

American Nuclear Society

nuclear safety design process for modular helium-cooled reactor plants

an American National Standard

REAFFIRMED

October 7, 2021

November 1, 2016

ANSI/ANS-53.1-2011; R2021

This standard has been reviewed and reaffirmed with the recognition that it may reference other standards and documents that may have been superseded or withdrawn. The requirements of this document will be met by using the version of the standards and documents referenced herein. It is the responsibility of the user to review each of the references and to determine whether the use of the original references or more recent versions is appropriate for the facility. Variations from the standards and documents referenced in this standard should be evaluated and documented.

This standard does not necessarily reflect recent industry initiatives for risk informed decision-making or a graded approach to quality assurance. Users should consider the use of these industry initiatives in the application of this standard.



published by the
American Nuclear Society
555 North Kensington Avenue
La Grange Park, Illinois 60526 USA

**American National Standard
Nuclear Safety Design Process
for Modular Helium-Cooled Reactor Plants**

Secretariat
American Nuclear Society

Prepared by the
**American Nuclear Society
Standards Committee
Working Group ANS-53.1**

Published by the
**American Nuclear Society
555 North Kensington Avenue
La Grange Park, Illinois 60526 USA**

Approved December 21, 2011
by the
American National Standards Institute, Inc.

American National Standard

Designation of this document as an American National Standard attests that the principles of openness and due process have been followed in the approval procedure and that a consensus of those directly and materially affected by the standard has been achieved.

This standard was developed under the procedures of the Standards Committee of the American Nuclear Society; these procedures are accredited by the American National Standards Institute, Inc., as meeting the criteria for American National Standards. The consensus committee that approved the standard was balanced to ensure that competent, concerned, and varied interests have had an opportunity to participate.

An American National Standard is intended to aid industry, consumers, governmental agencies, and general interest groups. Its use is entirely voluntary. The existence of an American National Standard, in and of itself, does not preclude anyone from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard.

By publication of this standard, the American Nuclear Society does not insure anyone utilizing the standard against liability allegedly arising from or after its use. The content of this standard reflects acceptable practice at the time of its approval and publication. Changes, if any, occurring through developments in the state of the art, may be considered at the time that the standard is subjected to periodic review. It may be reaffirmed, revised, or withdrawn at any time in accordance with established procedures. Users of this standard are cautioned to determine the validity of copies in their possession and to establish that they are of the latest issue.

The American Nuclear Society accepts no responsibility for interpretations of this standard made by any individual or by any ad hoc group of individuals. Responses to inquiries about requirements, recommendations, and/or permissive statements (i.e., “shall,” “should,” and “may,” respectively) should be sent to the Standards Department at Society Headquarters. Action will be taken to provide appropriate response in accordance with established procedures that ensure consensus.

Comments on this standard are encouraged and should be sent to Society Headquarters.

Published by

**American Nuclear Society
555 North Kensington Avenue
La Grange Park, Illinois 60526 USA**

Copyright © 2011 by American Nuclear Society. All rights reserved.

Any part of this standard may be quoted. Credit lines should read “Extracted from American National Standard ANSI/ANS-53.1-2011 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

Inquiry Requests

The American Nuclear Society (ANS) Standards Committee will provide responses to inquiries about requirements, recommendations, and/or permissive statements (i.e., “shall,” “should,” and “may,” respectively) in American National Standards that are developed and approved by ANS. Responses to inquiries will be provided according to the Policy Manual for the ANS Standards Committee. Nonrelevant inquiries or those concerning unrelated subjects will be returned with appropriate explanation. ANS does not develop case interpretations of requirements in a standard that are applicable to a specific design, operation, facility, or other unique situation, and therefore is not intended for generic application.

Responses to inquiries on standards are published in ANS’s magazine, *Nuclear News*, and are available publicly on the ANS Web site or by contacting the ANS standards administrator.

Inquiry Format

Inquiry requests must include the following:

- (1) the name, company name if applicable, mailing address, and telephone number of the inquirer;
- (2) reference to the applicable standard edition, section, paragraph, figure, and/or table;
- (3) the purposes of the inquiry;
- (4) the inquiry stated in a clear concise manner;
- (5) a proposed reply, if the inquirer is in a position to offer one.

Inquiries should be addressed to

American Nuclear Society
ATTN: Standards Administrator
555 N. Kensington Avenue
La Grange Park, IL 60526

or standards@ans.org

Foreword

(This Foreword is not a part of American National Standard “Nuclear Safety Design Process for Modular Helium-Cooled Reactor Plants,” ANSI/ANS-53.1-2011.)

The purpose of this standard is to provide nuclear safety criteria applicable to the design of modular helium-cooled reactor (MHR) nuclear power plants (hereinafter referred to as “plants”). To achieve this purpose, this standard provides a process that can be used to

- develop MHR top-level nuclear regulatory safety criteria;
- identify safety functions, top-level design criteria, licensing-basis events, design-basis accidents, and methods for performing safety analyses;
- determine safety classification of systems, structures, and components (SSCs);
- identify safety-related SSC special treatment requirements and defense-in-depth (DID) provisions;
- demonstrate the adequacy of DID by applying a risk-informed approach.

This standard does not address plant security design requirements or criteria. MHR security design requirements, including design-basis threats, are design elements that may be brought into the plant design process to address licensing requirements of the national nuclear regulator. In general, both deterministic and risk-based approaches may be considered in the plant security design process. It is anticipated that MHR passive safety features and inherent safety characteristics together with the use of the risk-informed nuclear safety process herein will effectively support plant security design.

This risk-informed process standard represents a new design approach for professional communities familiar with traditional, deterministic light water reactor (LWR) design processes. These include plant architect/engineers, nuclear licensing, and risk assessment professionals. This process presents an opportunity to extend traditional use of probabilistic risk assessment as applied to LWRs to MHRs and to incorporate risk insights early in the design process. Two examples are (a) modeling long-duration nonequilibrium plant conditions and (b) extensive quantification of event frequency and consequence, including uncertainty. Nuclear professional communities should develop other complementary risk-informed, performance-based consensus processes that continue to address the challenges presented with this standard.

In addition to designers, regulators, and the risk community, this standard provides a tool for plant operators who use design processes to maintain licensed plant designs. Some uses of this standard, such as SSC classification, apply beyond initial plant design, procurement, and construction into operations. Use of this standard for SSC classification also allows plant owner/operators to specify special treatments over the life of the plant for procurement, application, testing, and maintenance commensurate with risk. This standard documents an established process that nuclear design organizations can use to develop nuclear safety designs. It is anticipated that sponsors and communities of MHR-based designs will develop further specific designs with dependent standards that integrate these risk-informed characteristics. In any event, the fundamental objective of this standard is to provide clear design process guidance subordinate to the MHR’s fundamental design technology. Because the traditional LWR design community is unfamiliar with MHR technology, it is expected that this standard will present the first non-LWR design process challenge.

Consider the question of secondary containment in LWRs. For high-temperature gas-cooled reactors (HTGRs), fundamentally different approaches to retention of radionuclides lead to differences in the design of the reactor building.

To specify “containment” directly, as commonly used and interpreted for LWRs, would supersede the design development process of this standard. Therefore, that is not done. The design process provided in this standard is adequate alone to assure that the containment of radionuclide safety functions is accomplished. For that reason, this standard does not specify discrete design applications that those familiar with other reactor types, like LWRs, might expect. Rather, only the fundamental attributes that distinguish an MHR are provided. Those are the minimum set of design characteristics, agreed upon by this working group, which must be met for the use of this standard.

This standard could reference documents or other standards that have been superseded or withdrawn when the standard is applied. In that case, references in the section(s) include statements that provide guidance on their use. The format of the standard provides a table at the end of each body of text that summarizes and provides succinct actionable content required. The “Summary of Requirements” tables at the end of each body of text provide that body of text’s explicit requirements. Users should evaluate the requirements with the tables at the end of each body of text. In the event of a compliance question with the standard’s requirements, evaluation should include the explicit body of text in the standard. The tables should be used to evaluate compliance, in the event of a question of compliance with the standard’s requirements.

This standard was initiated in 1971 and released as N213, January 1974 Draft, “Nuclear Safety Criteria for the Design of Stationary Gas Cooled Reactor Plants,” for comment. Waning interest in gas reactors left that early deterministic standard incomplete. Two LWR counterparts, ANSI N18.2-1973, “Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants” (redesignated ANS-51.1), and ANSI/ANS-52.1-1978, “Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants,” were completed and approved. Revisions of both these standards were approved in 1983 adding a form of risk-based classification; however, all these documents remained essentially deterministic compilations of the state-of-the-art design from that era.

The American Nuclear Society Gas-Cooled Reactor Design and Operation Subcommittee, ANS-28, was inaugurated in November 2003 and tasked with developing ANS-53.1. The working group was quickly formed and began development on this standard in 2004. Use of this standard does not supersede the responsibility to review and apply the top-level safety criteria (TLSC) of the authorities in the country where the user plans to license, build, and operate MHR(s). The users of this standard are responsible to review and apply the TLSC set by the authorities in whichever country the user plans to license, build, and operate MHR(s). This standard may also be used to support the preparation of an MHR safety analysis report for the purpose of MHR licensing. When used for MHR licensing, the standard does not provide the only basis for establishing the MHR safety and design criteria. The designer also assesses the applicability of the existing body of technical licensing requirements and guidance for nuclear plant licensing in the particular country of application. In this regard, the designer determines the applicability, partial applicability, or nonapplicability of these licensing requirements. The designer may also use this standard and other supporting standards to determine what additional MHR licensing technical requirements are required for important technical design and safety aspects that are not addressed by the existing body of technical licensing requirements and guidance.

In light of the 2011 disaster in Japan at Fukushima Daiichi Units 1 through 4, the ANS-28 Subcommittee stresses that those events have been considered for

this standard as well as they are known at this time. Furthermore, while those issues are being developed, as a process standard, we do not anticipate that the process that this standard identifies will be changed at all. This standard does not exclude the use of any additional guidance or requirements to supplement that information.

The ANS-53.1 Working Group consisted of the entire ANS-28 Subcommittee of the American Nuclear Society. Members of ANS-28 who participated directly in the development of this standard are as follows:

J. K. August** (Chair, 2007–2011; Vice Chair, 2003–2007), *CORE, Inc.*
M. A. LaBar (Chair, 2003–2007), *General Atomics*
R. L. Bratton (Secretary), *Idaho National Laboratory*

J. M. Bolin, *General Atomics*
S. A. Caspersson, *Westinghouse Electric Company, LLC*
M. T. Coyle, *Exelon Nuclear*
J. C. Cunliffe, *Bechtel Systems & Infrastructure, Inc.*
K. N. Fleming, *Technology Insights*
J. P. Gaertner,** *Electric Power Research Institute*
L. J. Lommers,** *AREVA NP, Inc.*
P. P. Lowry, *Pacific Northwest National Laboratory*
Y. Makihara, *International Atomic Energy Agency*
P. M. Mills, *Idaho National Laboratory*
C. L. Reid, *Bechtel National, Inc.*
S. D. Rubin,** *U.S. Nuclear Regulatory Commission*
F. Shahrokhi,** *AREVA NP, Inc.*
K. R. Schultz, *General Atomics*
D. J. Spellman,** *Oak Ridge National Laboratory*
E. G. Wallace,** *Pebble Bed Modular Reactors (Pty), Ltd.*
Ben Holtzman, *ANS, Graduate Department, University of Illinois*

**Primary contributors participating since August 2004, which is the full project duration.

Other contributors included the following:

S. J. Ball, *Oak Ridge National Laboratory*
R. Black, *U.S. Department of Energy, Office of Nuclear Energy*
M. V. Frank, *Safety Factor Associates, Inc.*
N. P. Kadambi, *U.S. Nuclear Regulatory Commission*
N. Tricot, *International Atomic Energy Agency*

The ANS-28 Subcommittee acknowledges support from the U.S. Department of Energy (DOE) through Richard Black [DOE (NE-3)] and Donald Spellman [Oak Ridge National Laboratory (ORNL)]. Without their help, this 6-year effort would have been significantly more difficult to complete. Other contributors include AREVA NP, Inc., who contributed to the development of the MHR uncertainty consequences curves; General Atomics, who provided historical modular high-temperature gas reactor/HTGR licensing interpretations; and Pebble Bed Modular Reactors (Pty), Ltd., who provided the extensive basis behind its current license application, especially licensing application of DID principles. We are also indebted to the U.S. Nuclear Regulatory Commission for introducing risk-informed guidance, existing regulatory interpretations, and extensive unacknowledged staff review assistance. Finally, all contributor companies and their employees who so generously donated their time include CORE, Inc.; AREVA NP, Inc.; Westinghouse; UT-Battelle/ORNL; Battelle Energy Alliance and Oak Ridge contractors to DOE; the Electric Power Research Institute; Bechtel; Exelon Nuclear; and General Atomics.

The Nuclear Facility Standards Committee (NFSC) had the following membership at the time of its approval of this standard:

C. A. Mazzola (Chair), *Shaw Environmental & Infrastructure, Inc.*
R. M. Ruby (Vice Chair), *Constellation Energy*

J. A. August, *CORE, Inc.*
W. H. Bell, *South Carolina Electric & Gas Company*
J. R. Brault, *Shaw MOX Project*
C. K. Brown, *Southern Nuclear Operating Company*
K. R. Bryson, *Individual*
C. E. Carpenter, *U.S. Nuclear Regulatory Commission*
D. R. Eggett, *Automated Engineering Services Corporation*
R. W. Englehart, *Individual*
P. K. Guha, *U.S. Department of Energy*
P. S. Hastings, *Duke Energy Company (NuStart Liaison)*
R. A. Hill, *ERIN Engineering and Research, Inc.*
N. P. Kadambi, *Individual*
M. A. Linn, *Oak Ridge National Laboratory*
E. M. Lloyd, *Exitech Corporation*
S. A. Lott, *Los Alamos National Laboratory*
R. H. McFetridge, *Westinghouse Electric Company, LLC*
T. K. Meneely, *Westinghouse Electric Company, LLC*
C. H. Moseley, *ASME NQA Liaison*
D. G. Newton, *AREVA NP*
W. B. Reuland, *Individual*
J. C. Saldarini, *Bechtel Power Corporation*
D. J. Spellman, *Oak Ridge National Laboratory*
S. L. Stamm, *Shaw Nuclear Services*
J. D. Stevenson, *Individual*
J. A. Wehrenberg, *Southern Company Services*
M. J. Wright, *Entergy Operations, Inc.*
L. M. Zull, *Defense Nuclear Facilities Safety Board*

NFSC Liaison:

G. Hutcherson, *Institute of Nuclear Power Operations*
J. Riley, *Nuclear Energy Institute*

Contents	Section	Page
1	Introduction	1
1.1	Purpose	1
1.2	Scope	1
1.3	Applicability	2
1.4	Design process	2
1.5	Safety process description	3
2	Acronyms and definitions	5
2.1	List of acronyms	5
2.2	Definitions	6
3	Develop safety design criteria	14
3.1	Introduction to safety criteria development	14
3.2	Establish event categories and F-C curve	15
3.2.1	TLSC selection guidance	16
3.2.2	F-C curve and event region guidance	17
3.2.3	Cumulative risk	20
3.2.4	DID requirement	20
3.3	Establish safety functions	22
3.3.1	SSC categorization	22
3.3.2	MHR safety functions	24
3.4	Establish TLDC	29
3.4.1	Control radionuclides in fuel particles	29
3.4.2	Remove core heat	30
3.4.3	Control heat generation	31
3.4.4	Control chemical attack	31
3.4.5	Maintain core geometry	32
3.4.6	Maintain reactor building geometry	33
4	Perform and apply PRA	33
4.1	Establish PRA requirements	34
4.2	Perform PRA	37
4.3	Apply the PRA	39
4.3.1	Develop LBEs	39
4.3.2	Identify event families	40
4.3.3	Select LBEs in AOO region	41
4.3.4	Select LBEs in DBE region	41
4.3.5	Select LBEs in BDBE region	41
4.3.6	Plot LBEs on F-C curve	41
4.4	Evaluate cumulative risk	43
5	Determine DBA and classify SSCs	43
5.1	Overview	43
5.2	Identify SSC LBE accident roles	44
5.3	Classify SSCs	45
5.3.1	Safety classification for DBE mitigation	46
5.3.2	Safety classification for high-consequence BDBE prevention	48
5.3.3	Safety classification considerations	49
5.4	Determine DBAs	50
5.5	Confirm TLDC	53
5.6	Specify special treatment requirements	53

6	Perform deterministic safety analyses	54
6.1	Purpose of deterministic safety analyses	54
6.2	Safety analysis criteria	54
6.2.1	Deterministic safety analysis criteria	54
6.2.2	Deterministic analysis supporting criteria	55
6.3	Basic elements of MHR safety analyses	56
6.3.1	Initial conditions	56
6.3.2	System response	57
6.3.3	Radionuclide source term	57
6.3.4	Radionuclide transport within and outside the HPB	58
6.3.5	Consequence/dose assessment	58
6.3.6	Supporting analyses	58
6.4	MHR characteristics important to deterministic safety analyses	59
6.4.1	Particle fuel characteristics and safety analyses	59
6.4.2	Core structure characteristics and safety analyses	60
6.4.3	Negative temperature reactivity characteristics and safety analyses	60
6.4.4	Helium primary coolant characteristics and safety analyses	60
6.4.5	Thermal inertia characteristics and safety analyses	61
6.4.6	Passive decay heat removal characteristics and safety analyses	61
6.5	Deterministic safety analysis categories and analysis requirements	62
6.5.1	Normal operation and AOOs	62
6.5.2	Reactivity events	62
6.5.3	Depressurization events	63
6.5.4	Loss-of-forced-cooling events	64
6.5.5	Chemical attack events	65
6.5.6	Nonreactor events in plants	66
6.6	Treatment of uncertainties in MHR deterministic safety analyses	68
6.6.1	Level of conservatism	69
6.6.2	Major deterministic safety analysis uncertainties	69
6.6.3	Reduction of deterministic safety analysis uncertainties	70
6.6.4	Addressing uncertainties in deterministic safety analyses	70
6.7	Qualification of deterministic safety analysis methods	73
6.7.1	Identification of required model capabilities	73
6.7.2	Method evaluation and qualification	73
7	Evaluate DID	74
7.1	Overview	74
7.2	Plant capability DID	77
7.3	Programmatic DID	79
7.4	Risk-informed evaluation of DID	80
7.5	Implementation of DID process	81
8	Special treatments	84
8.1	Background	84
8.1.1	Purpose	84
8.1.2	Safety functions	85
8.1.3	Basis	86
8.1.4	Capability and reliability	87
8.1.5	Selection flowchart	88
8.2	Classify safety-related SSCs	90
8.2.1	Identify safety categories	91
8.2.2	Classify SSC safety functions	94

8.2.3	Classify SSC subassemblies	96
8.2.4	Identify critical characteristics	97
8.3	Specify special treatments	98
8.3.1	Scope	98
8.3.2	Requirements	100
8.3.3	Partition: SSCs and functions	103
8.3.4	Critical characteristics	105
8.3.5	Specify special treatments	106
8.3.6	Dedicate SSCs	107
8.3.7	Quality versus reliability	111
8.3.8	Historical differences	113
8.3.9	Defense-in-depth	114
8.3.10	Other industry use	115
8.4	Conclusion	115
9	References	116

Tables

Table 1	Required MHR safety design elements	14
Table 2	Summary of requirements for F-C curve	15
Table 3	Summary of requirements for TLSC selection	16
Table 4	Summary of requirements for F-C curve and event region	18
Table 5	Summary of requirements for BDBEs	19
Table 6	Summary of requirements for cumulative risk determination ..	20
Table 7	Summary of requirements for DID	21
Table 8	Summary of requirements for establishing MHR safety functions	22
Table 9	Summary of requirements for SSC categorization	24
Table 10	Summary of requirements for control of radionuclides in fuel particles	25
Table 11	Summary of requirements for removal of core heat	26
Table 12	Summary of requirements for control of heat generation	26
Table 13	Summary of requirements for control of chemical attack	27
Table 14	Summary of requirements for maintaining core geometry	28
Table 15	Summary of requirements for maintaining reactor building geometry	28
Table 16	Summary of requirements for control of radionuclides in fuel particles	29
Table 17	Summary of requirements for removal of core heat	30
Table 18	Summary of requirements for control of heat generation	31
Table 19	Summary of requirements for control of chemical attack	32
Table 20	Summary of requirements for maintaining core geometry	32
Table 21	Summary of requirements for maintaining reactor building geometry	33
Table 22	Summary of requirements for establishing the PRA	35
Table 23	Summary of requirements for performing PRA	38
Table 24	Summary of requirements for applying the PRA	42
Table 25	Summary of requirements for evaluating cumulative risk	43
Table 26	Summary of requirements for identifying SSC LBE accident roles	45
Table 27	Evaluation of SSCs for core heat removal capability on DBEs ..	47
Table 28	Evaluation of SSCs for core heat generation control on DBEs ..	48
Table 29	Summary of requirements for classifying SSCs	49
Table 30	Selection of deterministic DBAs for a set of MHR DBEs	51

Table 31	Summary of requirements to determine DBAs	52
Table 32	Summary of requirements for confirming TLDC	53
Table 33	Summary of requirements for specifying special treatment requirements	53
Table 34	Summary of requirements for safety analysis criteria	56
Table 35	Summary of requirements for deterministic safety analysis elements	58
Table 36	Summary of requirements for safety analysis regarding MHR characteristics	61
Table 37	Summary of safety analysis requirements for MHR accident categories	66
Table 38	Summary of requirements for safety analysis uncertainties ..	72
Table 39	Summary of requirements for safety analysis method qualification	74
Table 40	Elements of plant capability DID	78
Table 41	Summary of requirements for plant capability DID	79
Table 42	Elements of programmatic DID	79
Table 43	Summary of requirements for programmatic DID	80
Table 44	Elements of risk-informed evaluation DID	80
Table 45	Summary of requirements for risk-informed evaluation DID ..	81
Table 46	MHR/DID underlying principles	82
Table 47	Criteria for application of MHR DID principles	82
Table 48	Summary of requirements for implementation of DID process	83
Table 49	Summary of requirements for the purpose of special treatments	85
Table 50	Summary of requirements for safety functions	85
Table 51	Summary of requirements for treatment basis	86
Table 52	Safety-related NSRWST SSCs	87
Table 53	Summary of requirements for capability and reliability	88
Table 54	Summary of requirements for selection flowchart	90
Table 55	Summary of requirements for classifying safety-related SSCs	90
Table 56	Summary of requirements for identifying safety categories ...	91
Table 57	Summary of requirements for safety-related	93
Table 58	Summary of requirements for NSR	93
Table 59	Summary of requirements for NSRWST	94
Table 60	Summary of requirements for NSRWST basis	94
Table 61	Summary of requirements for classifying SSC safety functions	95
Table 62	Summary of requirements for classifying SSC subassemblies	97
Table 63	Summary of requirements for critical characteristics	98
Table 64	Summary of requirements for special treatment scope	100
Table 65	Summary of special treatment requirements	102
Table 66	Summary of requirements for partition: systems, SSCs, and functions	105
Table 67	Summary of requirements for critical characteristics	106
Table 68	Summary of requirements for specifying special treatment requirements	107
Table 69	Summary of requirements for reviewing fit, form, and function	108
Table 70	Summary of requirements for determining SSC special treatment strategies	109

Table 71	Summary of requirements for identifying special treatments	110
Table 72	Summary of requirements for dedication	111
Table 73	Summary of requirements for quality versus reliability	112
Table 74	Summary of requirements for historical management	114
Table 75	Summary of requirements for DID	115
Table 76	Summary of requirements for special treatment conclusion ..	115

Figures

Figure 1	Engineering safety design relationship	3
Figure 2	MHR safety design process overview	4
Figure 3	Illustrative F-C curve based on TLRC	17
Figure 4	MHR safety functions	23
Figure 5	Reliability and capability SSC roles preventing and mitigating LBEs	45
Figure 6	F-C curve showing DBA regions	51
Figure 7	MHR DID elements	75
Figure 8	Logic for implementing evaluation of DID	76
Figure 9	Barriers to radionuclide transport included in plant capability DID	77
Figure 10	Elements of safety design incorporated into plant capability DID	78
Figure 11	SSC special treatment selection processes	89

Nuclear Safety Design Process for Modular Helium-Cooled Reactor Plants

1 Introduction

1.1 Purpose

The purpose of this standard¹⁾ is to define the process for specifying criteria to assure that modular helium-cooled reactor (MHR) nuclear power plants²⁾ are designed so that they can be constructed and operated safely without undue risk to public health and safety. This purpose is achieved through the identification of applicable safety requirements from the national nuclear regulator, industrial codes and standards, and other published guidance and professional engineering practices. The MHR plant designer³⁾ is responsible for conformance to the criteria defined in this standard and supporting the design bases and expected operational characteristics by design analyses, experimental models, conformance with applicable standards, and comparisons with accepted designs or experience gained from similar designs.

The designer may consider additional or alternate requirements to accommodate specific site/design characteristics not covered (or referenced) by this standard or related document guidance. For licensing in the United States, this standard presumes that license applicants will meet all applicable U.S. Nuclear Regulatory Commission (NRC) licensing requirements.

1.2 Scope

This standard applies to the safety design process for plants. This standard provides a process for establishing top-level safety criteria (TLSC); safety functions; top-level design criteria (TLDC); licensing-basis events (LBEs); design-basis accidents (DBAs); safety classification of systems, structures, and components

(SSCs); safety analyses; defense-in-depth (DID); and adequate assurance of special treatment requirements for safety-related SSCs throughout the operating life of the plant. This standard does not provide detailed guidance for design; other existing standards cover that.

Plants maintain radioactive releases within public health and safety requirements by passive SSCs and/or inherent characteristics by design. They rely on intrinsic physical characteristics and specific design requirements to do this. While it is beyond the scope of this standard to explain how, the following description of MHR design characteristics provides the basis for this attribute claim. Plants have one or more standard helium-cooled reactor modules, where each module has the following fundamental design characteristics:

- helium primary coolant;
- graphite moderator;
- high integrity, ceramic coated particle nuclear fuel enclosed in a graphite matrix;
- passive decay heat removal capability under extreme undercooling accident conditions;
- defined core geometry that ensures adequate core cooling maintained under all conditions;
- core contained within a metallic reactor pressure vessel (RPV);
- RPV contained within a robust building structure;
- negative temperature coefficient of reactivity.

MHR modules consist of standard nuclear reactor configurations coupled to a direct or indirect power conversion system and/or a process heat utilization system. MHR modules allow replication to produce the required plant output. An MHR direct power conversion system

¹⁾ The current standard, ANSI/ANS-53.1-2011, will hereinafter be referred to as “this standard.”

²⁾ Modular helium-cooled reactor nuclear power plant(s) will hereinafter be referred to as “plant(s).”

³⁾ MHR plant designer(s) will hereinafter be referred to as “designer(s).”

employs a gas turbine in the primary coolant system to convert the thermal energy carried in the primary coolant into electrical energy. An MHR indirect cycle employs an intermediate heat exchanger to transfer thermal energy from the primary coolant to a secondary coolant/working fluid used for power generation. An MHR process heat utilization system employs the thermal energy produced in the reactor core as the energy input to a process for production, such as hydrogen. An MHR module providing process heat may be configured to also cogenerate electricity using either a direct or an indirect cycle.

1.3 Applicability

This standard is applicable to the design of plants defined for commercial, developmental research, and advanced reactor applications. This standard addresses safety licensing and development of design criteria for construction, operations, maintenance, and testing.

1.4 Design process

Section 1.4 discusses the overall design process for reference.

All designs start with the definition of top-level requirements. The owner, operator, regulators, vendors, users, and government parties—those vested with an interest in the project—determine the top-level requirements. Regulatory and government requirements place constraints on nuclear projects that reflect the public's interests. Nuclear safety is at the top of all requirements with nuclear projects. Nonnuclear requirements address output, fuel, siting, economics, schedule, availability, operations and maintenance (O&M), investment, and environmental goals. Once the owner has satisfactorily established the top-level requirements, the design process begins. Selection of appropriate technology is a first step; detailed facility design follows.

For decades, conventional power plant projects have begun essentially the same way—following proven practices and procedures. The owner selects the basic design features (i.e., heat source and power conversion systems); then, conventional power plant designers select process layouts, operational modes, and building arrangements that fulfill production requirements. Once selected, these features allow further design development to add other re-

quirements that assure adequate availability, reliability, and investment protection.

In choosing a nuclear heat supply system, the nuclear plant designer includes special nuclear safety considerations to control radionuclide releases to protect the off-site public and on-site workers from radioactive materials and prevent and mitigate nuclear accidents. In addition, selecting a nuclear heat supply system requires special siting that assures the ability to execute an emergency plan should a serious accident ever occur. The site choice and emergency planning capability are part of the nuclear plant project's DID strategy. The design process will also incorporate probabilistic risk assessment (PRA) techniques, developing the design as part of the strategy to assure adequate protection of the public and workers.

This standard uses a risk-informed, performance-based (RI-PB) approach in the design processes. The use of PRA further refines decisions and contributes to the traditional deterministic selection of DBAs beyond single-failure analysis. These DBAs confirm that the necessary functionality, safety classifications, and special treatments will be applied to SSCs and other plant programmatic features. A foundation of deterministic requirements, decisions, and evaluations supports this process.

Selecting designs requires assumptions, and uncertainties may exist. These include SSC functionality and performance requirements. For a relatively new technology like the MHR, the operating experience available may be limited relative to demonstrating the ability to achieve design and safety objectives. Therefore, development of technology may be required to address questions about SSC performance or uncertainties in phenomena, validate SSC assumptions, or answer questions about plant operating conditions. During the design life cycle, designer insights set a foundation in the highly iterative design activities. Following startup, though less iterative, designs still change as new information is learned, equipment and materials change, and other requirements become established. Figure 1 illustrates design development and its relationship to safety.

The actual step of performing plant design occurs after setting the TLDC but before evaluating the initial plant design with PRA. It is not the intent of this standard to develop

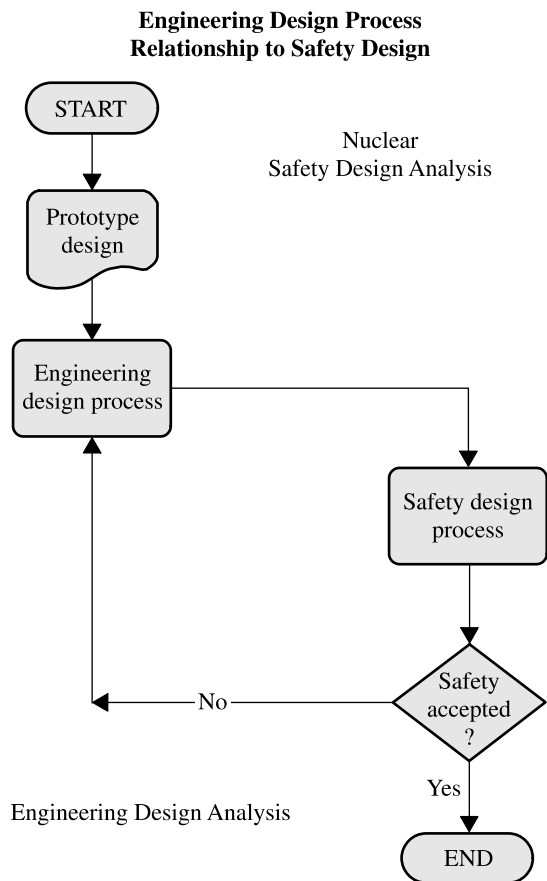


Figure 1 – Engineering safety design relationship

that process fully; the plant design process is well defined elsewhere. Failure to develop an effective design will result in complexities, difficulty meeting the TLDC, and potentially additional mitigative systems. A concern in nuclear design is to manage the interfaces between systems to minimize interactions, maintain the design's analyses, and avoid the perturbation effects of nonsafety equipment on higher-level encompassing systems.

Designers provide design interfaces between SSCs of different safety classes to ensure that any failure in a system classified in a lower class will not propagate to a system classified in a higher class. This principle of isolation of lower-tiered SSC effects requires expert insights into safety design and SSC technology, in addition to PRA, to develop.

The design basis specifies operational states and conforms to DBAs that determine the nec-

essary capabilities of the plant. The plant meets these requirements to conform to the TLSC radiological protection requirements. The design basis includes specifications for normal operation; plant states created by internal events; the safety classification; important assumptions; and in some cases, the particular methods of analysis. Conservative design measures and sound engineering practices are applied in the design bases for the areas under the frequency-consequence (F-C) curve. These are normal operation, anticipated operational occurrences (AOOs), DBAs, and beyond-design-basis accidents. This provides a high degree of assurance that no significant damage will occur to the reactor core and radiation doses will remain within prescribed limits and be as low as is reasonably achievable.

In addition to the design basis, the performance of the plant in specified accidents beyond the design basis, including selected severe accidents, is also addressed in the design. The assumptions and methods used for these evaluations may be on a best-estimate basis.

In the design of the plant, it is recognized that challenges to all levels of DID may occur, and design measures are provided to ensure that the necessary safety functions are accomplished and safety objectives can be met. These challenges stem from postulated initiating events, which are selected on the basis of deterministic, probabilistic, or risk-informed techniques (or a combination). Independent events, each having a low probability, are normally not anticipated in the design to occur simultaneously. An analysis of postulated initiating events is made to establish all those internal events that may affect plant safety. These events may include equipment failures or misoperation as a result of operator error.

1.5 Safety process description

The process defined in this standard for ensuring the nuclear safety of plants is based on identifying plant events having nuclear safety risk significance and analysis of the events for compliance with regulatory requirements. The process uses PRA to identify high-risk events and deterministic safety analysis methods for plant safety evaluation. As such, the process identified is a RI-PB approach.

Since the introduction of PRA techniques to light water reactors (LWRs) in 1975 [1],⁴⁾ these methodologies have evolved into a definitive, well-understood process. The use of PRA to define plant events important to nuclear safety provides a high degree of assurance that the most limiting events are identified. Once iden-

tified, the process in this standard evaluates events using both risk-informed and traditional deterministic methods.

The overall safety design process follows a flow-chart similar in nature to that identified in Fig. 2. This standard describes each process step in detail

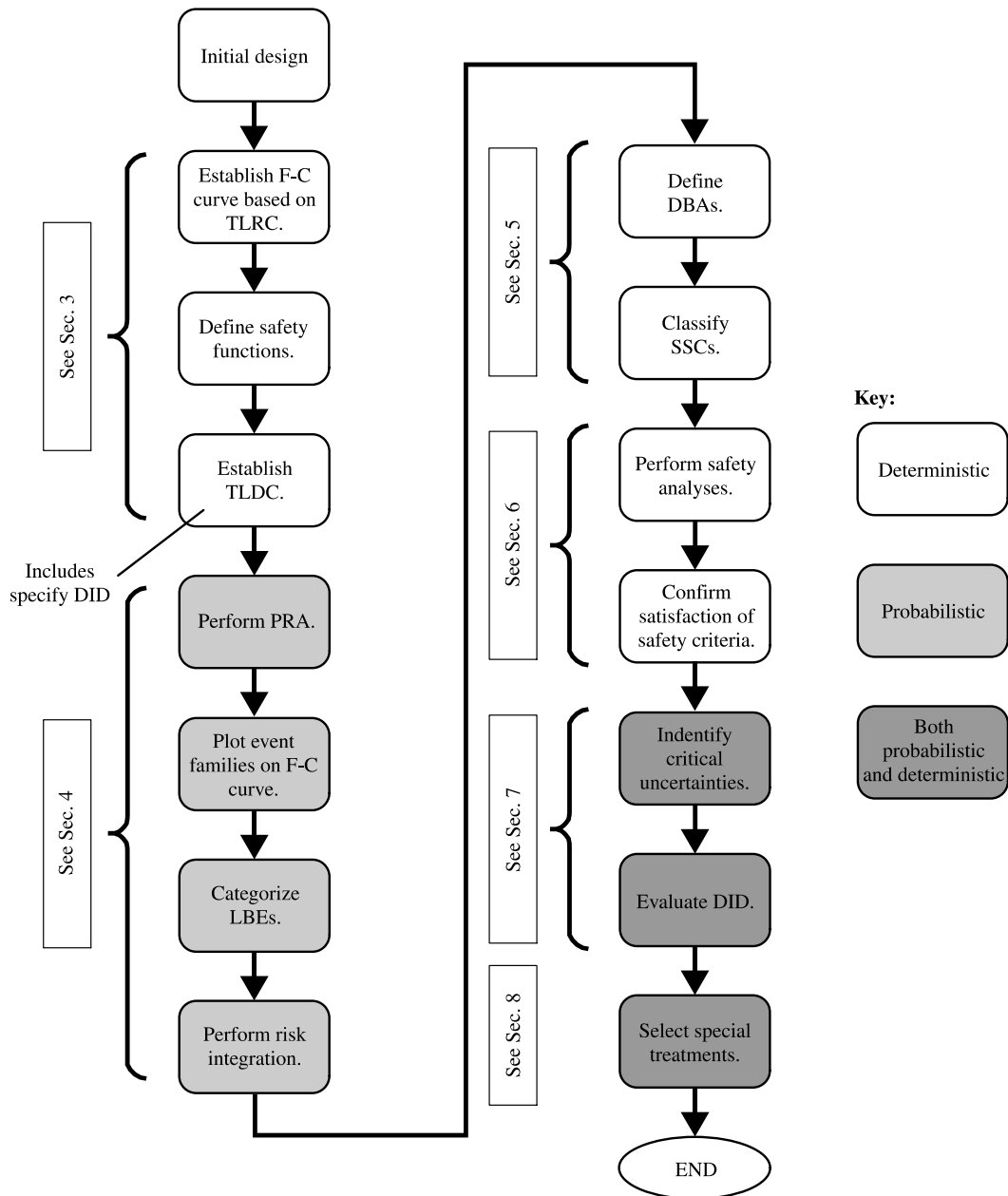


Figure 2 – MHR safety design process overview

⁴⁾ Numbers in brackets refer to corresponding numbers in Sec. 9, “References.”

in subsequent sections, as indicated in this flow-chart. The applicable section number containing the detail for each process step is as identified in Fig. 2. (Note that shading delineates probabilistic and deterministic safety design activities, traditionally interpreted.)

The MHR safety design process starts with an initial conceptual design. Following initial design definition, Sec. 3 identifies the first step of establishing the safety design criteria and an F-C curve from the TLSC limits. This section then describes the process for defining plant safety functions and establishing TLDC to ensure that equipment that is important to reactor safety will perform the intended safety functions when called upon.

Section 4 outlines performing the PRA, the next process step. Section 4 also describes plotting event families on the F-C curve, categorizing the LBEs, and performing an analysis of overall risk by summing each event's risk and accounting for frequency and consequence uncertainties.

Section 5 provides a process for using LBEs to define DBAs that enables SSC classification and the selection of special treatments using this classification. Section 6 then describes performing the safety analyses that verify satisfying the TLDC. Section 7 covers the identification of critical uncertainties and evaluation of DID. These activities qualify the analysis, adding depth to the numerical analysis outputs from the PRA. Section 8, the final activity, selects special treatments to translate the standard into performance requirements.

Although idealized in the linear format presented, like all complex design activities, the MHR safety design process iterates as the plant design evolves. At the end of the process, safety analyses and DID acceptance confirm steps taken for application of special treatments.

2 Acronyms and definitions

2.1 List of acronyms

ANS: American Nuclear Society

AOO: anticipated operational occurrence

ASME: American Society of Mechanical Engineers

ATWS: anticipated transient without scram

BDBE: beyond-design-basis event

CCS: core conditioning system

CFR: *Code of Federal Regulations*

CGI: commercial-grade item

DBA: design-basis accident

DBE: design-basis event

DCD: design control document

DID: defense-in-depth

EAB: exclusion area boundary

EPS: equipment protection system

F-C: frequency-consequence

FMEA: failure mode and effects analysis

GDC: general design criteria

HPB: helium pressure boundary

HTGR: high-temperature gas-cooled reactor

ITAAC: inspections, tests, analyses, and acceptance criteria

LBE: licensing-basis event

LWR: light water reactor

MEL: master equipment list

MHR: modular helium-cooled reactor

MPS: main power system

NRC: U.S. Nuclear Regulatory Commission

NSR: non-safety-related

NSRWST: non-safety-related with special treatment

O&M: operations and maintenance

PAG: protective action guideline

PCU: power conversion unit

P&M: prevention and mitigation

PRA: probabilistic risk assessment

QAP: quality assurance program

QHO: quantitative health objective

RAP: reliability assurance program

RCCS: reactor cavity cooling system

RCS: reactivity control system

RI-PB: risk-informed, performance-based

RPS: reactor protection system

RPV: reactor pressure vessel

RTNSS: regulatory treatment of non-safety systems

SAR: safety analysis report

SAS: small absorber spheres

SBS: start-up blower system

SSCs: systems, structures, and components

SSE: safe shutdown earthquake

TEDE: total effective dose equivalent

TLDC: top-level design criteria

TLRC: top-level regulatory criteria

TLSC: top-level safety criteria

TRISO: tri-isotopic

2.2 Definitions

acceptance criteria: Actionable, measureable guidance for evaluating tests, inspections, and performance.

accident sequence: One of the set of accident sequences, defined at the functional or systematic level, that when rank-ordered by decreasing frequency aggregate to a specified percentage of the release category core damage frequency or that individually contribute more than a specified percentage of core damage to the release category frequency. The aggregate percentage is 95%, and the individual percentage is 1%. Accident sequence significance can be measured relative to each separate release category frequency (an accident sequence may be significant to one release category and not necessarily significant to others).

accident family: The event family for an event sequence defined as an accident (see “event sequence”).

anticipated operational occurrence (AOO): LBEs and conditions of plant operation that are expected to occur one or more times during the life of the plant. Event sequences from the PRA are classified as AOOs when their expected frequency of occurrence exceeds 1×10^{-2} events/plant-year ($1\text{E}-02$ events/plant-year).

availability: A plant or SSC attribute defined as the probability or fraction of time that the SSC is capable of performing its function at the time of demand.

beyond-design-basis event (BDBE): LBEs that are not expected to occur during the lifetime of a large fleet of nuclear power plants but are considered to assure that the risk to the pub-

lic from low-frequency events is acceptable. Event sequences from the PRA are classified as BDBEs when their expected frequency of occurrence is between 5×10^{-7} events/plant-year ($5\text{E}-07$ events/plant-year) and 1×10^{-4} events/plant-year ($1\text{E}-04$ events/plant-year).

capability: SSC ability to maintain requirements to meet top-level regulatory criteria (TLRC) and quantitative health objectives (QHOs).

circulating activity: Activity from radioactive isotope fission product species circulating in the primary coolant helium, such as noble gases and volatile iodine. (In a depressurization event like offset rupture, activity in the helium primary coolant is more easily released and dispersed.)

commercial-grade supplier performance: Performance to commercial-grade contract specifications not nuclear safety quality specification.

common-cause events: An event that adversely impacts the performance of two or more components during a short time interval as a result of a single shared cause.

conduction cooldown events, pressurized or depressurized: An event involving a loss of forced circulation heat removal in which core heat removal is accomplished via thermal conduction, convection, and radiation heat transfer from the reactor core to the RPV walls and thermal radiation and convection heat transfer to the reactor cavity and/or reactor cavity cooling system (RCCS). Conduction cooldown may occur with the reactor pressurized or depressurized and with or without operation of the RCCS.

confinement: A safety function that involves the retention of radioactive material, or mitigation of release, using one or more radionuclide transport barriers.

consequence assessment: Evaluation of the radiological consequences of an accident. In this standard, consequences are assessed in terms of integrated radiological dose exposure to an individual (e.g., the public) at the exclusion area boundary (EAB).

core damage: Any physical disruption of the nuclear core including fuel, fission products, and containing geometry consisting of cladding, structure, and flow alignment that could release significant amounts of radioactivity from fission products by being undercooled or overreactive.

critical characteristics: Important design, material, and performance attributes of an item that, once verified, will provide reasonable assurance that the item will perform its intended safety function.

critical SSC: SSC, with critical characteristics, that performs critical safety functions, failure of which causes significant safety risks.

defense-in-depth (DID): An established safety philosophy in which multiple lines of defense and safety margins are applied to the design, operation, and regulation of plants to assure that public health and safety are adequately protected. This standard focuses on those aspects of DID of interest in the design of MHRs that include both deterministic and probabilistic elements. As used in this standard, plant capability DID is reflected in the reactor design, programmatic DID is in the requirements and regulations, and risk-informed evaluation of DID is the process of evaluating the adequacy of DID measures. Note that the NRC statement of DID is a safety philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs.⁵⁾ The NRC's safety philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the safety philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility.

depressurization event: An event that results in loss of helium primary coolant pressure to the surrounding building atmosphere resulting from a breach in the helium pressure boundary (HPB).

design: The process and result of developing a concept, detailed plans, supporting calculations, and specifications for a facility and its parts that describe the facility, using an engineering process. The description may include specifications, engineering drawings, reports

demonstrating compliance with regulatory requirements, and other relevant documentation.

design bases: Information that identifies the specific functions to be performed by facility SSCs and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (a) restraints derived from generally accepted "state-of-the-art" practices for achieving functional goals or (b) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which the SSC is relied upon to function.

design-basis functions: Functions performed by SSCs that are (a) required by or otherwise necessary to comply with regulations, license conditions, orders, or technical specifications or (b) credited in licensee safety analyses to meet regulatory requirements.

design basis: All the related specifications and detailed plans that support calculations for a facility from an initial design concept and its parts extending through its fulfillment as a detailed design constructed as a plant. The range of conditions and events explicitly taken into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems.

design-basis accident (DBA): Event sequences deterministically selected for the purpose of performing conservative deterministic safety analyses to demonstrate that DBA dose requirements can be achieved by assuming that only safety-related SSCs perform as required.

design-basis event (DBE): Those LBEs that are not expected to occur during the lifetime of a single plant but may be encountered during the lifetime of a population of plants. Event sequences from the PRA are classified as DBEs when their expected frequency of occurrence is between 1×10^{-4} events/plant-year (1E-04 events/plant-year) and 1×10^{-2} events/plant-year (1E-02 events/plant-year).

⁵⁾ The NRC's statement of DID derives from Speech No. S-04-009, presented at the 3rd Annual Homeland Security Summit Session, "The Best-Laid Plans: A Case Study in Preparedness Planning; The Very Best-Laid Plans (the NRC's Defense-in Depth Philosophy)," Remarks of Nils J. Diaz, Chairman, U.S. Nuclear Regulatory Commission, June 3, 2004, "Preparedness and Defense-in-Depth": <http://pbadupws.nrc.gov/docs/ML0415/ML041550865.pdf> (page last reviewed/updated March 29, 2012).

design margins: Additional performance capability above required design parameters that system design specifies to compensate for uncertainties at any design stage or to provide additional capacity or reliability.

design life: Plant life estimation used for design aging calculations to support the licensed plant life.

deterministic: Based on an exact model (in contrast with stochastic: based on a probabilistic model).

deterministic safety analysis: Engineering analysis of the plant response using computer models, calculations, and data that predict the transient response of the plant to an event sequence, mechanistic source term, and radiological consequences using validated models and data.

diversity: Use of different design principles in functionally redundant components in order to reduce susceptibility to common-cause failures.

emergency planning zone: An area surrounding a plant with a well-defined boundary for which emergency planning is provided including provisions for protective actions such as evacuation and sheltering.

end state: A stable plant state configuration from which conditions will not deteriorate without a new, separate event; the plant state at the end of an event sequence modeled in a PRA. Examples of end states include successful termination and release of radioactive material in a specified release category.

environmental qualification: Testing and analytical demonstration that equipment is suitable for its intended purpose and environment.

event: A condition that deviates from normal operation, i.e., an initiating occurrence or an initiating occurrence plus single failure or coincident occurrence combination. See also “event sequence family.”

event family: See “event sequence family.”

event sequence: A specific event tree pathway in a PRA model that begins with an initiating event in a specified plant operating state and describes the successful and unsuccessful responses of the SSCs that perform safety functions in response to the initiating event and ends in a well-defined end state.

event sequence analysis: An analysis that is performed as part of a PRA to determine the possible plant responses to an initiating event by constructing event trees, defining event sequences and end states, determining the success criteria for each event tree top event, and defining the end states.

event sequence family: A group of event sequences with similar initiating events, safety function responses, and end states. As used in this standard, many LBEs are defined by organizing individual event sequences from the PRA into event sequence families to avoid having to process too many event sequences and to prevent the subdivision of event sequences with similar consequences for application of the acceptable frequencies and consequences expressed by the TLSC curve. As used, the term “event” commonly refers to an event sequence family. When event sequences are combined into event sequence families, the frequency classification is based on the total frequency of the family.

event tree: A logic diagram that begins with an initiating event and progresses through a series of branches that represent the possible system or operator responses including successful and unsuccessful performance of safety functions in response to the initiating event and termination of each branch in a well-defined end state.

external event (also referred to as external plant hazard event): An event originating from an external plant hazard outside a plant that causes safety system failures, operator errors, or both, that in turn may lead to an initiating event, an event sequence, and a radioactive material release source term. Events such as earthquakes, tornadoes, and floods from sources outside the plant and fires from sources outside the plant are considered external events (see also “internal event” and “internal plant hazard”). Fires inside the plant are classified as internal plant hazard events. By convention, loss of off-site power not caused by another external event is considered to be an internal event. Note that external events may or may not involve an external event induced initiating event. (For example, an external event may occur without damage to the plant with continued plant operation.)

external plant hazard: A hazard located outside the plant that can cause an external event.

Examples of external hazards include earthquake faults, chemical or process plants, and airports. See “external event” and “internal plant hazard.”

frequency-consequence (F-C) curve: A curve of frequency based on consequences that defines operating limits for facility events based on the frequency and severity of consequences.

failure: The inability to perform an action or function at the proper time or performance of an action at an improper time. An alternate is a change from an operable state meeting specified requirements to an inoperable state that does not meet specified requirements.

failure mechanism: Any processes that result in failure modes, including chemical, electrical, mechanical, physical, thermal, and human error; a failure mode and its associated cause.

failure mode: A specific functional manifestation of a failure (i.e., the means by which an observer can determine that a failure has occurred) by precluding the successful operation of a piece of equipment, a component, or a system (e.g., fails to start, fails to run, leaks).

failure mode and effects analysis (FMEA): A procedure for analysis of potential failure modes within a system for classification by severity or determination of the failure’s effect upon the system. Widely used in the manufacturing industries in various phases of the product life cycle. Failure causes are any errors or defects in process, design, or item, especially ones that affect the customer, and can be potential or actual. Effects analysis refers to studying the consequences of those failures.

frequency mean value: The mean of an uncertainty distribution that expresses uncertainty in the estimate of an event frequency.

fuel failure: The release of fission products from the fuel kernel by an MHR tri-isotopic (TRISO) fuel coating particle failure mechanism.

full-scope probabilistic risk assessment: See “PRA, full scope.”

function: A design specification for what an SSC is expected to accomplish in order to serve a plant operation, maintenance, or safety purpose.

functional analysis: Analysis of functions provided by SSCs. For safety functions, the analysis

of the effects of safety-related SSCs on accident analysis.

functional performance requirements: A qualitative or quantitative determination of acceptable operability by observation of system or component behavior during operation.

functional requirements: Functional description of requirements that the designs provide. Expressed functionally, designers can translate system requirements into hardware designs.

graphite oxidation: An exothermic chemical oxidation reaction of graphite with oxygen or endothermic reaction of graphite with water.

helium pressure boundary (HPB): The pressure boundary for the primary helium coolant including the RPV, piping, vessels, valves, and heat exchangers required to maintain primary helium pressure and act as a barrier to fission product releases to the reactor building.

heat utilization system: The ultimate heat load that uses the thermal energy (heat output) from a reactor for energy production or process purposes.

hidden failure: Failure of a component or system that does not become evident until the affected component or system is called upon to function.

high-temperature gas-cooled reactor (HTGR): A reactor with graphite moderator, helium coolant, and coated particle fuel with core outlet temperatures normally above 750°C. HTGRs with passive core heat removal and reactivity control capabilities in steel RPVs and of modular design are referred to as modular HTGRs or MHRs.

initiating event: Any event, observed or postulated, either internal or external to the plant, that perturbs the steady-state operation of the plant or steady-state maintenance of the plant safety functions, thereby initiating an abnormal event such as transient or HPB breach within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could potentially lead to a significant release of radioactive material. Internal events, internal plant hazards, or external plant hazards, defined for specific plant operating states, can cause initiating events. In a PRA, initiating events that occur in specified plant operating states are

used as a starting point to define event sequences and LBEs. Used for analytical purposes, the (postulated) event that initiates an event sequence culminating in an analytical outcome for safety analysis.

internal event: An initiating event resulting from equipment failure, operator action, or other error internal to the plant. These events include equipment misoperation.

internal plant hazard: A hazard located inside the plant that could be the source of an internal plant hazard event. Examples of internal plant hazards are rotating machinery, high-energy piping, large-volume water tanks, and sources of combustible material.

internal plant hazard event: An event originating from an internal plant hazard external to modeled SSC supporting safety functions, which could cause an initiating event and/or prevent SSCs from performing safety functions, in response to the initiating event. This event category includes internal fires, internal floods, turbine missiles, high-energy line breaks, and other events that may impact or damage equipment in a spatially connected area in a manner that causes an initiating event, impacts the performance of a safety function, or both.

licensing-basis events (LBEs): Events selected from the event sequences modeled PRA to form part of the basis for the derivation of licensing requirements. LBEs include AOOs, DBEs, BDBEs, and deterministically selected DBAs.

liftoff: The physical disturbance and re-entrainment of deposited fission product material caused by rapid flows and shear forces during high-rate-of-depressurization events resulting from a large line break or penetration failure in a MHR.

light water reactor (LWR): A reactor with metal-clad core fuel elements cooled principally by light water.

mode, operating: Definitive configuration of the plant as the plant operates, from defueled to shutdown cooled down, to various startup configurations (auxiliary feedwater), to power operation configurations (synchronized and making electricity). Modes are significant operating points that define operating configurations. Consequently, plant accident analysis depends

greatly on the operating state (mode) at the start of an event.

model, mechanistic: Models based on fundamental mechanistic knowledge of process model interactions to constitute system analogs that define the model structure, allowing experiments to be performed to validate the model. In contrast, an empirical model uses a trial-and-error approach based on cause-effect relationships and real data, iteratively adjusting until an acceptable model has been established. Empirical models do not require understanding underlying physical processes but determine structure by the observed relationships among experimental data.

model, phenomenological: A model based on faithfully modeling a phenomenon. Modeling success depends on validating the observed phenomenon with the model. Phenomenological modeling combines elements of both mechanistic and empirical modeling.

model, validation, verification: Validation is the process of checking if a model satisfies an accuracy criterion. Validation usually addresses meeting the needs of an external customer or product or service user. Verification is an internal quality process that determines compliance with a regulation or specification. Validation is ensuring that “you built the right product,” and verification is ensuring that “you built the product right.”

modular: Unitized; addable in discrete, repetitive units.

multiple barriers: More than one barrier to the environmental release of fission products. For a MHR this includes multiple fuel particle coatings, graphite support matrix, RPV boundary, and building structure (or citadel).

nonconservative: Unconservative; assumptions or errors in a nonconservative direction increase proximity to margins and thus increase safety risk.

nuclear accident: An operating event in the beyond-abnormal-operating-occurrence range accompanied by loss of fission product barriers and increased risk of release of radioactive materials to the environment.

nuclear safety: Safety of the nuclear fuel reactivity and fission product boundary.

operating conditions: Normal conditions of service falling within operation limits for parameters like temperature, pressure, O₂ concentration, speed of operation, load, and stroke as well as other stated conditions.

passive component: A passive component has no moving parts and, for example, only experiences a change in pressure, temperature, or fluid flow in performing its functions. In addition, certain components that function with very high reliability based on irreversible action or change may be assigned to this category.

performance assessment: Assessment based on performance goals, in contrast with assessments of historical documentation, processes used to achieve performance, or other indirect outcome assessments.

performance-based: An approach to design or regulation that relies upon the desired, measurable results or performance outcomes based on objective criteria rather than a prescriptive process, technique, or procedure. Performance-based regulation differs from a traditional, prescriptive regulatory approach by emphasizing what is to be achieved rather than how desired results and outcomes are obtained. Effective regulatory decision makers using a performance-based approach consider (a) the most desirable results and (b) the activities (including monitoring) most likely to yield the desired results.⁶⁾

plant equipment: Equipment within the plant normally presumed to be operable.

plant operating state: A standard configuration of the plant during which the plant conditions are relatively constant, modeled as constant, and distinct from other configurations in ways that impact risk (e.g., core power level; HPB open/closed status, temperature, and pressure; reactor building status; and status of decay heat removal systems). A plant operating state can be a steady state or represent a transition between steady states. In a PRA model, each plant operating state provides a unique set of boundary conditions for selecting initiating events for the PRA event sequence analysis.

plateout: Deposit of lower-volatility fission products on lower-temperature surfaces. A form of physical volatile precipitation induced by temperature and pressure states.

power conversion: Conversion from thermal to mechanical and electrical power or vice versa.

primary heat transport system: Heat transport within the primary coolant boundary or the primary means of heat removal from the core.

probabilistic risk assessment (PRA): A qualitative and quantitative assessment of the *risk* associated with plant O&M that is measured in terms of frequency of occurrence of risk metrics, such as the frequency of a radioactive material release and its effects on the health of the public. Also referred to as a probabilistic safety assessment.

PRA event sequence: The event sequence defined by PRA for developing event families and evaluating top-level outcomes from initiating events.

PRA, full scope: A PRA that accounts for all known plant operating states, initiating events and their causes including those from internal and external plant hazards, and event sequences whose end states are sufficiently developed to support and include an estimation of mechanistic source terms and off-site radiological consequences. Full-scope PRAs include a definition of event sequences, quantification of sequence frequencies and consequences, and quantification of uncertainties in the frequency and consequence estimates that is sufficient to account for all risk-significant contributions to each modeled end state.

quantitative health objectives (QHOs): Numerical criteria for the acceptable levels of risk to public health and safety in the population surrounding plants that satisfy the national nuclear regulator's reactor safety goals. In the United States, the QHOs are expressed in terms of the annual average individual probability of death due to acute radiation syndrome within 1 mile of the site boundary and the annual average individual probability of death due to latent cancer per year within 10 miles of the site boundary of a plant, and these acceptance

⁶⁾ See item 7 in Memorandum dated February 24, 1999, from NRC Secretary A. L. Vietti-Cook to W. D. Travers, NRC Executive Director for Operations [2].

levels are set at <0.1% of the levels due to all manmade nonnuclear causes.

radionuclide transport barrier: A passive SSC designed to retain radionuclides and/or mitigate the radionuclide release source term during an accident sequence. Such barriers include physical barriers such as the fuel barrier, reactor coolant (e.g., helium) pressure boundary, and reactor building. For MHRs such barriers normally include the coated particle fuel, graphite or carbon fuel matrix, internal HPB surfaces, the HPB itself, and the reactor building associated barriers.

reactor building: The building immediately surrounding the RPV and HPB that provides structural integrity of the core, RPV, and HPB; physical protection from internal and external events to SSCs that perform safety functions; and a barrier to radionuclides that may be released from the HPB.

reactor characteristics, inherent: Intrinsic features to the type of reactor before considering safety features. Examples of inherent characteristics of MHRs include the material properties of silicon carbide and graphite, and the thermodynamic and chemical properties of graphite and helium.

release category: A grouping of event sequences into an event sequence family based on a common potential for release of radioactive material as characterized by its mechanistic source term. This common potential is based on common initiating events, combination of successful and failed safety functions, release magnitude, release timing and location, and radionuclide species that are released from the plant as a result of an event sequence. A release category may comprise one or more LBEs.

risk: Frequency and consequences of an event that answer the three fundamental safety questions. (1) What can go wrong? (2) How likely is it? (3) What are the consequences if it occurs? In PRA, risk is defined by a comprehensive set of event sequences, a quantitative assessment of the event sequence frequencies and their consequences, and an evaluation of the uncertainties in the assessments.

risk-informed decision process: A process that uses risk information and insights from PRA with traditional deterministic approaches and judgments to inform decisions.

root-sum-square uncertainty combination:

A mathematical uncertainty calculation based on the error stack equal to the sum of the extreme tolerances. This rule greatly overestimates the stackup if the errors are truly statistical; thus, taking assumed tolerances, squaring each, summing them, and taking the square root produce a statistical tolerance.

safety analysis: An analysis to confirm the adequacy of design once basic parameters including fundamental technology, TLSC, and reasonably likely events based on PRA have been developed.

safety criteria: Criteria that are to be met to conform to TLDC during a DBA, based on safety analysis.

safety features: Active and passive design features that are provided in the design of a plant specifically to perform a safety function. Active safety features involve mechanical action or motion to perform the safety function that requires application of external motive power such as electric or hydraulic power. Passive safety features perform their safety function without any active SSCs or externally applied motive power. Some safety features involve a combination of passive safety features and inherent reactor characteristics. In MHRs, examples of passive safety features normally include a negative coefficient of reactivity and a capability to remove decay heat via conduction, convection, and radiation heat transfer principles. Examples of active safety features include forced circulation core cooling systems and electrically powered reactor building filtration systems.

safety functions: Functions provided in the design to prevent and mitigate accidents and assure that TLRC are met under all conditions. Those functions necessary and sufficient to assure that the TLSC are met in the DBE portion of the F-C curve and regulatory dose limits for deterministically selected DBAs are met.

safety-related: Classification for plant SSCs relied on to perform safety functions for DBAs.

safety system: Systems that provide one or more safety functions.

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.

site boundary: The extent of site control for occupational exposure and the start of off-site accident exposure.

sorbed: Retention of a liquid or gas substance taken into and retained by another substance.

source term: The timing, quantity, physical and chemical form of, and thermal energy associated with, a release of radioactive material from a plant during an accident. The definition of the source term includes sufficient information to calculate the off-site radiological consequences of an accident.

source term, mechanistic: Calculated using validated models and supporting scientific data that simulate the physical and chemical processes that describe the radionuclide inventories and time-dependent radionuclide transport mechanisms that are necessary and sufficient to predict the source term.

special treatment: Requirements imposed on the design, material, manufacture, construction, inspection, testing, operation, and/or maintenance of an SSC that assure that the SSC will perform (e.g., with adequate reliability and capability) its safety functions for a specific set of LBEs. Special treatments specify critical characteristic inspections, tests, their analyses, and acceptance criteria that assure safety functions required. Also see SECY 99-256 [3], Definition, Appendix I: (1) go beyond industry-established requirements for equipment classified as commercial grade and (2) provide additional confidence that the equipment is capable of meeting its functional requirements under design-basis conditions. These additional special treatment requirements include additional design considerations, qualification, change control, documentation, reporting, maintenance, testing, surveillance, and quality assurance requirements.

stacking of uncertainties: Addition of multiple uncertainties in one analysis: Depending on stacking assumption, the final analysis may be either extremely overly conservative, moderately conservative, or (potentially) nonconservative.

systems, structures, and components (SSCs): Generic term for those components, structures, and integrated systems that comprise the designed plant.

systems, structures, and components (SSCs), non-safety-related (NSR) (NSR SSCs): SSCs whose reliabilities and capabilities are not required or credited for the frequency and consequences of any LBE to fall within the TLSC.

systems, structures, and components (SSCs), non-safety-related with special treatment (NSRWST) (NSRWST SSCs): SSCs selected by the designer to provide DID for safety functions.

SSCs, safety-related: SSCs selected by the designer that have sufficient reliability and capability to fulfill their safety functions and thereby ensure that frequencies and consequences of DBEs fall within the TLSC and that the consequences of the deterministically selected DBAs meet regulatory dose limits in the deterministic safety analysis.

success criteria: Criteria for establishing the safe and stable plant parameters and minimum levels of performance per component during a specific mission time to ensure that a reactor-specific safety function is satisfied.

system failure: System-level failure involving at least one (but probably more) system functional failures.

system, support: An auxiliary or supporting system providing services or power.

take credit: Rely upon SSCs in safety analysis DBAs (limiting conservative analysis), Chapter 15 of the NRC Safety Analysis Report (SAR) (NUREG-0800 [4]). The analysis to demonstrate safety criteria relies on, takes into account, uses, and bases analysis on the “credited” SSC performance. (The SSCs relied on are then subject to special treatment commensurate with their safety significance. Balance-of-plant SSCs are not credited in Chapter 15 for positive responses. Balance-of-plant SSCs are included or “credited” in other analyses of realistic plant performance, such as Chapter 19, design chapters, etc., of NUREG-0800.

technology neutral: Applicable to any type of reactor and independent of any single reactor technology.

top-level design criteria (TLDC): TLSC design implementing criteria; design criteria based on meeting the TLSC, unique to a specific type of plant technology.

top-level regulatory criteria (TLRC): Criteria expressed in the national nuclear regulator's regulations that are used to define the TLSC.

top-level safety criteria (TLSC): Limits on the frequency and consequences of LBEs derived from TLRC.

total effective dose equivalent (TEDE): The sum of the deep-dose equivalent (for external exposures) and the committed effective dose equivalent (for internal exposures).

uncertainty distribution: Probability distribution used to describe the uncertainty in the estimation of a parameter that is used to calculate the frequency, consequences, or risk associated with an event sequence.

3 Develop safety design criteria

This standard establishes safety design criteria for MHRs. These safety design criteria provide the technical basis for ensuring that an MHR design meets applicable top-level health and safety regulatory criteria and that equipment that is important to reactor safety has the design capability and the performance reliability needed to perform the intended safety functions.

3.1 Introduction to safety criteria development

MHR designs are required to meet the top-level off-site and on-site regulatory dose limits

and guidelines established by the national nuclear regulator. MHR designs are also expected to meet the applicable safety goals that have been established by the national nuclear regulator. The MHR TLSC established by this standard are to provide the acceptance criteria for meeting the established regulatory dose limits, guidelines, and safety goals. This standard provides an approach for developing these TLSC.

MHR designs also need to meet equipment-related MHR TLDC, which provide assurance that the MHR equipment important to safety perform as required. This standard provides an approach for developing MHR TLDC. The approach to MHR safety design links protection of public health and safety with specific safety design requirements. Table 1 shows the required elements of the approach.

Section 3.2 discusses TLSC; in Sec. 3.4, the TLDC are specified. MHR safety design requirements use TLSC as the acceptance criteria for the LBE consequences.

Section 3.3 presents the approach to LBE selection, including expected plant performance demonstrated by PRA. This section also defines safety functions provided by plant SSCs.

Section 3.4 discusses development of TLDC to be met in conjunction with the deterministic analysis of the DBAs. These include "required" safety functions that prevent and mitigate DBEs

Table 1 – Required MHR safety design elements

Element	Purpose
TLSC	Establish <i>which</i> safety acceptance criteria are to be met
LBEs	Define <i>when</i> and under what conditions the TLSC are to be met
Required MHR specific safety functions; TLDC	Establish <i>how</i> TLSC are to be met
Safety-classified SSCs	Identify which SSCs are required to meet the TLSC
Special treatment requirements for DBA conditions	Provide assurance that the SSCs required to meet the TLSC by design can meet the TLSC
DID	Provides additional assurance that the TLSC are met

and “supportive” safety functions that contribute to DID.

Section 4 summarizes the specific requirements for the plant PRA scope, quality, and completeness.

3.2 Establish event categories and F-C curve

The RI-PB approach used in this safety standard establishes a set of TLSC. The TLSC are the event frequency-dependent radionuclide retention acceptance criteria for the LBEs.

The top-level off-site and on-site regulatory dose limits and guidelines are established by the national nuclear regulator. These regulatory limits and guidelines provide the basis for the TLSC on-site and off-site consequences. MHR designs meet these quantitative regulatory requirements and guidance to ensure adequate public health and safety. The TLSC limit the frequency of events as a function of the radiological dose consequences to individuals. These regulatory criteria provide the basis for the acceptance criteria established for this standard. The designer shall identify the specific national regulatory requirements and guidance used to develop the quantitative acceptance criteria or TLSC to be met by the MHR design. In this regard, the existing national nuclear regulatory authority regulations, safety goals, and guidance establish the TLSC basis by setting allowable dose consequences for different types of events and associated probabilistic and deterministic safety analyses.

Quantitative TLSC that are established support a RI-PB MHR safety design approach. A

TLSC F-C curve, of acceptable dose versus event frequency, shall be established for the following LBE categories for the MHR:

- AOOs are expected to occur one or more times during the life of the plant;
- DBEs are not expected to occur during the lifetime of a single plant but may occur during the lifetime of a population of plants;
- BDBEs are those LBEs not expected to occur during the lifetime of a large fleet of plants but are included to assure that risk to the public from very low-frequency events is acceptable.

The F-C curve shall establish an event frequency range for all LBEs. Event sequences shown to have a sufficiently low frequency on a per plant-year basis are not identified as LBEs but are evaluated in the PRA to a frequency level that is sufficiently low to meet risk significance criteria established in the American Society of Mechanical Engineers (ASME) PRA standards. The ASME PRA standards include the assessment of events, failures, and natural phenomena as follows:

- multiple, dependent, and common-cause failures to the extent they contribute to LBE frequencies;
- events affecting more than one reactor module;
- internal events and internal and external plant hazards that occur in all operating and shutdown modes and potentially challenge the capability to satisfactorily retain any source of radioactive material.

Table 2 – Summary of requirements for F-C curve

Designator	Requirement
3-FC-1	The designer shall identify the specific national regulatory requirements and guidance used to develop the quantitative acceptance criteria or TLSC to be met by the MHR design.
3-FC-2	A TLSC F-C curve, of acceptable dose versus event frequency, shall be established for the following LBE categories for the MHR: AOOs, DBEs, and BDBEs.
3-FC-3	The F-C curve shall establish an event frequency range for all LBEs.

Note: The format of this standard provides a table at the end of each body of text that summarizes and provides succinct actionable content required.

3.2.1 TLSC selection guidance

The TLSC selected and used should be based on the following objectives:

- (1) Provide direct public health and safety acceptability limits in terms of individual radiological consequences;
- (2) Assure that technology is neutral, independent of MHR type and site;
- (3) Provide well-defined, quantifiable risk criteria;
- (4) Meet the national nuclear regulator's TLRC.

The dose acceptance criteria for LBEs shall be based on the regulatory dose guidelines established by the national nuclear regulator for meeting risk goals from plant operation and emergency planning protective action guidelines (PAGs).

For example, to meet these objectives in the United States, the following regulatory criteria were identified as providing an acceptable compilation of regulatory requirements and guidelines (TLRC) for establishing the TLSC for MHR safety design:

- "Reactor Safety Goal Policy Statement" [5]: Limits public safety risk resulting from plant operation. Limits are stated in the form of the maximum allowable risk of immediate death and the risk of delayed mortality from exposure to radiological releases of all types from plants;
- 10 CFR 20, Subpart D [6]: Limits the dose consequences of relatively high-frequency events and releases that occur as part of normal plant operations;

- 10 CFR 50, Appendix I [7]: Contains cost-benefit criteria for normal releases;
- 40 CFR 190 [8]: Limits the radiological exposures to the public from routine plant operations;
- 10 CFR 100 [9]: Imposes limits on radiological consequences associated with low-frequency DBEs and hypothetical scenarios selected to qualify the location of the site and the site boundary in relation to nearby population zones;
- 10 CFR 50.34(a) [10]: Specifies dose limits that are similar to those in 10 CFR 100 but are expressed in TEDE units;
- EPA-400-R-92-001 [11]: Sets conditions for initiating off-site emergency protective actions in the event of a threat of significant radiological exposure that would exceed 10 CFR 20 [12] and 10 CFR 50, Appendix I, limits.

The regulatory dose consequence limits associated with the above TLRC can be used to establish an F-C curve (i.e., the TLSC) of dose consequence limits versus event frequencies for plant design in the United States. The selected frequency ranges are those that the nation nuclear regulator associates with AOOs, DBEs, and BDBEs, respectively. For example, for MHR design in the United States,

- (1) 10 CFR 20, Subpart D; 10 CFR 50, Appendix I; and 40 CFR 190 pertain to normal operation and AOOs that are expected to take place sometime during the operational life of a plant;
- (2) 10 CFR 100 and 10 CFR 50.34(a)(1) pertain to DBEs that are not expected to occur during the life of a plant but could reasonably occur within the operational life of a large fleet of similar plants;
- (3) The reactor safety goals and PAGs generally pertain to accidents that are within and beyond the design basis of the plant.

Table 3 – Summary of requirements for TLSC selection

Designator	Requirement
3-TLSC-1	The dose acceptance criteria for LBEs shall be based on the regulatory dose guidelines established by the national nuclear regulator for meeting risk goals from plant operation and emergency planning PAGs.

3.2.2 F-C curve and event region guidance

The spectrum of potential accidental radionuclide releases from a plant is divided into three LBE frequency regions (Fig. 3):

- normal operation and AOO region;
- DBE region;
- BDBE region.

The event frequency range selected for categorizing a LBE shall be on a per plant-year basis for all reactor modules and the frequency range, including the lower cutoff frequency that the national nuclear regulator associates with BDBEs. The F-C curve shall display the annual frequency and consequences and include the uncertainty range for each LBE.

Figure 3 illustrates a F-C curve. The F-C curve shows the TLSC partitioned into the above three regions. This illustrative F-C curve is based on the TLRC established by the U.S. national nuclear regulator for plant licensing. The illustrative F-C curve, based on the TLRC, assigns specific event frequency ranges for

these TLSC that the U.S. national nuclear regulator associates with AOOs, DBEs, and BDBEs, respectively.

In interpreting plant-year frequencies associated with the F-C curve, Fig. 3 accounts for the total number of reactor modules in the plant. Designers shall assess the cumulative probability of events for a plant with multiple reactor modules to determine whether the events are within the frequency bounds for an AOO, DBE, or BDBE. The event frequency shall be the event sequence frequency and shall be on a plant-year basis to account for the number of reactor modules in the plant. The plant PRA is used to establish the mean frequency and frequency range for events on a single reactor module (on a reactor-year basis), as well as the mean frequency and frequency range for events, for all reactor modules in the plant (on a plant-year basis). In addition, the PRA is to account for the integrated release and total dose consequences for events when simultaneous source terms from multiple reactor modules are involved.

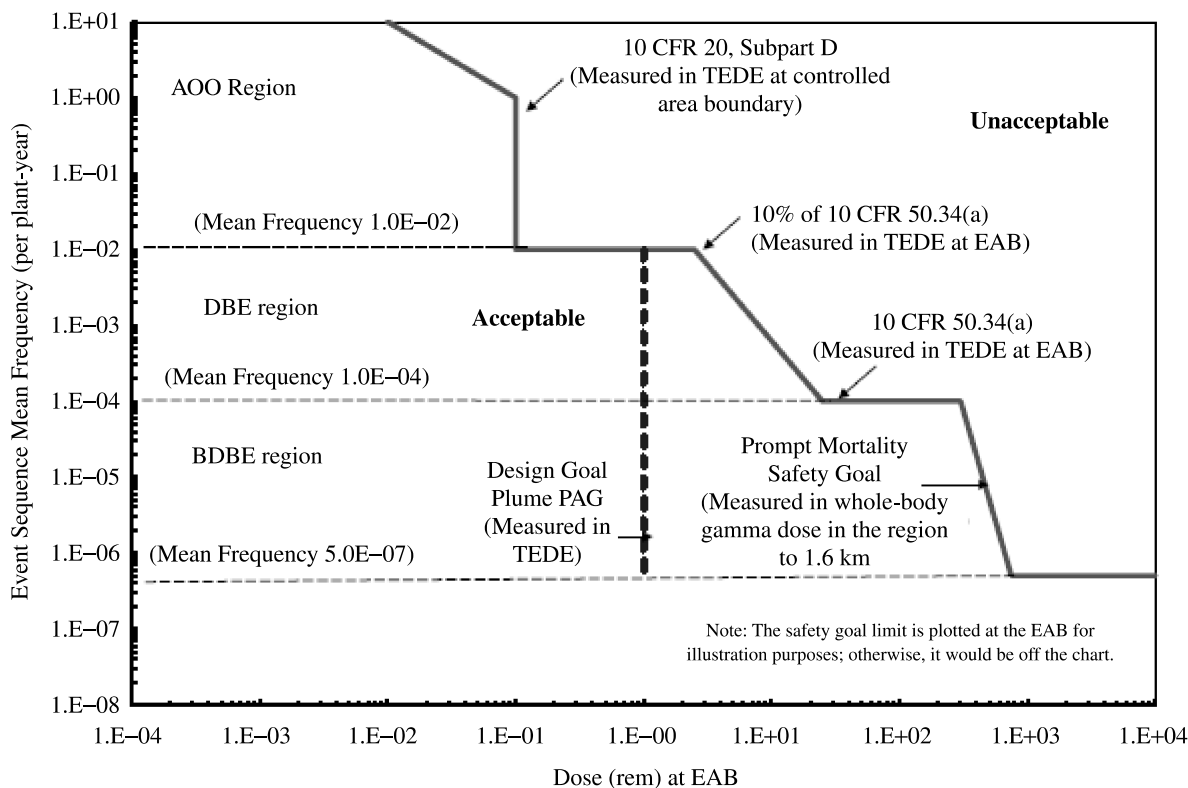


Figure 3 – Illustrative F-C curve based on TLRC

Table 4 – Summary of requirements for F-C curve and event region

Designator	Requirement
3-FCER-1	The event frequency range selected for categorizing a LBE shall be on a per plant-year basis for all reactor modules and the frequency range, including the lower cutoff frequency that the national nuclear regulator associates with BDBEs.
3-FCER-2	The F-C curve shall display the annual frequency and consequences and include the uncertainty range for each LBE.
3-FCER-3	Designers shall assess the cumulative probability of events for a plant with multiple reactor modules to determine whether the events are within the frequency bounds for an AOO, DBE, or BDBE.
3-FCER-4	The event frequency shall be the event sequence frequency and shall be on a plant-year basis to account for the number of reactor modules in the plant.

3.2.2.1 Normal operation and AOO region

The AOO region involves those frequent conditions of normal operation and transients (i.e., event sequences) that a design expects to occur one or more times during the life of a single reactor module. Additionally, design assumes a reactor-operating period of 60 years. Events in this category are conservatively assumed to occur at a rate of 1×10^{-1} events/reactor-year ($1\text{E}-01$ events/reactor-year).

Multiple modules increase the frequency of reactor module-related scenarios and create the potential for scenarios involving multiple modules concurrently. The cumulative probability of events for a plant with multiple reactor modules is to be evaluated in establishing whether an event is within the frequency bounds of an AOO. Again, the plant PRA is used to establish the frequency of individual reactor module events, on a reactor-year basis, and the frequency of such events, for all reactor plant modules, on a plant-year basis.

A conservative value of 1×10^{-2} events/plant-year ($1\text{E}-02$ events/plant-year) establishes the lower bound of the AOO region. For events in this region, in the United States, 10 CFR 50, Appendix I, would be the applicable TLRC, as it specifies the numerical guidance to ensure that releases of radioactive material to unrestricted areas during normal reactor operations, including AOOs, are maintained as low as is reasonably achievable.

3.2.2.2 DBE region

The DBE region encompasses infrequent events that are not expected to occur during the lifetime of a single plant but may occur during the lifetime of a population of plants. Therefore, a value of 1×10^{-4} events/plant-year ($1\text{E}-04$ events/plant-year) is used to establish the lower frequency bound of the DBE region. Again, the cumulative probability of events for a plant with multiple reactor modules is evaluated in establishing whether an event is within the bounds for categorizing the event as a DBE. Again, the plant PRA is used to establish the frequency of individual reactor module events, on a reactor-year basis, and the frequency of such events, for all reactor plant modules, on a plant-year basis.

The adoption of the DBE region's lower frequency limit of 1×10^{-4} events/plant-year ($1\text{E}-04$ events/plant-year) is appropriate because it is applied on a per-plant basis and accounts for possible multiple MHR modules. In addition, the expression of the frequency metric on a per plant-year basis enables the assessment to include event sequences involving only one or multiple reactor module source terms and thereby provides a more complete risk assessment as compared with the approach of analyzing each reactor module on an independent reactor-year basis.

As shown in Fig. 3, in the United States, for events in the DBE frequency region, 10 CFR 50.34(a) is selected as the TLRC quantitative dose guidance for accidental releases for siting

to ensure that the surrounding population is adequately protected. However, the TLSC dose allowed by 10 CFR 50.34(a) is scaled so the allowed dose is reduced for events of higher frequency within the DBE frequency region. The F-C curve for the DBE region has been established, in this case, such that event sequences that fall within the DBE region are limited in the allowed dose consequences in order to facilitate meeting the NRC safety goal QHOs for individual risk of latent cancer fatality.

3.2.2.3 BDBE region

The BDBE region involves rare events that are not expected to occur during the lifetimes of a large fleet of similar plants. The F-C curve categorizes such rare events to ensure that the risk to the public from very low-probability events is acceptable. The curve also ensures that adequate emergency planning is developed to protect the public from potential elevated exposure to radiation from rare events to avoid potential doses that could exceed the limits for the U.S. Environmental Protection Agency PAGs for sheltering and evaluation.

The BDBE region shall consider events with a mean value below the DBE region's lower frequency limit of 1×10^{-4} events/plant-year (1E-04 events/plant-year). As guidance, the lower frequency boundary of the BDBE region is 5×10^{-7} events/plant-year (5E-07 events/plant-year). This frequency cutoff is implicit in the U.S. national nuclear regulator acute fatality risk goal identified in NUREG-0880 [13]. This prompt mortality risk objective limits the increase in an individual's annual risk of accidental death to 0.1% of 5×10^{-4} events/plant-year (5E-04 events/plant-year), or an incremental increase of no more than 5×10^{-7} events/year (5E-07 events/year). The risk-informed safety design approach interprets these QHOs to be applied to the site as

whole as each individual near the plant site is exposed to all the sources of risk on that site. If the frequency of a scenario or set of scenarios as defined on a per site-year basis is at or below this value, it can be assumed that the individual risk contributions from these scenarios would still fall within the safety goal independent of the magnitude of the consequences with a significant residual margin.

As guidance, very rare event sequences that can be shown to fall below the 5×10^{-7} events/plant-year (5E-07 events/plant-year) are not formally included as BDBEs. However, events with calculated mean probabilities below 5×10^{-7} events/plant-year (5E-07 events/plant-year) generally involve very large uncertainties in the event probability because of the limited test data and operational data associated with the models. Additionally, very low-probability-event dose consequences may jump abruptly from transformative "cliff-edge" events that involve a relatively large increase in the calculated consequences for a small change in an independent input variable. Dose consequence uncertainty arises from accident phenomenon modeling, accident progression, and release. The uncertainty in the event frequency and event consequences shall be used to determine whether an event sequence with a very low mean frequency below 5×10^{-7} events/plant-year (5E-07 events/plant-year) is to be included as a BDBE. The magnitude of the uncertainties in both the event frequency and event consequences for very low frequency events shall be based on the plant PRA. Event sequences with a mean frequency below 5×10^{-7} events/plant-year (5E-07 events/plant-year) shall be addressed in the assessment. Event sequences that involve cliff-edge effects below 5×10^{-7} events/plant-year (5E-07 events/plant-year) shall be included as a BDBE.

Table 5 – Summary of requirements for BDBEs

Designator	Requirement
3-BDBE-1	The BDBE region shall consider events with a mean value below the DBE region's lower frequency limit of 1×10^{-4} events/plant-year (1E-04 events/plant-year).
3-BDBE-2	The uncertainty in the event frequency and event consequences shall be used to determine whether an event sequence with a very low mean frequency below 5×10^{-7} events/plant-year (5E-07 events/plant-year) is to be included as a BDBE.
(Continued)	

Table 5 – Summary of requirements for BDBEs (Continued)

Designator	Requirement
3-BDBE-3	The magnitude of the uncertainties in both the event frequency and event consequences for very low frequency events shall be based on the plant PRA.
3-BDBE-4	Event sequences with a mean frequency below 5×10^{-7} events/plant-year (5E-07 events/plant-year) shall be addressed in the assessment.
3-BDBE-5	Event sequences that involve cliff-edge effects below 5×10^{-7} events/plant-year (5E-07 events/plant-year) shall be included as a BDBE.

3.2.3 Cumulative risk

In addition to having to meet the F-C curve for individual events, the overall integrated risk of all event sequences from the plant PRA shall be shown to meet the plant's operational risk objectives (safety goals for plant risk) as set by the national nuclear regulator. As guidance, in the United States, the national nuclear regulator has established safety goals in terms of QHOs to assess the acceptability of individual event families to the TLSC. This sums each event's risk, accounting for uncertainties in both the frequency and consequence. As guidance, a

simple sum of products of the expected frequencies times the expected consequences divided by the population inside the annulus "doughnut" will yield the calculated QHO risk metric. Families shall be developed consistently to reveal integrated risk above limits. Families developed to arbitrarily reduce the SSC frequency below the levels for integrated risk limits would avoid meeting the intent of the PRA and are not allowable.

For plants in the United States, the NRC safety goal QHOs compare the overall integrated risk from all plant PRA event sequences to determine event families' TLSC acceptability.

Table 6 – Summary of requirements for cumulative risk determination

Designator	Requirement
3-CR-1	The overall integrated risk of all event sequences from the plant PRA shall be shown to meet the plant's operational risk objectives (safety goals for plant risk) as set by the national nuclear regulator.
3-CR-2	Families shall be developed consistently to reveal integrated risk above limits.

3.2.4 DID requirement

DID is a philosophy as well as a design concept. The term holds special regulatory meaning. Designers shall establish DID goals by specifying design philosophy and goals with criteria like redundancy, diversity, and design margin.

To assure adequate DID, designers shall specify design DID requirements and design goals prior to safety design. Upon completing safety design analyses (Sec. 6), designers evaluate DID adequacy against their specified DID criteria

for adequacy to overall DID in light of the design technology applied (Sec. 7).

To assure adequate DID development, designers need to consider how they will provide the following criteria to satisfy evaluation in Sec. 7:

Designers shall

- provide successive compensatory means to prevent accidents or lessen the effects of damage if an accident or malfunction occurs;
- implement a multiple-barrier approach against fission product releases;

- provide redundancy in safety function performance;
 - assure that safety will not be wholly dependent on any single nuclear facility design, construction, maintenance, or operation element, nor be wholly dependent on any single design feature (or features) that enhances (enhance) safety by reducing challenges to SSCs relied on for safety;
 - demonstrate preference for selecting engineered over administrative controls to increase overall safety function reliability;
 - address uncertainty by employing measures including safety margins and special treatments that ensure SSC equipment reliability to the level assumed in the design PRA;
 - assure that the public is adequately protected on the intended site and that well-conceived, workable emergency plans surround the nuclear facility;
 - evaluate plant design features in an integrated manner as part of an overall risk management approach.
- Designers shall broadly use risk analysis to improve engineering and operational decisions by identifying and taking advantage of opportunities to reduce risk.

Table 7 – Summary of requirements for DID

Designator	Requirement
3-DID-1	Designers shall establish DID goals by specifying design philosophy and goals with criteria like redundancy, diversity, and design margin.
3-DID-2	Designers shall specify design DID requirements and design goals prior to safety design.
3-DID-3	Designers shall provide successive compensatory means to prevent accidents or lessen the effects of damage if an accident or malfunction occurs.
3-DID-4	Designers shall implement a multiple-barrier approach against fission product releases.
3-DID-5	Designers shall provide redundancy in safety function performance.
3-DID-6	Designers shall assure that safety will not be wholly dependent on any single nuclear facility design, construction, maintenance, or operation element, nor be wholly dependent on any single design feature (or features) that enhances (enhance) safety by reducing challenges to SSCs relied on for safety.
3-DID-7	Designers shall demonstrate preference for selecting engineered over administrative controls to increase overall safety function reliability.
3-DID-8	Designers shall address uncertainty by employing measures including safety margins and special treatments that ensure SSC equipment reliability to the level assumed in the design PRA.
3-DID-9	Designers shall assure that the public is adequately protected on the intended site and that well-conceived, workable emergency plans surround the nuclear facility.
3-DID-10	Designers shall evaluate plant design features in an integrated manner as part of an overall risk management approach.
3-DID-11	Designers shall broadly use risk analysis to improve engineering and operational decisions by identifying and taking advantage of opportunities to reduce risk.

3.3 Establish safety functions

MHR safety functions ensure that the radiological dose consequences of LBEs are limited so that the TLSC can be met. MHR SSCs perform safety functions. MHR safety functions and associated MHR SSCs provide for both prevention and mitigation of event sequences that could exceed the TLSC. Safety functions shall be established for the plant design that

- limit radiological dose consequences of each LBE so that the F-C curve TLSC are not exceeded by any LBE;

- reduce the likelihood of each LBE so that the F-C curve TLSC are not exceeded by any LBE.

A plant SSC shall be selected to perform each established safety function. MHR SSC design capability (TLDC of the MHR SSCs) shall ensure that the TLSC are met for all LBEs. The TLDC define the SSC design acceptance criteria, which ensure that the performance and capability of the SSCs result in the TLSC being met.

Table 8 – Summary of requirements for establishing MHR safety functions

Designator	Requirement
3-SF-1	Safety functions for the plant design shall limit radiological dose consequences of each LBE so that the F-C curve TLSC are not exceeded by any LBE.
3-SF-2	Safety functions for the plant design shall reduce the likelihood of each LBE so that the F-C curve TLSC are not exceeded by any LBE.
3-SF-3	A plant SSC shall be selected to perform each established safety function.
3-SF-4	MHR SSC design capability (TLDC of the MHR SSCs) shall ensure that the TLSC are met for all LBEs.

3.3.1 SSC categorization

MHR safety functions shall be accomplished by MHR SSCs. MHR safety-related SSCs shall be categorized as either “required” or “supportive.” SSCs that perform required safety functions shall be classified as “safety-related.” SSCs that perform supportive safety functions are not classified as safety-related. MHR SSCs that are not associated with MHR nuclear safety are categorized as non-safety-related (NSR). MHR required safety-related SSCs alone (i.e., necessary and sufficient) ensure that the TLSC associated with the DBE region are not exceeded by any DBE. Required safety-related SSCs also ensure that the TLRC for the DBE region are not exceeded by any of the deterministically selected DBAs (discussed in Sec. 5). To the extent possible, the required safety-related SSCs shall be passive. MHR supportive safety-related SSCs together with the MHR required safety-related SSCs ensure that the F-C curve TLSC for the other event categories, (i.e., AOs and BDBEs) are not exceeded.

Identifying required safety-related SSCs shall be the initial step in the safety classification of plant SSCs (Sec. 5). For each required safety-related SSC, TLDC shall be established and shown to be met by analysis.

However, TLDC shall also be developed for supportive safety functions if the functional capability provided by the SSC is safety or risk beneficial. The consequences of DBEs are prevented and/or mitigated to meet the TLSC solely by required safety-related SSCs; supportive safety-related SSCs are not modeled in the safety analyses (e.g., “credited”) for DBEs. Accordingly, supportive safety-related SSCs shall be used only to provide margin or DID for meeting the DBA TLRC.

Although the top-level functions are generic to all nuclear power plants, the lower-level functions become more specific to MHR plant technology. Section 3.4 provides TLDC corresponding to the shaded blocks in Fig. 4. The required safety functions and TLDC shall be derived

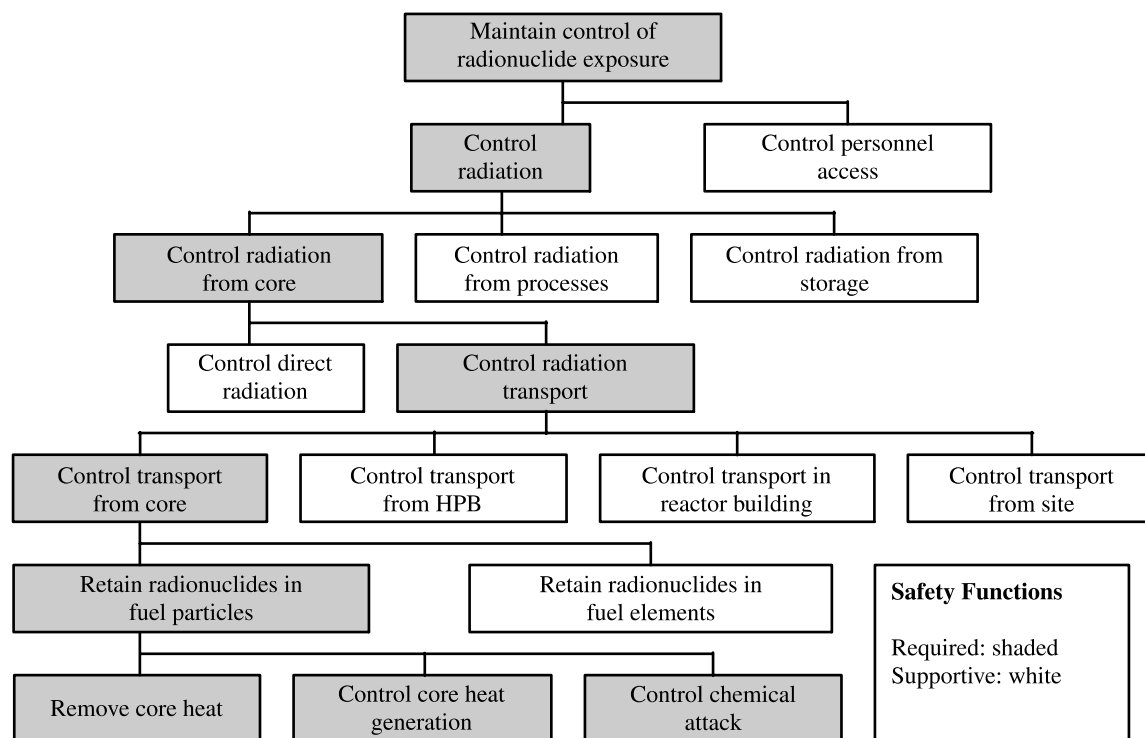


Figure 4 – MHR safety functions

from a complete functional analysis for each plant. Figure 4 illustrates the required safety function derivation using the top-down functional analysis technique. Figure 4 shows the safety functions needed to maintain the TLSC: control of radionuclide exposure (shown by the shaded boxes). The white boxes show other supportive safety functions.

In the most general sense, the designer starts by identifying the safety functions needed to maintain the TLSC. These depend on the fundamental top-level requirements listed earlier (control heat generation, remove heat, and maintain fission product barriers). Then, from phenomenological relationships such as

$$\text{Dose Exposure} = (\text{Dose Rate})$$

$$\times (\text{Time of Exposure}) ,$$

the designer can develop functional requirements. For example, to control dose exposure to meet the TLSC in the occupational exposure (AOO) area requires controlling the dose rate and the exposure time. When the designer can completely control one of the two factors, or

when one factor otherwise dominates reducing the influence of the other, the designer can select controlling that factor as the primary functional requirement. The other functional requirement becomes supportive, not anticipated to be required to meet the TLSC. From the functional requirements, the designer can then identify the safety systems that will be required to deliver the functional requirements for the TLSC. Partitioning the facility using other functional requirements for the same system SSCs, the analyst can develop layers of safety systems and SSCs: requirements, functions (systems), system partition (all systems' descriptions required to meet the same functions), their SSCs and their functions, and so forth.

The objective is not to develop the detailed design but only to develop the high-level requirements as much as needed to identify the systems required, and whether they are "required" or supportive to meet the TLSC. The result is a set of detailed system functional statements that allows the designer to develop the more detailed requirements: the required and supportive safety functions. "Required" safety

functions are those that are required to meet the TLSC; “supportive” safety functions are those that are not required but that may still be used to demonstrate DID. All safety functions are to be demonstrated by PRA (Sec. 4),

and the required safety function design (e.g., required safety systems and their safety-related SSCs) is to be proven adequate by performing detailed safety analyses (Sec. 6).

Table 9 – Summary of requirements for SSC categorization

Designator	Requirement
3-SFC-1	MHR safety functions shall be accomplished by MHR SSCs.
3-SFC-2	MHR safety-related SSCs shall be categorized as either “required” or “supportive.”
3-SFC-3	SSCs that perform required safety functions shall be classified as “safety-related.”
3-SFC-4	To the extent possible, the required safety-related SSCs shall be passive.
3-SFC-5	Identifying required safety-related SSCs shall be the initial step in the safety classification of plant SSCs (Sec. 5).
3-SFC-6	For each required safety-related SSC, TLDC shall be established and shown to be met by analysis.
3-SFC-7	TLDC shall also be developed for supportive safety functions if the functional capability provided by the SSC is safety or risk beneficial.
3-SFC-8	Supportive safety-related SSCs shall be used only to provide margin or DID for meeting the DBA TLRC.
3-SFC-9	The required safety functions and TLDC shall be derived from a complete functional analysis for each plant.

3.3.2 MHR safety functions

3.3.2.1 Control radionuclides in fuel particles

MHR coated fuel particles are the primary barrier to the release of radionuclides from a plant. Retaining radionuclides requires designing, fabricating, and operating the fuel limiting normal operational releases to the radionuclide inventory within the particle’s coating barrier [i.e., within the tri-isotopic (TRISO) coatings of individual particles]. This avoids challenging 10 CFR 50.34(a) dose limits. Control radionuclides in design, fabrication, and operation of the fuel to limit operational releases to ones considered normal on the F-C curve. With this limit, only the radionuclide inventory within the fuel itself presents a potential challenge to meeting TLRC. Each individual coated fuel particle shall retain the radionuclide inventory within its barriers, which (combined with other plant radionuclide barriers)

ensures meeting the dose consequence acceptance limits across the spectrum of evaluated events. The coated fuel particles shall be designed, fabricated, and operated to provide for a very low fuel particle failure rate and to limit fission product releases from the coated fuel particles during normal operation, AOOs, DBEs, and BDBEs. The fuel specification shall be selected so that the TLSC are not exceeded by any events in the respective event categories. In support of this, the following parameters shall be specified:

- maximum allowed coated fuel particle defect rate from manufacture;
- maximum allowed heavy metal contamination rate outside the intact fuel particles due to manufacture;
- maximum allowed coated fuel particle failure rate due to MHR normal operations;
- maximum allowed coated fuel particle failure rate due to MHR accident conditions.

Table 10 – Summary of requirements for control of radionuclides in fuel particles

Designator	Requirement
3-CRFP-1	Each individual coated fuel particle shall retain the radionuclide inventory within its barriers, which (combined with other plant radionuclide barriers) ensures meeting the dose consequence acceptance limits across the spectrum of evaluated events.
3-CRFP-2	The coated fuel particles shall be designed, fabricated, and operated to provide for a very low fuel particle failure rate and to limit fission product releases from the coated fuel particles during normal operation, AOOs, DBEs, and BDBEs.
3-CRFP-3	The fuel specification shall be selected so that the TLSC are not exceeded by any events in the respective event categories.
3-CRFP-4	The maximum allowed coated fuel particle defect rate from manufacture shall be specified.
3-CRFP-5	The maximum allowed heavy metal contamination rate outside the intact fuel particles due to manufacture shall be specified.
3-CRFP-6	The maximum allowed coated fuel particle failure rate due to MHR normal operations shall be specified.
3-CRFP-7	The maximum allowed coated fuel particle failure rate due to MHR accident conditions shall be specified.

3.3.2.2 Remove core heat

The plant is designed to ensure reactor decay heat removal during AOOs relying primarily on active standby core cooling systems. During DBEs and BDBEs, the plant may rely solely on passive core cooling systems. The principal safety requirement is to ensure reliable decay heat removal.

The plant decay heat removal systems shall be designed for performance and reliability during normal and AOO conditions using active standby core cooling systems. The plant shall have the capability to remove reactor decay heat during AOOs relying primarily on active standby core cooling systems without exceeding the TLSC for AOOs.

During DBEs and BDBEs, the core heat function (core heat removal) shall be capable of being performed solely by passive means using conduction, convection, and radiation charac-

teristics of the core components in conjunction with a passive RCCS to discharge core decay and residual heat to the ultimate heat sink. The plant shall have the capability to remove reactor decay heat during DBEs and BDBEs without exceeding the respective TLSC for DBEs or BDBEs relying solely on passive core cooling systems. The plant shall have the capability to remove reactor decay heat during the deterministically selected DBAs solely with safety functions performed by the required safety-related SSCs without exceeding the TLRC for DBAs.

During active and/or passive core heat removal, the fuel temperature shall not exceed the fuel temperature design limits where excessive fuel failure could occur over a large portion of the core. A limited amount of TRISO fuel failure is acceptable; however, site boundary dose limits ultimately determine the amount of fuel failure allowed.

Table 11 – Summary of requirements for removal of core heat

Designator	Requirement
3-RCH-1	The plant decay heat removal systems shall be designed for performance and reliability during normal and AOO conditions using active standby core cooling systems.
3-RCH-2	The plant shall have the capability to remove reactor decay heat during AOOs relying primarily on active standby core cooling systems without exceeding the TLSC for AOOs.
3-RCH-3	During DBEs and BDBEs, the core heat function (core heat removal) shall be capable of being performed solely by passive means using conduction, convection, and radiation characteristics of the core components in conjunction with a passive RCCS to discharge core decay and residual heat to the ultimate heat sink.
3-RCH-4	The plant shall have the capability to remove reactor decay heat during DBEs without exceeding the TLSC for DBEs relying solely on passive core cooling systems.
3-RCH-5	The plant shall have the capability to remove reactor decay heat during BDBEs without exceeding the TLSC for BDBEs relying solely on passive core cooling systems.
3-RCH-6	The plant shall have the capability to remove reactor decay heat during the deterministically selected DBAs solely with safety functions performed by the required safety-related SSCs without exceeding the TLRC for DBAs.
3-RCH-7	During active and/or passive core heat removal, the fuel temperature shall not exceed the fuel temperature limits where excessive fuel failure could occur over a large portion of the core.

3.3.2.3 Control heat generation

The plant shall be designed, fabricated, and operated to ensure inherent reactor core shutdown and active reactor core shutdown to control reactor core heat generation during DBEs and BDBEs.

The reactor passive negative feedback shall be designed to ensure that the reactor thermal power does not exceed acceptable values during any DBE. The active reactor shutdown systems shall

ensure that reactivity insertion events in the DBE region do not result in the reactor power exceeding acceptable values. The plant shall be designed with sufficient inherent negative reactivity feedback to limit reactor core heat generation so that the TLRC are not exceeded for any DBA without the use of active reactor shutdown. A redundant and diverse active means of negative reactivity insertion shall be provided and be capable of bringing the reactor to a cold shutdown condition from any operating state.

Table 12 – Summary of requirements for control of heat generation

Designator	Requirement
3-CHG-1	The plant shall be designed, fabricated, and operated to ensure inherent reactor core shutdown and active reactor core shutdown to control reactor core heat generation during DBEs and BDBEs.
(Continued)	