plant parameters with reactor power and core exposure,
- (4) Spatial power distribution in the core including the effects of:
 - (a) Reactivity feedback through fuel temperature, moderator, density, pressure, and voids,
 - (b) Distribution of fixed and movable solid neutron absorbing materials, and
 - (c) Distribution of fission products (e.g., xenon and samarium),
- (5) Status of motive power systems (e.g., electrical, air, hydraulic), including emergency motive power systems,
- (6) Status of protection systems, and

(7) Status of related systems (event coupling and multi-unit considerations);

b. The variation of plant parameters during events that might significantly affect the analytical results, such as pressure, distribution of core voids, heat transfer coefficients, reactor coolant system water inventory, and response of control or protection system;

c. Any force or pressure transients that might affect the integrity of fission product barriers (e.g., reactivity effects, additional energy release); and

d. The performance characteristics of the protection systems and engineered safety features utilized to mitigate the consequences of the event, including circuit characteristics (e.g., response times, saturation effects), instrument errors, and dynamic characteristics of the required motive power and fluid systems.

Table 3-1
Offsite Radiological Dose Criteria for Plant Conditions

<u>Best-Estimate Frequency of Occurrence (F) Per Reactor Year</u>	<u>Plant Condition (PC)</u>	<u>Offsite Radiological Dose Criterion</u>
Normal Operations	PC-1	10 CFR 50, App. I ^(a) [18]
$F \geq 10^{-1}$	PC-2	10 CFR 50, App. I ^(a) [18]
$10^{-1} > F \geq 10^{-2}$	PC-3	10% 10 CFR 100 ^(b) [2]
$10^{-2} > F \geq 10^{-4}$	PC-4	25% 10 CFR 100 ^(b) [2]
$10^{-4} > F \geq 10^{-6}$	PC-5	100% 10 CFR 100 ^(b) [2]

NOTES:

- (a) The plant shall be designed to meet the dose objectives of the Code of Federal Regulations, Title 10, "Energy," Part 50, "Licensing of Production and Utilization Facilities," Appendix I [18], for the summation of the radioactive releases during PC-1 normal operations and the annual average radioactive releases (i.e., product of event release and event frequency) due to PC-2 events based on realistic analyses.
- (b) The plant shall be designed to meet the dose criteria for PC-3, PC-4, and PC-5 events based on reasonably conservative analyses, considering initial plant parameters may be at their limiting values consistent with the technical specifications. The conservative analyses shall be performed using methods that reasonably account for the actual plant and site characteristics and using methods that conservatively include the dose reducing features of both the plant and the site. These dose criteria do not apply to the long-term recovery phase of an event. The point at which these criteria cease to apply and what criteria shall replace them shall be determined on a case-by-case basis.

Table 3-2
Plant Nuclear Safety Criteria

Nuclear Safety Criteria	Plant Condition				
	<u>PC-1</u>	<u>PC-2</u>	<u>PC-3</u>	<u>PC-4</u>	<u>PC-5</u>
a. The normal operations or event shall be accommodated within the offsite radiological dose criteria of Table 3-1.	X	X	X	X	X
b. The normal operations or event shall be accommodated within the code and standard requirements of 3.4.	X	X	X	X	X
c. The normal operations or event shall be accommodated with appropriate margin to ensure that fuel design limits are not exceeded.	X	X	X		
d. The normal operations shall not preclude achieving and maintaining normal shutdown and cooldown of the plant.	X				
e. The event shall not preclude achieving and maintaining an orderly shutdown and cooldown of the plant.		X			
f. The event shall not preclude achieving and maintaining a controlled shutdown and cooldown of the plant.			X	X	X
g. The normal operation or event shall cause no loss of nuclear safety function to require nuclear safety-related equipment.	X	X	X	X	X

Table 3-3

Example of a Set of Limiting Normal Operations and Limiting Events³⁰

This table illustrates an interpretation and application of the criteria presented in 3.2 in categorizing an example set of limiting normal operations and limiting events. The categorization of a given event might be different for a specific plant. The designer shall ensure that a limiting set of normal operations and events are identified for each specific plant and the appropriate categorization is determined for each normal operation and event.³¹

PC-1

- Startup
- Shutdown (hot and cold)
- Refueling
- Hot standby
- Power operation
- During any of the above:
 - Accommodation of the normal range of internal environmental effects (i.e., pressure, temperature, humidity, radiation),
 - Fuel cladding defects within plant technical specification limits,
 - Operation with specific items of equipment out of service or under testing within plant technical specification limits,
 - Plant conditions providing industrial security, see American National Standard Security for Nuclear Power Plants, ANSI/ANS-3.3-1982 [19],
 - Operation with steam generator tube leakage within plant technical specification limits, or
 - Accommodation of maintenance, testing and inspection requirements (e.g., ASME Boiler and Pressure Vessel Code, Section XI [16]).

PC-2

- Inadvertent control assembly group withdrawal
- Partial loss or interruption of reactor coolant flow, excluding reactor coolant pump locked rotor
- Partial loss of safety-related equipment cooling or area cooling (e.g., loss of one cooling train)
- Control rod drop
- Reactor coolant system depressurization by inadvertent operation of an active component (e.g., a safety or relief valve)
- Minor reactor coolant system or connecting system leakage that would not prevent orderly reactor shutdown and cooldown using only makeup provided by normal makeup systems
- Fire limited to one fire area
- Minor power conversion system leakage that would not prevent orderly reactor shutdown and cooldown using only makeup provided by normal makeup systems
- Reactor-turbine load mismatch, including loss of load, excess load and turbine trip. (Causes could be secondary system equipment failure, such as main steam isolation valve, loss of feedwater flow, or partial loss of feedwater heating)

³⁰Site conditions in 3.2.7 and natural and man-made hazards in 3.2.8 are to be accommodated according to their frequency of occurrence; they occur as items in all plant conditions.

³¹The following events that were under development concurrent with the preparation of this standard are not included in the example but might be required on specific plants by regulatory authorities:

- Loss of offsite AC power and onsite emergency AC power sources,
- Control room personnel evacuation, and
- Anticipated transient without scram.

Table 3-3 (Continued)

- Inadvertent chemical shim dilution
- Loss of feedwater flow
- Partial loss of feedwater heating
- Reactor trip
- Inadvertent emergency core cooling system actuation
- Inadvertent reactor coolant system depressurization by normal or auxiliary pressurizer spray cooldown
- Single operator error
- Single failure of an active component or control component (nuclear safety-related or not)
- Single failure in the electrical systems (nuclear safety-related or not)
- Loss of instrument or service air compressor
- Generator trip
- Turbine trip
- Steam generator tube leakage in excess of plant technical specifications but less than the equivalent of a full-tube rupture.

PC-3

- Reactor coolant system leakage that would not prevent a controlled reactor shutdown and cooldown
- Power conversion system leakage that would not prevent a controlled reactor shutdown and cooldown
- Loss of offsite ac power, including consideration of voltage and frequency disturbances
- Operation with a fuel assembly in any misoriented or misplaced position
- Inadvertent withdrawal of any single control assembly during refueling
- Inadvertent primary containment spray actuation
- Minor fuel handling accident
- Complete loss or interruption of forced reactor coolant flow excluding reactor coolant pump locked rotor
- Full rupture of one steam generator tube.

PC-4

- Small LOCA
- Drop of a spent fuel assembly involving only the dropped assembly
- Leakage from spent fuel pool in excess of normal makeup capability
- Single reactor coolant pump locked rotor
- Blowdown of reactor coolant through multiple safety or relief valves
- Rupture of any non-seismic Category I vessel containing radioactive materials
- Control rod withdrawal error such that plant technical specification limits could be exceeded
- Any design basis moderate energy line crack or high energy line break outside primary containment except in the main steamline upstream of the turbine stop valve or the main feed line downstream of the feedwater control valve.

PC-5

- Major LOCA, up to and including the largest justified pipe rupture in the reactor coolant pressure boundary
- Single control rod ejection
- Major power conversion system pipe rupture, up to and including the largest justified pipe rupture
- Drop of a spent fuel assembly onto other spent fuel assemblies.