CONTENTS

Section A

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

November 10, 2020

Mr. Peter Hastings
Vice President, Regulatory Affairs
and Quality
Kairos Power LLC
707 W Tower Ave
Alameda, CA 94501

SUBJECT: FINAL SAFETY EVALUATION FOR KAIROS POWER LLC TOPICAL REPORT "KP-FHR RISK-INFORMED PERFORMANCE-BASED LICENSING BASIS DEVELOPMENT METHODOLOGY" (REVISION 1) (EPID NO. L-2019-TOP-0009/CAC NO. 000431)

Dear Mr. Hastings:

By letter dated August 6, 2019 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML19217A420), Kairos Power LLC (Kairos Power, the applicant) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review, Topical Report (TR) "KP-FHR Risk-Informed Performance-Based Licensing Basis Development Methodology". The NRC staff provided initial feedback and questions to Kairos Power on January 8, 2020 (ADAMS Accession No. ML20009E754), and on March 19, 2020 (ADAMS Accession No. ML20104A031). In response to these questions and following a teleconference between the NRC staff and Kairos Power, the applicant submitted an updated TR (Revision 1) by letter dated April 10, 2020 (ADAMS Accession No. ML20101P623), on which this final safety evaluation (SE) is based.

A draft SE was issued on September 9, 2020 (ADAMS Accession No. ML20191A357). This draft SE was discussed with the Advisory Committee on Reactor Safeguards (ACRS) Kairos Power Subcommittee on September 24, 2020. The ACRS discussed the SE at a full committee meeting on October 9, 2020 and decided not to write a letter report on the TR. The NRC staff's final SE for TR KP-FHR Risk-Informed Performance-Based Licensing Basis Development Methodology (Revision 1) is enclosed.

If you have any questions, please contact Stewart Magruder at 301-348-5766 or by e-mail at Stewart.Magruder@nrc.gov.

Sincerely,

Benjamin G. Beasley, Chief
Advanced Reactor Licensing Branch
Division of Advanced Reactors and Non-Power
Production and Utilization Facilities
Office of Nuclear Reactor Regulation

Project No. 99902069

Enclosure:
Final SE

SUBJECT: FINAL SAFETY EVALUATION FOR KAIROS POWER LLC TOPICAL REPORT "KP-FHR RISK-INFORMED PERFORMANCE-BASED LICENSING BASIS DEVELOPMENT METHODOLOGY" (REVISION 1) (EPID NO. L-2019-TOP-0009/CAC NO. 000431) DATED: NOVEMBER 10, 2020

DISTRIBUTION:
E-MAIL
PUBLIC
SMagruder, NRR
RidsNrrDanuUarl Resource
RidsOgcMailCenter
RidsACRS_MailCTR
RidsNrrDanu Resource
RidsNrrLASLent Resource
RRivera, NRR
SCuadrado, NRR
MSpencer, OGC
IJung, NRR
ABarrett, NRR
WWang, ACRS
BBeasley, NRR
MHayes, NRR

----
gardner@kairospower.com
peebles@kairospower.com

ADAMS Accession No.: ML20294A337 ***via e-mail**

OFFICE	NRR/DANU/UARL/PM*	NRR/DANU/UARL/LA*	NRR/DANU/UART/BC*
NAME	SMagruder	SLent	MHayes
DATE	10/14/2020	10/22/2020	10/22/2020
OFFICE	OGC*	NRR/DANU/UARL/BC*	
NAME	MASpencer	BBeasley	
DATE	11/04/2020	11/10/2020	

OFFICIAL RECORD COPY

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

FINAL SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO TOPICAL REPORT "KP-FHR RISK-INFORMED PERFORMANCE-BASED

LICENSING BASIS DEVELOPMENT METHODOLOGY" (REVISION 1)

KAIROS POWER, LLC

PROJECT NO. 99902069

1.0 INTRODUCTION

By letter dated August 6, 2019 (Reference 5), Kairos Power LLC (Kairos Power, the applicant) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review, Topical Report (TR) "KP-FHR Risk-Informed Performance-Based Licensing Basis Development Methodology". On October 3, 2019 (Reference 2), the NRC staff found that the material presented in the TR provides technical information in sufficient detail to enable the staff to conduct a detailed technical review.

The applicant requested the NRC staff's review and approval to use the methodology presented in the TR to select the licensing basis events (LBEs) for, and classify the structures, systems, and components (SSCs) and assess the defense-in-depth (DID) adequacy of, a Fluoride-Salt-Cooled, High-Temperature Reactor (KP-FHR). The methodology would be used as part of safety analysis reports required by Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50 "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

As part of the NRC staff review, initial feedback and questions were provided to the applicant on January 8, 2020 (Reference 6), and March 19, 2020 (Reference 7). In response to these questions and a teleconference with the NRC staff, the applicant submitted Revision 1 of the TR on April 20, 2020 (Reference 12). This safety evaluation (SE) is based on Revision 1 of the TR.

2.0 REGULATORY EVALUATION

The regulations in 10 CFR 50.34, 10 CFR 52.47, 10 CFR 52.79, 10 CFR 52.137, and 10 CFR 52.157 contain the technical requirements for applications for a construction permit, operating license, standard design certification, combined license, standard design approval, and manufacturing license, respectively. The applicable portions of the regulations above require a safety analysis and an evaluation of the safety features and barriers to a radioactive release to be included in a preliminary or final safety analysis report (FSAR).

The safety features and barriers to a radioactive release are required by 10 CFR 50.34(a)(1)(ii)(D) to be evaluated to ensure that:

(1) An individual located at any point on the boundary of the exclusion area for any 2 hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 25 rem [Roentgen equivalent man] total effective dose equivalent (TEDE).

(2) An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem total TEDE.

This requirement is echoed for the FSAR in 10 CFR 50.34(b)(11) and for Part 52 licensing paths in 10 CFR 52.47(a)(2)(iv), 10 CFR 52.79(a)(1)(vi), 10 CFR 52.137(a)(2)(iv), 10 CFR 52.157(d).

In addition to addressing these regulations, the TR also addresses the quantitative health objectives (QHOs) in the NRC Safety Goal Policy Statement, 51 FR 30028, "Safety Goals for the Operations of Nuclear Power Plants," which are as follows:

- The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

- The risk to the population in the area of nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks resulting from all other causes.

Regulations in 10 CFR 50.2 define safety-related SSCs as those SSCs that are relied upon to remain functional during and following design basis events to assure:

(1) The integrity of the reactor coolant pressure boundary
(2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
(3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable.

Kairos Power intends to request an exemption from the first safety-related criterion above as discussed in another TR, "Principal Design Criteria for the Kairos Power Fluoride Salt-Cooled High Temperature Reactor," KP-TR-003, December 2018 (Reference 11). The TR under review in this SE does not provide a justification for a requested exemption, and the staff is not taking a position in this SE on whether such an exemption would be granted. The guidance in Nuclear Energy Institute (NEI) 18-04 provides a methodology to identify the SSCs that would fall under only the third criterion above. This TR explicitly adds the second criterion (SSCs that assure the capability to shut down the reactor and maintain it in a safe shutdown condition) to the definition of safety-related SSCs to ensure that the portions of the 10 CFR 50.2 definition for which Kairos does not intend to request an exemption are addressed.

The TR references Draft Regulatory Guide DG-1353 (Reference 1), which provided draft NRC staff guidance on using a technology-inclusive, risk-informed, and performance-based methodology to inform the licensing basis and content of applications for non-light water reactors (non-LWRs). The DG-1353 endorsed, with clarifications, NEI 18-04, Draft Report Revision N (Reference 3), as one acceptable method for non-LWR designers to use when carrying out these activities and preparing their applications. In December 2019, the NRC staff submitted to the Commission SECY-19-0117, "Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors." (Reference 8) The SECY paper requested that the Commission find that the staff's use of the technology-inclusive, risk-informed, and performance-based methodology described in the paper (referring to DG-1353 and NEI 18-04, Revision 1 (Reference 4)), is a reasonable approach to establish key parts of the licensing basis and content of applications for licenses, certifications, and approvals for non-LWRs. The Commission issued a Staff Requirements Memorandum (SRM) to SECY-19-0117 (Reference 9), which approves the use of the technology-inclusive, risk-informed, and performance-based methodology described in SECY-19-0117 as a reasonable approach for establishing key parts of the licensing basis and content of applications for licenses, certifications, and approvals for non-LWRs. Subsequently, DG-1353 was finalized and issued as Regulatory Guide (RG) 1.233, Revision 0 (Reference 10), which endorses with clarifications, NEI 18-04, Revision 1 as one acceptable method for non-LWR designers to use when carrying out these activities and preparing their applications.

This TR provides the applicant's methodology for LBE identification, SSC classification, and DID adequacy using the guidance in DG-1353 and NEI 18-04, Revision 1. As part of this review, the staff confirmed there is no significant change from DG-1353 to RG 1.233 or in the primary referenced document NEI 18-04, Revision N to NEI 18-04, Revision 1. The staff confirmed that the guidance and clarifications in DG-1353 and RG 1.233 are the same.

The methodology does not exempt licensing applicants of the KP-FHR design from applicable regulations, nor does it address all regulations applicable to nuclear power plants. Rather, the TR describes the methodology to inform the safety analysis report for the KP-FHR design, which demonstrates compliance with the regulations.

3.0 TECHNICAL EVALUATION

3.1 INTRODUCTION

This TR provides a KP-FHR-specific methodology for the selection of LBEs, classification and special treatment of SSCs, and assessment of DID adequacy, which are considered fundamental to the safe design of a nuclear reactor, including a non-LWR. The staff finds that this TR:

- Is based on NEI 18-04, Revision 1, (Reference 4) and DG-1353 (Reference 1) which has been finalized and issued as RG 1.233, Revision 0 (Reference 10). NEI 18-04, Revision 1, has been endorsed by the NRC staff via RG 1.233, Revision 0, with clarifications. The applicable clarifications have been incorporated into the TR;
- Is a customized version of the technology-inclusive NEI 18-04 methodology for the KP-FHR technology; and
- Deviates from NEI 18-04 with a limited number of minor differences that do not alter the principles and methodology of DG-1353 and NEI 18-04.

As a result, the NRC staff narrowed its review scope to assessing the differences between this TR and NEI 18-04 and confirming that this TR incorporates the applicable clarifications identified in RG 1.233. The NRC staff reviewed all the differences but primarily focused its review on those considered to be of some significance.

Since the TR is based on NEI 18-04 and guidance included in RG 1.233, statements from RG 1.233 regarding exemptions from NRC regulations apply. For example, the applicant's methodology defines and uses some terms in a manner that differs from NRC regulations. Thus, consistent with RG 1.233, an applicant referencing this TR is expected to "identify exceptions to and exemptions needed from NRC regulations," as needed. Also, as stated in RG 1.233, "system designs and safety evaluations may also demonstrate compliance with or justify exemptions from specific NRC regulations." The TR does not request approval of any exemptions and the staff is not approving any exemptions in this SE. Thus, the NRC staff is adding Item 1 in Section 4.0 of this SE, "Limitations and Conditions," to clarify that this SE is not approving any exemptions and that an applicant using this TR will need to address compliance with pertinent regulations and request exemptions as needed.

Appendix B of the TR includes a sample application of the KP-FHR methodology, which is outside the scope of the NRC staff's review.

3.2 STAFF EVALUATION OF THE METHODOLOGY

Licensing Basis Development Process (TR Section 2)

For this section, this TR makes minor deviations from and does not alter the principles and methodology in NEI 18-04. One of the deviations of note is that the terminology 'Safety Function' is used in the TR instead of Probabilistic Risk Assessment (PRA) Safety Function. This TR replaces the following in NEI 18-04:

"The LBEs are defined in terms of successes and failures of SSCs that perform safety functions modeled in the PRA, hereafter referred to as PRA Safety Functions (PSFs). PSFs are defined as those functions responsible for the prevention and mitigation of an unplanned radiological release from any source within the plant."

With:

"The LBEs are defined in terms of successes and failures of SSCs that perform Safety Functions (SFs). The SFs are defined as those functions responsible for the prevention and mitigation of an unplanned radiological release from any source within the plant."

The NRC staff finds this deviation to be minor because the definitions of Safety Function in this TR and PRA Safety Function in NEI 18-04 are essentially the same and the deviation does not change the principles and methodology of NEI 18-04.

The NRC staff reviewed TR Section 2 and found it acceptable because it is essentially the same as NEI 18-04.

Selection of Licensing Basis Events (TR Section 3)

In describing Task 7a (Evaluate LBEs Against F-C Target) of Figure 3.2, this TR replaces the following text in NEI 18-04

"The upper bound consequences for each DBA, defined as the 95th percentile of the uncertainty distribution, shall meet the 10 CFR 50.34 dose limit at the EAB [exclusion area boundary]."

With:

"The upper bound consequences for each DBA shall meet the 10 CFR 50.34 dose limit at the EAB. Justification that the DBA evaluation models are sufficiently bounding may be based on qualitative arguments rather than direct calculation of 95th percentile figures of merit. This justification will be provided in future licensing submittals."

The applicant deviates from NEI 18-04 in that it allows for the use of qualitative arguments instead of quantitative calculation of uncertainty for determining the bounding consequences of each design basis accident (DBA). The applicant proposes to justify that the DBA evaluation models are sufficiently bounding using future licensing submittals. The NRC staff finds it reasonable from a methodology perspective, as this TR is intended, because the staff will have a future opportunity to assess the acceptability of any qualitative arguments. The staff is not now making a finding on the acceptability of potential future qualitative arguments from a technical perspective.

In the TR, Section 3.3.6, "Contributors to Risk and Risk Importance Measures," uses the risk reduction importance measure, among the various importance measures listed in NEI 18-04 to assess risk significance of PRA basic events. The risk reduction measure is compared to 1 percent of each of the cumulative risk metrics as in TR Table 3-1. Regarding the use of risk reduction importance measure, the staff finds it reasonable because it is an element of the integrated risk informed performance based (RIPB) approach in the TR, which is expected to determine a reasonable set of risk- or safety-significant SSCs and associated special treatments.

The staff notes, however, that the Joint Committee on Nuclear Risk Management (JCNRM) of the American Nuclear Society/American Society of Mechanical Engineers (ANS/ASME) is developing a PRA standard for non-LWRs. The NRC staff is expected to review this standard after publication to determine whether to endorse the standard via a Regulatory Guide. The standard may define risk significance of SSCs differently from this TR. Licensing applicants referencing this TR should address, or justify alternatives to, the acceptance criteria in a possible future Regulatory Guide and endorsed standard related to the determination of risk significance of SSCs. Accordingly, the NRC staff included Item 2 in Section 4.0 of this SE, "Limitations and Conditions," to clarify that licensing applicants referencing this TR should address, or justify alternatives to, the acceptance criteria in such an RG and endorsed standard related to the determination of risk significance of SSCs if the RG is issued at least 6 months before submission of the license application.

Safety Classification and Performance Criteria for SSCs (TR Section 4)

This TR proposes the definition of the safety-related SSCs to be as follows:

- SSCs relied on to perform the required safety function (RSF)s to mitigate the consequences of design basis event (DBE)s to within the LBE F-C Target, and to mitigate DBAs that only rely on the safety-related SSCs to meet the dose limits of 10 CFR 50.34 using conservative assumptions.

- SSCs relied on to perform RSFs to prevent the frequency of beyond design basis event (BDBE) with consequences greater than the 10 CFR 50.34 dose limits from increasing into the DBE region and beyond the F-C Target.

- SSCs relied on to shut down the reactor and maintain it in a safe shutdown condition.

The first two criteria are the same as those in NEI 18-04; however, this TR adds a third criterion that is the same as the second criterion in the definition of "safety-related" in 10 CFR 50.2. The addition is to ensure that the definition in 10 CFR 50.2, "Definitions," is addressed, with the exception of the portion of this definition for which Kairos plans to request an exemption. The applicant's definition adds a traditionally used criterion for a set of SSCs performing reactor shutdown function in addition to the criteria in NEI 18-04. The NRC staff finds that the applicant's proposal to add the third criterion is acceptable since the prescriptive criterion is consistent with the regulations and has the potential to increase the number of safety-related SSCs beyond those identified by the two other criteria.

Evaluation of Defense-In-Depth Adequacy (TR Section 5)

Under TR Section 5.7, "Evaluation of LBEs against Layers of Defense," Kairos Power included the following:

"NEI 18-04 contains some general guidance in Section 5.7 for defense in depth layers and source term that do not translate to specific actions or documentation for this process. Detail on the mechanistic source term approach for the KP-FHR will be provided as part of future licensing submittals."

The applicant proposes to justify the mechanistic source term approach for the KP-FHR using future licensing submittals. The NRC staff finds this reasonable from a methodology perspective because the staff will have a future opportunity to assess the acceptability of the mechanistic source term approach. The staff is not now making a finding on the acceptability of the mechanistic source term approach from a technical perspective.

Under TR Section 5.8.1, "Guidelines for Programmatic DID Adequacy," Kairos Power deviates from the objectives of the programmatic DID adequacy in NEI 18-04. Specifically, the TR replaces the following in NEI 18-04:

- Assuring that appropriate targets for SSC reliability and performance capability are reflected in design and operational programs for each LBE

- Providing adequate assurance that the risk, reliability, and performance targets will be met and maintained throughout the life of the plant with adequate consideration of sources of significant uncertainties

With:

- Providing adequate assurance that the risk, reliability, and performance margins are maintained throughout the life of the plant in design and operational programs with adequate consideration of sources of significant uncertainties

The TR states:

"These objectives differ slightly from the objectives stated in NEI 18-04. The Kairos Power approach to establishing programmatic DID adequacy focuses activities on assuring that frequency targets are maintained at the event sequence level. At the more detailed SSC level, the focus shifts to performance-based measures such as surveillance frequency and test success rates."

The NRC staff finds the deviation acceptable because the programmatic DID adequacy can be effectively addressed with targets for reliability at the event sequence level while detailed performance-based measures are used at the individual SSC level.

4.0 LIMITATIONS AND CONDITIONS

The staff imposes the following limitations and conditions with regard to the TR:

1. (**Section 3.1)** This SE does not approve any exemptions from NRC regulations, and an applicant using this TR will need to address compliance with pertinent regulations and request exemptions as needed.

2. (**Section 3.3.6)** The JCNRM of the ANS/ASME is developing a PRA standard for non-LWRs. If the NRC staff concludes that the ANS/ASME PRA standard is acceptable, the staff expects to endorse the standard via a Regulatory Guide. If the Regulatory Guide is issued 6 months before submission of the licensing application, the applicant should address, or justify alternatives to, the acceptance criteria in the Regulatory Guide and endorsed PRA standard related to the determination of risk significance of SSCs as a part of implementing the methodology in this TR.

5.0 CONCLUSION

Based on the above evaluation, the NRC staff concludes that the applicant has provided an acceptable KP-FHR design-specific risk-informed, performance-based methodology for LBE selection, classification and special treatments of SSCs, and assessment of DID adequacy to inform the licensing basis and content of licensing applications under 10 CFR Parts 50 and 52 for the KP-FHR design, subject to the limitations and conditions above. In summary, this conclusion is based on (1) the methodology being essentially the same as NRC staff-approved NEI 18-04, Revision 1, and incorporating the applicable clarifications and points of emphasis from RG 1.233, Revision 0 and (2) the differences between this TR and NEI 18-04 have been evaluated to be reasonable as described in Section 3.0.

6.0 REFERENCES

1. U.S. Nuclear Regulatory Commission, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," Draft Regulatory Guide DG-1353, dated April 2019 (ADAMS Accession No. ML18312A242)

2. U.S. Nuclear Regulatory Commission, "Kairos Power LLC - Acceptance Of "KP-FHR Risk-Informed Performance-Based Licensing Basis Development Methodology" Topical Report (CAC NO. 000431)," dated October 23, 2019 (ADAMS Accession No. ML19284D767)

3. Nuclear Energy Institute, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," NEI 18-04, Draft Report Revision N, dated September 28, 2018 (ADAMS Accession No. ML18271A172)

4. Nuclear Energy Institute, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," NEI 18-04, Revision 1, dated August 2019 (ADAMS Accession No. ML19241A472)

5. Kairos Power LLC, "KP-FHR Risk-Informed Performance-Based Licensing Basis Development Methodology Topical Report.", KP-TR-009, Revision 0, dated August 6, 2019 (ADAMS Accession No. ML19217A420)

6. Email, Nuclear Regulatory Commission Stewart Magruder to Darrell Gardner, "Discussion Items on Kairos Risk-Informed Performance-Based Licensing Basis Development Methodology Topical Report" (KP-TR-009)," dated January 8, 2020 (ADAMS Accession No. ML20009E836)

7. Email, Nuclear Regulatory Commission Stewart Magruder to Drew Peebles and Darrell Gardner, "Discussion Items on Kairos LMP topical," dated March 19, 2020 (ADAMS Accession No. ML20104A041)

8. U.S. Nuclear Regulatory Commission, SECY-19-0117, "Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors" dated December 2, 2019 (ADAMS Accession No. ML18312A253)

9. U.S. Nuclear Regulatory Commission, SRM to SECY-19-0117, "Staff Requirements – SECY-19-0117 – Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors" dated May 26, 2020 (ADAMS Accession No. ML20147A504)

10. Regulatory Guide 1.233, Revision 0, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," dated June 2020 (ADAMS Accession No. ML20091L698)

11. Kairos Power LLC, letter KP-NRC-1907-006, P. Hastings, Vice President, Regulatory Affairs and Quality, to USNRC document control desk, re: "Principal Design Criteria for the Kairos Power Fluoride Salt-Cooled, High Temperature Reactor (Revision 1)," dated July 31, 2019 (ADAMS Accession No. ML19212A756)

12. Kairos Power LLC, "KP-FHR Risk-Informed Performance-Based Licensing Basis Development Methodology Topical Report.", KP-TR-009, Revision 1, dated April 10, 2020 (ADAMS Accession No. ML20101P623)

Principal Contributors: Ian Jung, NRR
Antonio Barrett, NRR

Date: November 10, 2020

Section B

LICENSING DOCUMENT APPROVAL SHEET

KP-FHR Risk-Informed Performance-Based Licensing Basis Development Methodology Topical Report

Document Approval			
Name	Function	Date	Signature
Drew Peebles	Preparer		
Matt Warner	Reviewer		
Jordan Hagaman	Reviewer		
Darrell Gardner	Approver		

KP-TR-009-NP-A

Kairos Power LLC
707 W. Tower Ave
Alameda, CA 94501

KP-FHR Risk-Informed Performance-Based Licensing Basis Development Methodology

Topical Report

Revision No. 1
Document Date: April 2020

Non-Proprietary

Rev	Description of Change	Date
0	Initial Issuance	August 2019
1	Revision 1 incorporates changes to the topical report content initiated by conversations with the NRC during a phone call on 1/30/20. Changes include: • Direct responses to NRC questions produced changes in Sections: 3.1, 3.2.2, 3.3.6, 4.0, 4.1, 4.3, 4.4.5, 5.3, 5.7, 5.8.1, 5.9.3, and Table 5-6 • In discussion with the NRC, Kairos committed to review Revision 1 of NEI 18-04 and make associated changes. This resulted in changes to Sections: 3.2.2, 5.3, 5.6.1, 5.6.2, 5.7, 5.8.1, 5.8.2, Table 5-7, and Appendix A • The NRC review staff sent additional comments following a call on 3-19-20 that resulted in changes to Sections: "Executive Summary", 1.1, 1.3.1, 1.4, 3.2.1, 3.2.2, 3.2.3, 3.3, 3.3.4, 3.3.5, 4.1, 4.4.2, 5.3, 5.9.3, 6, 7, Appendix A, B.2.4, B.2.7, B.2.9 • During the review period, Kairos Power self-identified changes in Sections: 3.2.2, 3.3, 4.1, 5.3, Figure 3-3, Figure 4-2 and Figure 5-4.	April 2020

Executive Summary

This document describes the risk-informed performance-based methodology that develops the following portions of the KP-FHR licensing basis: licensing basis event (LBE) identification, the classification of structures, systems, and components (SSCs), and the defense in depth (DID) adequacy. The methodology was developed as part of the industry-led Licensing Modernization Project (LMP), which was created to develop technology-inclusive, risk-informed, and performance based regulatory guidance for licensing non-light water reactors. The LMP guidance was documented in an NEI 18-04, “Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development”. The US Nuclear Regulatory Commission (NRC) prepared a draft regulatory guide, DG-1353 “Guidance for a technology-inclusive, risk-informed, and performance-based approach to inform the content of applications for licenses, certifications, and approvals for non-light-water reactors” for public comment that endorses the guidance in NEI 18-04. This topical reproduces the NEI 18-04 content with minor technology-specific changes to the risk-informed, performance-based guidance, to assert the methodology as applicable to the KP-FHR.

The LBE selection methods provide a systematic definition, categorization, and evaluation of event sequences for selection of LBEs, which include Anticipated Operational Occurrences (AOOs), Design Basis Events (DBEs), Design Basis Accidents (DBAs), and Beyond Design Basis Events (BDBEs). The methodology provides a systematic method for defining the events in terms of frequency and consequence. Using this method, the selected LBEs adequately cover the range of hazards that a KP-FHR could be exposed to and reflect the impacts of SSC failure modes. This method ensures the LBEs are defined in terms of successes and failures of SSCs that perform RSFs (required safety functions responsible for the prevention and mitigation of an unplanned radiological release from any source within the plant). This portion of the methodology is illustrated by a sample LBE provided in an appendix to this report. Although Kairos Power is not asking NRC approval of the sample LBE, the example is provided as an illustration of the methodology.

The methodology also provides a systematic process for safety classification of SSCs, development of performance requirements, and application of special treatments. These methods are integrated with the LBE selection process because the frequency-consequence targets and limits on the LBEs rely on the functionality of certain SSCs. The SSCs are then classified as Safety-Related, Nonsafety-Related with Special Treatment, or Nonsafety-Related. The methodology ensures that the SSCs that perform RSFs are adequately capable, reliable, diverse, and/or redundant across the layers of defense in the design.

The DID adequacy evaluation process is considered and incorporated into various phases of the licensing process. The DID evaluation methodology ensures that adequate layers of defense are in place to ensure the LBE consequences are within regulatory limits. The DID methods also ensure that appropriate targets for SSC reliability and performance capability are reflected in design and operational programs for each LBE.

Kairos Power is requesting NRC review and approval of the methodology in this topical report as an appropriate method to develop licensing basis events, classify SSCs, and ensure DID adequacy as part of safety analysis reports required to be submitted in licensing applications to satisfy the applicable regulations in 10 CFR 50 and 10 CFR 52.

Table of Contents

List of Figures

List of Tables

ABBREVIATIONS

Abbreviation or Acronym	Definition
ANS	American Nuclear Society
AOO	Anticipated Operational Occurrence
ASME	American Society of Mechanical Engineers
BDBE	Beyond Design Basis Event
CFR	Code of Federal Regulations
DBA	Design Basis Accident
DBE	Design Basis Event
DBEHL	Design Basis External Hazard Level
DID	Defense-in-Depth
EAB	Exclusion Area Boundary
EPA	Environmental Protection Agency
ES	Event Sequence
F-C	Frequency-Consequence
FDC	Functional Design Criteria
FMEA	Failure Modes and Effects Analysis
FSAR	Final Safety Analysis Report
FSF	Fundamental Safety Function
HAZOP	Hazard and Operability Study
IAEA	International Atomic Energy Agency
IDP	Integrated Decision-Making Panel
IE	Initiating Event
LBE	Licensing Basis Event
LMP	Licensing Modernization Project
LWR	Light Water Reactor
MHTGR	Modular High-Temperature Gas-Cooled Reactor
MST	Mechanistic Source Term
NEI	Nuclear Energy Institute

Abbreviation or Acronym	Definition
NRC	Nuclear Regulatory Commission
NSRST	NonSafety-Related with Special Treatment
NST	NonSafety-Related with No Special Treatment
O&M	Operations and Maintenance
PAG	Protective Action Guide
PB	Performance-Based
PHA	Process Hazard Analysis
PIRT	Phenomena Identification and Ranking Table
POS	Plant Operating State
PRA	Probabilistic Risk Assessment
SF	Safety Function
QHO	Quantitative Health Objective
RAP	Reliability Assurance Program
RCPB	Reactor Coolant Pressure Boundary
REM	Roentgen Equivalent Man
RFDC	Required Functional Design Criteria
RG	Regulatory Guide
RI	Risk-Informed
RIPB	Risk-Informed and Performance-Based
RIPB-DM	Risk-Informed and Performance-Based Decision-Making
RSF	Required Safety Function
SR	Safety-Related
SRDC	Safety-Related Design Criteria
SRP	Standard Review Plan (NUREG-0800)
SSC	Structures, Systems, and Components
ST	Special Treatment
TEDE	Total Effective Dose Equivalent
TRISO	Tristructural Isotropic

1 INTRODUCTION

1.1 PURPOSE

Kairos Power LLC (Kairos Power) is pursuing the design, licensing, and deployment of a Fluoride-Salt-Cooled, High-Temperature Reactor (KP-FHR). To enable these objectives, a risk-informed, performance-based methodology developed through the Licensing Modernization Project (an industry-led initiative to develop technology-inclusive, risk-informed, and performance based regulatory guidance for licensing non-light water reactors) is used to define licensing basis events (LBEs), provide safety classifications for structures, systems, and components (SSCs), and assess the defense-in-depth (DID) adequacy of the KP-FHR.

Kairos Power is requesting U.S. Nuclear Regulatory Commission (NRC) review and approval to use the methodology presented in this report to define the LBEs, to classify the SSCs, and to assess the DID adequacy of the KP-FHR as part of safety analysis reports required to be submitted to meet the associated requirements for content of licensing applications required in 10 Code of Federal Regulations (CFR) 50.34(a), 10 CFR 50.34(b), 10 CFR 52.47, 10 CFR 52.79, 10 CFR 52.137, and 10 CFR 52.157. A sample licensing basis event (LBE) evaluation is provided in Appendix B to illustrate the methodology. This sample LBE evaluation does not represent final KP-FHR design information and is only intended to be an illustration of the methodology in application. Kairos Power is not requesting NRC approval of the design information presented in Appendix B.

1.2 BACKGROUND

The NRC communicated their expectations for advanced reactors in the 2008 NRC Policy Statement on the Regulation of Advanced Reactors, [73 FR 60612; ADAMS ML082750370],

> *"…the Commission expects that advanced reactors will provide enhanced margins of safety and/or use simplified, inherent, passive, or other innovative means to accomplish their safety and security functions."*

The NRC intends to achieve its mission through adherence to the principles of good regulation—independence, openness, efficiency, clarity, and reliability. The NRC staff noted in "Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident" that the current nuclear regulatory infrastructure was:

> *"…developed for the purpose of reactor licensing in the 1960s and 1970s and supplemented as necessary to address significant events or new issues."*

To modernize the nuclear regulatory infrastructure, in 1995 the Commission published "Final Policy Statement on the Use of Probabilistic Risk Assessment [PRA] Methods in Nuclear Regulatory Activities," [60 FR 42622; ADAMS ML021980535] which states in part:

> *"The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy."*

This document builds on these policy statements by providing a foundation upon which a more fully risk-informed and performance-based technical licensing environment can be developed while allowing the current regulatory framework to be used.

1.3 DESIGN FEATURES

1.3.1 Design Background

To facilitate the NRC review of this topical report, key design features are described in Section 1.3.2 which are considered inherent to the KP-FHR technology. These features are not expected to change during the design development by Kairos Power and provide the basis to support the safety review of the methodology provided in this report. Should fundamental changes occur regarding these key design features or revised regulations be promulgated, the changes would be reconciled and addressed in future licensing application submittals.

The KP-FHR is a U.S. developed Generation IV advanced reactor technology. In the last decade, U.S. national laboratories and universities have developed pre-conceptual FHR designs with different fuel geometries, core configurations, heat transport system configurations, power cycles, and power levels. More recently, the University of California at Berkeley developed the Mark 1 pebble-bed FHR incorporating lessons learned from the previous decade of FHR pre-conceptual designs. Kairos Power has built on the foundation laid by U.S. Department of Energy sponsored university Integrated Research Projects to develop the KP-FHR.

Although not intended to support the findings necessary to approve this topical report, additional design and testing concept information is provided in the “Design Overview of the Kairos Power Fluoride Salt Cooled, High Temperature Reactor” Technical Report (Reference 1) and the “Testing and Development Program Overview for the Kairos Power Fluoride Salt Cooled, High Temperature Reactor” Technical Report (Reference 2).

1.3.2 Key Design Features of the KP-FHR

The KP-FHR is a high-temperature reactor with molten fluoride salt coolant operating at near-atmospheric pressure. The fuel in the KP-FHR is based on the tristructural isotropic (TRISO) high-temperature carbonaceous-matrix coated particle fuel developed for high-temperature gas-cooled reactors, in a pebble fuel element. Coatings on the particle fuel provide retention of fission products. The reactor coolant is a chemically stable molten fluoride salt mixture, $2{\cdot}LiF{:}BeF_2$, which also provides retention of fission products that escape from fuel defects. A primary coolant loop circulates the reactor coolant using pumps and transfers the heat to an intermediate coolant loop via a heat exchanger. The pumped flow intermediate coolant loop utilizes a nitrate salt and transfers heat from the reactor coolant to the power conversion system through a steam generator. The design includes two decay heat removal systems. A normal decay heat removal system is used following normal shutdowns and anticipated operational occurrences (AOOs). A separate passive decay heat removal system, which along with natural circulation in the reactor vessel, is used to remove decay heat in response to a loss of the normal decay removal system and does not rely on electrical power.

The KP-FHR design relies on a functional containment approach similar to the Modular High Temperature Gas-Cooled Reactor (MHTGR) instead of the typical light water reactor (LWR) low-leakage, pressure retaining containment structure. The KP-FHR functional containment safety design objective is to meet 10 CFR 50.34 (10 CFR 52.79) offsite dose requirements at the plant's exclusion area boundary with margin. A functional containment is defined in Regulatory Guide 1.232 revision 0, "*Developing Principal Design Criteria for Non-Light Water Reactors*," as a "barrier, or set of barriers taken together, that effectively limit the physical transport and release of radionuclides to the environment across a full range of normal operating conditions, AOOs, and accident conditions." RG 1.232 includes an example design criterion for the functional containment (MHTGR Criterion 16). As also stated in RG 1.232, the NRC has reviewed the functional containment concept and found it "generally acceptable," provided that "appropriate performance requirements and criteria" are developed. The NRC staff has developed a proposed methodology for establishing functional containment performance criteria for non-LWRs, which is presented in SECY-18-0096, "*Functional Containment Performance Criteria for Non-Light-Water-Reactors.*" This SECY document has been approved by the Commission.

The functional containment approach for the KP-FHR is to control radionuclides primarily at their source within the coated fuel particle under normal operations and accident conditions without requiring active design features or operator actions. The KP-FHR design relies primarily on the multiple barriers within the TRISO fuel particles and fuel pebbles to ensure that the dose at the site boundary as a consequence of postulated accidents meets regulatory limits. However, in the KP-FHR as opposed to the MHTGR, the molten salt coolant serves as a distinct barrier providing retention of fission products that escape the fuel particle and fuel pebble barriers. This additional retention is a key feature of the enhanced safety and reduced source term in the KP-FHR.

1.4 REGULATORY INFORMATION

Applicants are anticipated to pursue a licensing application for the KP-FHR under Title 10 of the Code of Federal Regulations (10 CFR) using a licensing pathway provided in Part 50 or Part 52. Regardless of the licensing path, there are associated requirements to provide a safety analysis and evaluate the potential dose consequences of the design. The applicable portion of 10 CFR 50.34(a)(4) provides the requirement for a safety analysis to be performed by an applicant submitting a preliminary safety analysis report:

> A preliminary analysis and evaluation of the design and performance of structures, systems, and components of the facility with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of structures, systems, and components provided for the prevention of accidents and the mitigation of the consequences of accidents.

This requirement is echoed for the final safety analysis report (FSAR) in 10 CFR 50.34(b)(4) and for Part 52 licensing paths in 10 CFR 52.47(a)(4), 10 CFR 52.79(a)(5), 10 CFR 52.79(b)(4), 10 CFR 52.137(a)(4), and 10 CFR 52.157(f)(1).

The safety features and barriers to a radioactive release are required by 10 CFR 50.34(a)(1)(D) to be evaluated to ensure that:

> (1) An individual located at any point on the boundary of the exclusion area for any 2 hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).

(2) An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem total TEDE.

This requirement is echoed for the FSAR in 10 CFR 50.34(b)(1) and for Part 52 licensing paths in 10 CFR 52.47(a)(2)(iv), 10 CFR 52.79(a)(1)(vi), 10 CFR 52.137(a)(2)(iv), 10 CFR 52.157(d).

Additionally, the quantitative objectives identified in the Safety Goal Policy Statement, 51 FR 28044, "*Safety Goals for the Operations of Nuclear Power Plant*," are evaluated. These goals are as follows:

- The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

- The risk to the population in the area of nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks resulting from all other causes.

10 CFR 50.2 defines safety-related SSCs as those SSCs that are relied upon to remain functional during and following design basis events to assure:

(1) The integrity of the reactor coolant pressure boundary
(2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
(3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable.

Kairos Power intends to take an exemption to the first safety-related criterion as discussed in Reference 10. The guidance in Nuclear Energy Institute (NEI) 18-04 provides a methodology to identify the SSCs that would fall under the third criterion. This topical report explicitly adds the second criterion (SSCs that assure the capability to shut down the reactor and maintain it in a safe shutdown condition) to the definition of safety-related SSCs to ensure that the 10 CFR 50.2 definition is addressed.

Draft regulatory guide 1353 (DG-1353), "*Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Approach to inform the Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors*" provides the NRC endorsed guidance to select LBEs, classify SSCs, and provide appropriate DID for non-light water reactor designs. DG-1353 endorses, with clarifications, the principles and methodology in NEI 18-04, "*Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development* (Reference 3)*.*" The methodology described in NEI 18-04 is also referred to as the Licensing Modernization Project (LMP) methodology.

This report provides the KP-FHR methodology for LBE identification, SSC classification, and DID adequacy using the guidance in DG-1353 and NEI 18-04. Kairos Power is requesting NRC review and approval of this methodology for use by licensing applicants for a KP-FHR as an acceptable means to:

- define the KP-FHR LBEs that will be used in safety analysis reports required for licensing applications in 10 CFR 50.34 (a)(4) and 10 CFR 50.34(b)(4) to meet the dose requirements of 10 CFR 50.34(a)(1)(D) and 10 CFR 50.34(b)(1) and the quantitative safety goals set by the NRC; as well as approval for use under the associated requirements for other licensing application paths in 10 CFR 52 cited above

- classify safety-related SSCs in a manner consistent with the definitions provided in 10 CFR 50.2

- assess the defense in depth adequacy of the KP-FHR plant capabilities and programmatic controls

This methodology does not exempt Kairos Power, or other licensing applicants for the KP-FHR, from existing regulations, nor does the process address all regulations applicable to nuclear power plants. Rather, the process describes the methodology to inform the safety analysis report for the KP-FHR design which demonstrates compliance with the regulations.

2 LICENSING BASIS DEVELOPMENT PROCESS

The overall objective of this report is to describe a systematic and reproducible process for selection of LBEs, classification of SSCs, and determination of DID adequacy such that different knowledgeable parties would come to like conclusions. These outcomes are important to the development of KP-FHR applications for licenses, certifications, or approvals and to the development of the facility design and operation. The process facilitates a systematic and iterative process for completion of tasks as the design progresses, providing immediate feedback to make better informed decisions.

This section includes descriptions of the following risk-informed performance-based (RIPB) processes:

- Systematic definition, categorization, and evaluation of event sequences for selection of LBEs, which include AOOs, Design Basis Events (DBEs), Design Basis Accidents (DBAs), and Beyond Design Basis Events (BDBEs)
- Systematic safety classification of SSCs, development of performance requirements, and application of special treatments (ST)
- Guidelines for evaluation of DID adequacy

These processes are:

- Risk-informed to fully utilize the insights from systematic risk assessment in combination with structured prescriptive rules to address the uncertainties which are not addressed in the risk assessment. This approach provides reasonable assurance that adequate protection is provided for public radiological protection.
- Performance-based to evaluate effectiveness relative to realizing desired outcomes that are achieved by using quantifiable performance metrics for LBE frequencies and consequences and performance requirements for SSC capabilities to prevent and mitigate events. This is an alternative to a prescriptive approach specifying particular features, actions, or programmatic elements to be included in the design or process as the means for achieving desired objectives.

This methodology is used to:

- Develop logical, coherent, and complete bases for the development of the safety design and evaluation of the safety design.
- Apply a sound PRA, including appropriate probabilistic models based on available standards, to develop and evaluate the facility design and operation.
- Answer the following broad questions:

  What are the plant Initiating Events and event sequences that are associated with the design?

How does the proposed design and its SSCs respond to Initiating Events and event sequences?

What are the margins provided by the facility's response, as it relates to prevention and mitigation of radiological releases within prescribed limits in the protection of public health and safety?

Is the philosophy of DID adequately reflected in the design and operation of the facility?

The outcomes of the processes support a risk-informed and performance-based (RIPB) safety basis for the design and a safety-focused application for NRC review by systematically demonstrating that:

- The selected LBEs adequately cover the range of hazards and reflect the impacts of SSC failure modes.
- The LBEs are defined in terms of successes and failures of SSCs that perform Safety Functions (SFs). SFs are defined as those functions responsible for the prevention and mitigation of an unplanned radiological release from any source within the plant.
- Collectively, the SSCs that perform the SFs are adequately capable, reliable, diverse, and/or redundant across the layers of defense in the design.
- The philosophy of DID is apparent in the design and programmatic features included in the licensing application and outcomes of systematic evaluations of DID adequacy. The DID evaluation focus is to assure adequate layers of defense.
- Sufficient and integrated design decisions are made, reconciling plant capabilities and programmatic capabilities based on risk-informed insights with respect to providing reasonable assurance of adequate protection.
- The scope and level of detail for plant SSCs and programmatic controls included in applications are commensurate with their safety and risk significance.

The processes covered in this report are integrated and highly interdependent, starting with the process for the selection of LBEs.

This report is organized as follows to support implementation:

- Section 3 provides a description of the LBE selection and evaluation process.
- Section 4 provides a description of SSC classification process and derivation of performance requirements.
- Section 5 provides a description of the DID adequacy determination process.

3 SELECTION OF LICENSING BASIS EVENTS

3.1 LICENSING BASIS EVENT DEFINITIONS

NRC regulatory requirements for a reactor design refer to several different kinds of events included within the licensing basis, comprising AOOs, DBEs, DBAs, and BDBEs. The definitions of these terms (see Appendix A) are intended to establish transparent and consistent quantification of existing terms without changing their intent or expected use.

For normal operations and AOOs, the NRC regulations are, for the most part, generic and applicable to KP-FHR, as discussed in Reference 11. Historically the off-normal events considered within the design basis are classified as either an AOO or a DBA based on a list of historically considered events for light water reactors (LWRs) and with subjective assessment of the expected frequency of occurrence. For KP-FHR, the prescriptive lists of generic LWR events may not be applicable. Therefore, the following systematic process is provided to derive the appropriate list of LBEs to assist with meeting the requirements.

In this document, Licensing Basis Events are defined in terms of event sequences comprised of an Initiating Event, the plant response to the Initiating Event (which includes a sequence of successes and failures of mitigating systems) and a well-defined end state. The term “event sequence” is used in lieu of the term “accident sequence” used in LWR PRA standards because the scope of the LBEs includes Anticipated Operational Occurrences and Initiating Events with no adverse impacts on public safety. The only use of the term “accident” in the LMP process is with the term “Design Basis Accident,” which is one of the LBE categories developed for the safety analysis report. It is recognized that some design and licensing requirements (e.g., definition of the safe shutdown earthquake) are defined for individual events rather than event sequences.

3.2 LBE SELECTION APPROACH

3.2.1 Frequency–Consequence Evaluation Criteria

Based on insights from the review of existing regulatory criteria, this approach uses a set of frequency–consequence criteria; this frequency–consequence evaluation correlation, hereafter referred to as the F-C Target, is shown in Figure 3-1.

The F-C Target in this figure is based on the following considerations:

- LBE categories are based on mean event sequence frequency of occurrence per plant-year. AOOs are off-normal events that are expected to occur in the life of the plant with frequencies exceeding 10^{-2}/plant-year, where a plant may be comprised of multiple reactor units. DBEs are less frequent events that may be expected to occur with frequencies between 10^{-4} to 10^{-2}/plant-year. BDBEs are rare events with frequencies less than 10^{-4}/plant-year but with upper bound frequencies greater than 5×10^{-7}/plant-year. LBEs may or may not involve release of radioactive material and may involve two or more reactor units or radionuclide sources.

- The regions of the graph separated by the frequency-dose evaluation line are identified as “Increasing Risk” and “Decreasing Risk” to emphasize that the purpose of the criteria is to evaluate the risk significance of individual AOOs, DBEs, and BDBEs, and to recognize that risk evaluations are not performed on a pass-fail basis, in contrast with deterministic safety evaluation criteria. This change is consistent with NRC risk-informed policies such as those expressed in Regulatory Guide 1.174 Revision 3, "*An Approach For Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis*," in which risk insights are used along with other factors within an integrated decision-making process.

- The F-C Target values shown in the figure are not considered as a demarcation of acceptable and unacceptable results. The F-C Target provides a general reference to assess events, SSCs, and programmatic controls in terms of sensitivities and available margins.

- The F-C Target for high-frequency AOOs down to a frequency of 10^{-1}/plant-year are based on an iso-risk profile defined by the annual exposure limits of 10 CFR 20, i.e., 100 mrem/plant-year.

- The F-C Target for lower frequency AOOs at frequencies of 10^{-1}/plant-year down to 10^{-2}/plant-year are set at a reference value of 1 rem corresponding with the Environmental Protection Agency (EPA) Protective Action Guide (PAG) limits and consistent with the goal of avoiding the need for offsite emergency response for any AOO. Many LBEs do not result in the release any radioactive material, and the identification of plant capabilities to prevent such releases is a factor considered in the formulation of SSC safety classification and performance requirements.

- The F-C Target for DBEs range from 1 rem at 10^{-2}/plant-year to 25 rem at 10^{-4}/plant-year with the dose calculated at the Exclusion Area Boundary (EAB) for the 30-day period following the onset of the release. This aligns the lowest frequency DBEs to the limits in 10 CFR 50.34 and provides continuity to the lower end of the AOO criteria. A straight line on the log-log plot connects these criteria. The identification of plant capabilities to prevent releases is a factor considered in the formulation of SSC safety classification and performance requirements.

- The F-C Target for the BDBEs range from 25 rem at 10^{-4}/plant-year to 750 rem at 5×10^{-7}/plant-year to ensure that the Quantitative Health Objective (QHO) for early health effects is not exceeded for individual BDBEs. The question of meeting the QHOs for the integrated risks over all the LBEs is addressed using separate cumulative risk targets described later in this report.

- The frequency-dose anchor points used to define the shape of the curve are indicated in the figure. The lines between the anchor points are straight lines on a log frequency vs. log dose graph.

- The F-C Target used in Figure 3-1 provides the basis for establishing the risk significance of LBEs.

- Event sequences with frequencies less than 5×10^{-7}/plant-year are retained in the PRA results and used to confirm there are no cliff edge effects. They are also taken into account in the RIPB evaluation of defense-in-depth.

Across the spectrum of AOOs, DBEs, and BDBEs on the F-C chart, the F-C Target is selected such that the risk, defined as the product of the frequency and consequence, does not increase as the frequency decreases. In addition, the principle of risk aversion (reduced frequencies as consequences increase) is applied at frequencies below 10^{-2}/plant-year. The evaluation of the consequences of all LBEs is supported by mechanistic source terms.

While interpreting the 10 CFR 20 annual exposure limits of 100 mrem/year, it is recognized that the use of this criteria in developing the F-C Target is to be applied to individual LBEs. To establish an aggregate risk measure including AOOs and other lower consequence events, the LBE process includes an activity to assure that the total frequency of exceeding 100 mrem summed over all the AOOs, DBEs, and BDBEs does not exceed 1/plant-year. This limit serves to control the risks in the high-frequency low-consequence end of the event spectrum, while the NRC safety goal QHO cumulative risk targets are most effective in controlling the low-frequency, high-consequence end of the spectrum. The LBE approach also includes performance of an integrated assessment over all the LBEs to ensure that NRC safety goal QHOs for both early and latent health effects are met.

The LBEs corresponding to event sequence families in the PRA identify events that have the potential to release radioactivity to the public. Thus, the LBEs inform the determination of the limiting source terms and potential releases considered for the required normal operations and safety analysis evaluations.

3.2.2 LBE Selection Process

A logic chart indicating the tasks to identify and evaluate LBEs in concert with the design evolution is shown in Figure 3-2. The process informs the preparation of appropriate licensing application submittals that describe the derivation of the LBEs. The LBE selection and evaluation process is implemented in LBE selection tasks described below.

The tasks identified in Figure 3-2 are not performed in any specific order and their completion is recognized as an iterative process. In addition, the LBE selection and evaluation process may be performed using alternative tasks that provide comparable technical information as needed to identify a sufficiently complete set of design specific LBEs and to evaluate the frequencies and consequences of the LBEs against the F-C Target and cumulative risk targets. The LBE process is developed in a manner that facilitates the determination of risk significant LBEs and SSCs and the evaluation of defense-in-depth adequacy. If the DBAs and SSC safety classification steps are completed prior to the application of this methodology, the evaluation of LBEs is viewed as a means of confirming or refining prior selections in formulating the design and licensing bases.

Task 1: Propose Initial List of LBEs

During design development, an initial set of LBEs is selected which may not be complete but is used to develop the basic elements of the safety design. These events are selected deterministically and supported by qualitative risk insights based on relevant and available experience, including prior experience from the design and licensing of reactors. The initial selection of events is supported by analysis techniques such as process hazard analyses (PHAs), failure modes and effects analyses (FMEAs), hazard and operability studies (HAZOPs), and Master Logic Diagrams. It is acceptable to have an initial assessment regarding which SSCs are classified as Safety-Related (SR) to meet the safety design objectives for the reactor design. This classification would also be deterministically based and may be supported by qualitative risk insights using the same information utilized for the initial selection of LBEs.

Task 2: Design Development and Analysis

Design development includes various phases (e.g., pre-conceptual, conceptual, preliminary, final) and iterations within phases. Design development and analysis includes definition of the elements of the safety design approach, the design features to meet the top-level design requirements for energy production and investment protection, and analyses to develop sufficient understanding to perform a PRA and the deterministic safety analyses. The subsequent Tasks 3 through 10 are generally iterated with the design until the list of LBEs becomes stable in support of licensing (and later, operations). Because the selection of deterministic DBAs requires the selection of SR SSCs, this process also yields an initial selection of SR SSCs that are needed for the deterministic safety analysis in Task 7d.

Task 3: PRA Development/Update

A PRA model is developed and then updated as appropriate for each phase of the design. Prior to the first introduction of the PRA, a technically sound understanding of the potential failure modes of the reactor concept, how the plant would respond to such failure modes, and how protective strategies can be incorporated into formulating the safety design approach is developed. The incorporation of safety analysis methods appropriate to early stages of design, such as FMEA and PHA, provide early stage evaluations that are systematic, reproducible, and as complete as the current stage of design permits. PRA development begins early in the design.

Early in the design, the PRA comprises a coarse level of detail, and makes use of engineering judgment much more than would a completed PRA that meets applicable PRA standards. The scope and level of detail of the PRA are enhanced as the design matures and siting information (or site envelope) is defined. The event sequences modeled in the PRA include event sequences involving single or multiple reactor units or radionuclide sources. The PRA process exposes sources of uncertainty encountered and provides estimates of the frequencies and doses for each LBE, including a quantification of the impacts of uncertainties using quantitative uncertainty analyses and supported by sensitivity analyses.

Task 4: Identify/Revise List of AOOs, DBEs, and BDBEs

The event sequences modeled and evaluated in the PRA are grouped into event sequence families, each having a similar Initiating Event, challenge to the SFs, plant response, end state, and mechanistic source term if there is a radiological release. Each of these families is assigned to an LBE category based on mean event sequence frequency of occurrence per plant-year summed over all the event sequences in the LBE family. The event sequence families from this task may confirm or revise the initial events identified in Task 1.

AOOs are off-normal events that are expected to occur during the life of the plant with frequencies exceeding 10^{-2}/plant-year, where a plant may be comprised of multiple reactor units. DBEs are less frequent events that may occur in a plant with frequencies between 10^{-4} to 10^{-2}/plant-year. BDBEs are rare events with frequencies less than 10^{-4}/plant-year but with upper bound frequencies greater than 5×10^{-7}/plant-year. An LBE may be assigned a classification associated with a higher frequency as a design decision (i.e. An event with a frequency of a DBE may conservatively be assigned an AOO classification and evaluated as such). LBEs could involve release of radioactive material and could involve two or more reactor units or radionuclide sources. For LBEs with no radiological release, challenges to SSCs including barriers that are responsible for preventing or mitigating a release of radioactive material are identified.

Such insights are inputs to the subsequent task of identifying the Required Safety Functions (RSFs). The evaluation of the consequences of LBEs is supported by mechanistic source terms.

Event sequences with upper 95th percentile frequencies less than 5×10^{-7}/plant-year are retained in the PRA results and used to confirm that there are no cliff-edge effects. They are also taken into account in the RIPB evaluation of defense-in-depth in Task 7e.

Task 5a: Identify Required Safety Functions

In Task 5a, RSFs are identified by examining the full set of DBEs to identify the SFs that are necessary and sufficient to meet the F-C Target for all DBEs and high-consequence BDBEs, and to conservatively ensure that 10 CFR 50.34 dose requirements are met. SFs are those associated with the prevention or mitigation of releases from any radionuclide source within the scope of the PRA. High consequence BDBEs are those with consequences that exceed 10 CFR 50.34 dose criteria. For the DBEs these SFs, when fulfilled, are responsible for mitigating the consequences within the F-C Target. RSFs for any high-consequence BDBEs are responsible for preventing them from increasing in frequency into the DBE region and outside the F-C Target by exhibiting sufficient reliability performance to keep the BDBE frequency sufficiently low.

Task 5b: Select/Revise Safety-Related SSCs

For each of these RSFs identified in Task 5a, a decision is made on which set of SSCs is selected to perform these RSFs among those found to be available on each DBE. As a result of this selection, each DBEs is protected by a set of SR SSCs to perform each RSF. Structures and physical barriers that are necessary to protect any SR SSCs in performing their RSFs in response to any design basis external event are also classified as Safety-Related. SR SSCs are also selected for any RSF associated with any high-consequence BDBEs in which the reliability of the SSC is necessary to keep the event in the BDBE frequency region. The remaining SSCs that are not classified as SR are considered in other evaluation tasks including Tasks 7b, 7c, 7d, and 7e. Performance targets and design criteria for both SR and Nonsafety-related SSCs are developed and described more fully in Section 4.

Task 6: Select Deterministic DBAs and Design Basis External Hazard Levels

For each DBE identified in Task 4, a deterministic DBA is defined that includes the RSF challenges represented in the DBE but assumes that the RSFs are performed exclusively by SR SSCs, and all nonsafety-related SSCs that perform these same functions are assumed to be unavailable. These DBAs are then used in DBA analysis of the licensing application for supporting the conservative deterministic safety analysis.

NRC Regulatory Guide 1.203 Revision 0, "*Transient and Accident Analysis Methods,*" provides additional discussion of developing appropriate evaluation models for analyzing DBAs. The selection of conservative assumptions used in the DBA analysis is informed by the quantitative uncertainty analysis of consequences that is performed for the corresponding DBEs. In view of the fact that KP-FHR employs a diverse combination of inherent, passive, and active design features to perform the RSFs across layers of defense, and, taking into account the fact that the reactor safety design approach is subjected to an evaluation of DID adequacy, the application of a single failure criterion is deemed not necessary.

A set of Design Basis External Hazard Levels (DBEHLs) is selected to form an important part of the design and licensing basis. This determines the design basis seismic events and other external events that as necessary, SR SSCs and certain other SSCs are required to withstand. When supported by available methods, data, design, site information, and supporting guides and standards, these DBEHLs are included in the PRA after the design features that are incorporated to withstand these hazards are defined. Other external hazards not supported by a probabilistic hazard analysis are covered by DBEHLs that are determined using traditional deterministic methods.

The initial selection of SR SSCs and selection of the DBAs is informed by a PRA that includes internal events but does not address external hazards. With the understanding that as necessary, SR SSCs and other SSCs are capable of performing their RSFs in response to external events within the DBEHL, there are no new DBAs introduced by external hazards.

Some design basis external events such as external floods or seismic events may impact multiple reactor units concurrently; therefore, a design objective is to prevent a substantial release for such events. The term "substantial" is used to mean that the site boundary dose when plotted and evaluated on the F-C Target with the LBE frequency would not result in a risk-significant LBE.

The codes and thermal hydraulic models used within the PRA are subject to the technical adequacy requirements in the supporting PRA standards, whereas the codes and models used in DBA analysis are informed by Regulatory Guide 1.203 guidance for evaluation models.

Task 7: Perform LBE Evaluations

The deterministic and probabilistic safety evaluations that are performed for the full set of LBEs are covered in the following five tasks.

Task 7a: Evaluate LBEs Against F-C Target

In this task, the results of the PRA (which have been organized into LBEs) are evaluated against the F-C Target shown in Figure 3-1. The figure does not define specific acceptance criteria for the analysis of LBEs but rather serves as a tool to focus on the most significant events and possible means to address those events. The evaluations in this task are performed for each LBE separately.

The mean values of the frequencies are used to classify the LBEs into AOOs, DBEs, and BDBE categories. However, when the uncertainty bands defined by the 5^{th} percentile and 95^{th} percentile of the frequency estimates straddles a frequency boundary, the LBE is evaluated in both LBE categories. It is recognized that the PRA may not fully resolve the impacts of all sources of uncertainty, such as modeling uncertainty. The guidance in NUREG-1855 Revision 1, "*Guidance on the Treatment of Uncertainties Associated with PRAs in Risk Informed Decision Making*," is used to address uncertainties. Uncertainties not quantified in the PRA are important inputs to the evaluation of defense-in-depth adequacy. An LBE with mean frequency above 10^{-2}/plant-year and 5^{th} percentile less than 10^{-2}/plant-year is evaluated as an AOO and DBE. An LBE with a mean frequency less than 10^{-4}/plant-year with a 95^{th} percentile above 10^{-4}/plant-year is evaluated as a BDBE and a DBE. An event sequence family with a mean frequency less than 5×10^{-7}/plant-year but with a 95^{th} percentile frequency estimate above 5×10^{-7}/plant-year is evaluated as a BDBE. Uncertainties about the mean values are used to help evaluate the results against the frequency-consequence criteria and to identify the margins against the criteria.

DBE doses are evaluated against the F-C Target based on the mean estimates of consequence. This approach is consistent with the way in which uncertainties are addressed in risk-informed decision-making in general, where mean estimates supported by a robust uncertainty analysis are generally used to support risk significance determinations.

When evaluating risk significance, comparing risks against safety goal QHOs, and evaluating changes in risk against the Regulatory Guide 1.174 change in risk criteria, the accepted practice is to first perform a quantitative uncertainty analysis and then use the mean values to compare against the various goals and criteria, which are set in the context of uncertainties in the risk assessments. These assessments apply to both the frequency and consequence estimates.

The primary purpose of comparing the frequencies and consequences of LBEs against the F-C Target is to evaluate the risk significance of individual LBEs. The objective for this activity is that uncertainties in the risk assessments are evaluated and included in discussions of design features and operational programs related to the most significant events and possible compensatory measures to address those events.

The PRA process exposes sources of uncertainty encountered in the assessment of risk and provides estimates of the frequencies and doses for each LBE, including a quantification of the impacts of uncertainties using quantitative uncertainty analyses and supporting sensitivity analyses. Sources of uncertainty that are identified by the PRA and not fully resolved via quantification are addressed as part of a risk-informed evaluation of DID, as discussed in Section 5. The evaluation of the consequences of LBEs is supported by mechanistic source terms and a quantitative uncertainty analysis. The upper bound consequences for each DBA shall meet the 10 CFR 50.34 dose limit at the EAB. Justification that the DBA evaluation models are sufficiently bounding may be based on qualitative arguments rather than direct calculation of 95th percentile figures of merit. This justification will be provided in future licensing submittals.

Sources of uncertainty in both frequencies and consequences of LBEs are identified and addressed in the approach to DID.

A function of the LBE frequency-dose evaluation is to ensure that LBEs involving radiological releases from two or more reactor units do not make a significant contribution to risk and to ensure that measures to manage the risks of multi-reactor unit or multi-source events are taken. The term “plant” is used to define the entity that is being subjected to the process for LBE selection and evaluation and may be comprised of a single reactor or multiple reactor units. In addition, the plant is expected to include additional non-reactor sources of radioactive material. Hence, each LBE may involve one or more reactor units or radionuclide sources.

The final element of the LBE evaluation in this task is to identify design features that are responsible for keeping the LBEs within the F-C Target including those design features that are responsible for preventing or mitigating risk-significant releases for those LBEs with this potential. This evaluation leads to performance requirements and design criteria that are developed within the process of the SSC classification task in the risk-informed, performance-based approach.

Task 7b: Evaluate Integrated Plant Risk against QHOs and 10 CFR 20

In this task, the integrated risk of all the LBEs, is evaluated against three cumulative risk targets:

- The total frequency of exceeding a site boundary dose of 100 mrem from all LBEs should not exceed 1/plant-year. This metric is introduced to ensure that the consequences from the entire range of LBEs from higher frequency, lower consequences to lower frequency, higher consequences are considered. The value of 100 mrem is selected from the annual cumulative exposure limits in 10 CFR 20.

- The risk to the average individual of early fatality within 1 mile of the EAB from all LBEs should not exceed 5×10^{-7}/plant-year to ensure that the NRC safety goal QHO for early fatality risk is met.

- The risk to an average individual of latent cancer fatalities within 10 miles of the EAB from all LBEs should not exceed 2×10^{-6}/plant-year to ensure that the NRC safety goal QHO for latent cancer fatality risk is met.

One element of this task is to identify design features that are responsible for preventing and mitigating radiological releases and for meeting the integrated risk criteria. This evaluation leads to performance requirements and design criteria that are developed within the process of the SSC classification task.

In addition to the two QHOs, the 10 CFR 20 criterion is considered in recognition that the referenced regulatory requirement is for the combined exposures from all releases even though it has been used in developing the F-C Target used for evaluating the risks from individual LBEs. Having these cumulative risk targets as part of the process provides a mechanism to ensure that the F-C Target is conservatively defined.

Task 7c: Evaluate Risk Significance of LBEs and SSCs Including Barriers

In this task, the details of the definition and quantification of each of the LBEs in Task 7a and the integrated risk evaluations of Task 7b are used to define the risk significance of individual LBEs and SSCs which include radionuclide barriers. These evaluations include the examination of the effectiveness of each of the layers of defense in retaining radionuclides. LBEs are classified as risk-significant if the combination of the upper bound estimates of the frequency and consequence of the LBE are within 1% of the F-C target and the upper bound 30-day TEDE dose at the EAB exceeds 2.5 mrem. SSCs are classified as risk-significant if the SSC function is necessary to keep any LBEs inside the F-C Target, or if the total frequency of LBEs with the SSCs failed is within 1% of any of the three cumulative risk targets identified in Task 7b. This information is used to provide risk insights, to identify safety-significant SSCs, and to support the RIPB evaluation of DID in Task 7e.

Task 7d: Perform Deterministic Safety Analyses Against 10 CFR 50.34

This task corresponds to the traditional deterministic safety analysis that is found in the DBA analysis of the licensing application. It is performed using conservative assumptions. The uncertainty analyses in the mechanistic source terms and radiological doses that are part of the PRA are available to inform the conservative assumptions used in this analysis and to avoid the arbitrary "stacking" of conservative assumptions.

Task 7e: Risk-Informed, Performance-Based Evaluation of Defense-in-Depth

In this task, the definition and evaluation of LBEs is used to support a RIPB evaluation of DID. This task involves the identification of risk-significant sources of uncertainty in both the frequency and consequence estimates, and evaluation against DID criteria. Outcomes of this task include possible changes to the design to enhance the plant capabilities for DID, formulation of conservative assumptions for the deterministic safety analysis, and input to defining and enhancing programmatic elements of DID.

It is noted that this DID evaluation does not change the selection of LBEs directly. This evaluation could lead to compensatory actions that change the design capability or programmatic controls on the design, which in turn would lead to changes in the PRA and thereby affect the selection or evaluation of LBEs.

Plant features are also assessed for effective satisfaction of regulatory requirements such as 10 CFR 50.155, "Mitigation of Beyond-Design Basis Events," and 10 CFR 73, "Physical Protection of Plants and Materials." The results from the evaluation support related licensing matters such as defining appropriate constraints in terms of siting (i.e., 10 CFR 100, "Reactor Site Criteria"), offsite emergency planning, and development of plant emergency operating procedures and guidelines.

Task 8: Decide on Completion of Design/LBE Development

The purpose of this task is to decide if additional design development is needed to proceed to the next logical stage of design or to incorporate feedback from the LBE evaluation into the facility design, operation, or programs. Such improvements could be motivated by a desire to increase margins against the frequency-consequence criteria, reduce uncertainties in the LBE frequencies or consequences, manage the risks of multi-reactor unit events, limit the need for restrictions on siting or emergency planning, or enhance the performance against DID criteria. The DID adequacy evaluation may result in the need for additional iterations on the adequacy of design, operational, and programmatic programs, which in turn could influence the PRA and result in a need for cycling through some or all the LBE evaluation tasks.

Task 9: Proceed to Next Stage of Design Development

The decision to proceed to the next stage of design is reflected in this task.

Task 10: Finalize List of LBEs and Safety-Related SSCs

Establishing the final list of LBEs and SR SSCs signifies the completion of the LBE selection process and the selection of the SR SSCs. The next task in implementing the RIPB approach is to complete the SSC safety classification process and to formulate performance requirements and design criteria for SSCs that are necessary to control the LBE frequencies and doses and other performance standards associated with the protection of fission product barriers as discussed in Sections 4 and 5.

3.2.3 Evolution of LBEs Through Design Stages

The LBE selection logic chart in Figure 3-2 reflects an iterative process involving design development, PRA development, selection of LBEs, and evaluation of LBEs. The process logic chart can be viewed as beginning in pre-conceptual or conceptual design when many design details are unavailable, the PRA effort has not begun, and the safety design is just being formulated. To begin the process outlined in Figure 3-2, an initial set of LBEs is proposed based on engineering judgment in Task 1 of the process. This may generate an initial target selection of SR SSCs.

During conceptual design, different design concepts are explored, and alternatives are considered to arrive at a feasible set of alternatives for the plant design. Traditional design and analysis techniques are applied during conceptual design, including (1) use of traditional design bases of engineering analysis and judgment, (2) application of research and development programs, (3) use of past design and operational experience for other types of reactors, (4) performance of design trade studies, and (5) decisions on how or whether to conform to established applicable LWR-based reactor design criteria and whether other principle criteria are needed as discussed in Reference 10.

The early stages of design development are guided by deterministic decisions that outline the desired safety characteristics for a given design. RG 1.232 is used as one input to initially establish principal design criteria as discussed in Reference 10.

Creation of the initial event list of LBEs includes expert evaluation and review of the relevant experience gained from previous reactor designs and associated PRAs when available. It starts by answering the first question in the risk triplet series: What can go wrong? Care is exercised to ensure that information taken from other reactor technologies is interpreted correctly. Once design alternatives and trade studies are developed, the safety design is defined. A review of the major systems takes place, and techniques such as a FMEA and PHAs such as HAZOPs are applied to identify initial failure scenarios and to support the initial PRA tasks to define Initiating Events.

Preliminary design activities balance regulatory and design requirements, cost, schedule, and other owner requirements to optimize the design, cost, and capabilities that satisfy the objectives for the plant.

As the design matures, the scope and level of detail of the PRA is expanded, and it is used to support design decisions along the way. An early simplified PRA supports design trade studies performed to better define the safety design. Questions that arise in the efforts to build a PRA model are helpful in the understanding of what kind of challenges need to be addressed. Because the design is being changed more frequently at this point and is better characterized as the design evolves, the PRA results and their inputs to the LBE selection process are also subject to change. As a result, refinements to the list of LBEs are expected. The simplifying perception that a design has stages that contain bright lines is a frequent description at the system level but is not correct at the plant level. Different parts of the design mature at different times. Systems often go through design stages, however, at any given time, there may be systems in many design phases simultaneously. Consequently, the PRA development is a continuum as well, maturing with the system designs. PRA updates with system development provide a more frequent integrated plant performance check that is otherwise missing in the conventional design process and also provide risk insights to help the design decisions. When the design and PRA are developed in a manner that is sufficient to meet requirements reflected in applicable PRA standards and regulatory guides, the LBEs are finalized and included in the licensing application.

3.3 ROLE OF THE PRA IN LBE SELECTION

Applicants under the 10 CFR 52 framework are required by NRC regulations to develop a PRA (10 CFR 50.71(h)) and to provide a description of the PRA results in its licensing applications (e.g., 10 CFR 52.79). If Kairos Power pursues a license under 10 CFR 50, the applicable 10 CFR 52 regulations regarding PRA will still be relevant as discussed in Reference 11, meeting the intent of SECY-15-0002. The primary motivation to utilize inputs from a PRA in the selection of LBEs is that the PRA has the systematic capability to identify and evaluate events that are specific and unique to the KP-FHR. This does not suggest that the PRA produces the LBEs, but rather informs and validates the LBE selection and evaluates the LBE selection for completeness. Traditional methods for selecting LBEs, such as those reflected in the General Design Criteria and Chapter 15 of the Standard Review Plan (SRP) "*NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition*," do not refer to a systematic process for identifying design-specific events. The generic lists of events provided in the SRP as examples of transients and postulated event sequences to consider are specific to LWRs. Traditional techniques for systems analyses (i.e., FMEAs, HAZOPs, single failure analyses, etc.), which were used to define the LBEs for currently licensed reactors, have been incorporated into the PRA methodology for selecting Initiating Events and developing event sequence models. PRA is also a mature technology that is supported by industry consensus standards and regulatory guides.

Kairos Power is developing a technically sound understanding of the potential failure modes of the KP-FHR, how the plant responds to such failure modes, and how protective strategies can be incorporated into the safety design. The incorporation of safety analysis methods appropriate to early stages of design, such as FMEA and PHA, provide industry-standardized practices to ensure that such early stage evaluations are systematic, reproducible, and as complete as the current stage of design permits. This information supports development of the PRA.

There are many interfaces between the design and engineering processes and the PRA. The PRA is developed in parallel with the design and provides important risk insights to the design development and supporting analyses.

Barriers that prevent a release of radioactive material and the SSCs that protect these barriers contribute to the layers of defense and are evaluated for DID adequacy. This supports the PRA goal of identifying event sequences that involve a release of radioactive material. SSCs that perform the SFs to protect the barriers serve to prevent challenges to the barriers or enhance the effectiveness of barriers in preventing or limiting releases of radioactive material.

The PRA is also used to evaluate the safety characteristics of the design and to provide a structured process from which the initial set of LBEs is risk-informed. The evaluation of the risks of the LBEs against the F-C Target helps make the LBE selection process both risk-informed and performance-based. It highlights the issues that merit the greatest attention in a safety-focused process. Subsequently, the PRA provides important input to the formulation of performance targets for the capability and reliability of the SSCs to prevent and mitigate events and thereby contribute to the performance-based aspects of the design and licensing development process.

In addition, engineering judgment and utilization of relevant experience continues to ensure that LBE selection and classification is complete. The PRA systematically enumerates event sequences and assesses the frequency and consequence of each event sequence. Event sequences include internal events, internal plant hazards, and external events. The modeled event sequences include the contributions from common-cause failures.

Each event sequence family reflected in the LBE definitions is defined as a collection of event sequences that similarly challenge plant SFs. This means that the Initiating Events within the family have a similar impact on the plant such that the event sequence development following the plant response are the same for each sequence within the family. If the event sequence involves a radiological release, each sequence in the family has the same or similar mechanistic source term and offsite radiological consequences. Many of the LBEs do not involve a release and understanding the plant capabilities to prevent release is an extremely important insight to feed back to the design. Selection of LBEs is facilitated by grouping many individual events into a manageable event sequence family.

The PRA's quantification of both frequencies and consequences address uncertainties, especially those associated with the potential occurrence of rare events. The quantification of frequencies and consequences of event sequences, and the associated quantification of uncertainties, provides an objective means of comparing the likelihood and consequence of different scenarios against the F-C Target. The scope of the PRA, when completed, covers a full set of internal and external Initiating Events and provides determination of radiological consequences when the design is completed, and site characteristics are defined. All parts of the process are evaluated by assessing fission product barriers and showing that radioactive materials are retained within the facility with a high degree of confidence. This approach benefits from some of the information provided by a PRA, including the identification of challenges to the barriers and identification and evaluation of dependencies among the barriers and layers of defense.

If applicable, the PRA includes event sequences involving two or more reactor units as well as two or more sources of radioactive material. This enables the identification and evaluation of risk management strategies for reactor units and sources within the scope of a single application to ensure that sequences involving multiple reactor units and sources are not risk-significant. The NRC staff has developed technical criteria (e.g. Quantitative Health Objectives) for evaluating multi-reactor unit risk. Satisfying these technical criteria ensure that multi-reactor unit plants are designed and operated in such a way to demonstrate that the event sequences are not significant contributors to risk and large release events, and, if these events should occur, to mitigate their impact on the public health and safety. Additionally, these criteria ensure that relevant risk insights related to multi-reactor unit design and operation are identified and evaluated.

The LBE selection process is not risk-based, but rather risk-informed as there are strong deterministic inputs to the process. First, the PRA development is anchored to traditional deterministic engineering analyses that involve numerous applications of engineering judgment. These include FMEAs, PHAs, application of relevant experience from design and licensing of other reactors, and deterministic models of the plant response to events. Second, the deterministic DBAs are selected based on prescriptive rules and analyzed using conservative assumptions. Finally, the LBE selection includes a review to ensure that the LBE selection and the results of the LBE evaluations meet a set of guidelines to evaluate DID adequacy.

These evaluations often lead to changes to the plant design and programmatic controls that are reflected in changes to the PRA and, hence, changes to the selection of LBEs and SSC safety classification. In addition to these elements, peer reviews and regulatory reviews of the PRA provide an opportunity to challenge the completeness and treatment of uncertainties in the PRA to ensure that the deterministic DBAs and the conservative assumptions that are used in the DBA analysis are sufficient to meet the applicable regulatory requirements.

3.3.1 Use of PRA in LBE Selection Process

In the course of developing the PRA model, a comprehensive set of Initiating Events and event sequence families are systematically identified, building on the engineering and systems analyses that are performed to support the design development. These events and event sequences are considered in the selection of the LBEs, and the quantitative estimates of the event sequence frequencies and consequences provide a basis for evaluating their risk significance. Deterministic evaluations of prescriptively derived DBAs benefit from the identification and evaluation of LBE uncertainties that result from the PRA process.

SSC safety classification requires an assessment of the risk significance of SSCs and the LBEs that describe the SFs of the SSCs in the prevention and mitigation of events. Information from the PRA is used as input to the selection of reliability targets and performance requirements for SSCs that set the stage for the selection of special treatment requirements.

The PRA process, in the course of addressing the three questions of the risk triplet (what can go wrong, how likely is it and what are the consequences?) exposes many sources of uncertainty in the definition of event sequences, the estimation of their frequencies, and the quantification of the consequences. This information on uncertainties is important input in the selection of protective strategies and in the evaluation of DID adequacy. Additional roles of the PRA in the DID evaluation include information on the LBE risk margins against the F-C Target and the cumulative risk targets and evaluation of quantitative DID evaluation criteria.

The above uses of the PRA complement the use of deterministic methods traditionally employed in the development of the design and licensing bases as part of a risk-informed, rather than risk-based, process.

3.3.2 PRA Scope for LBE Selection

The PRA model addresses the spectrum of internal events and external hazards that pose challenges to the capabilities of the plant. The size, complexity, and potential risk of the KP-FHR influences the level of detail necessary to support this process.

Quantification of the frequencies and radiological consequences of each of the significant event sequences modeled is an important outcome of the PRA. This quantification includes mean point estimates and an appropriate quantification of uncertainty in the form of uncertainty probability distributions. These distributions account for quantifiable sources of parameter and model uncertainty in the event frequencies, mechanistic source terms, and offsite radiological consequences. The evaluations include an appropriate set of sensitivity analyses to provide adequate assurance that major contributors to risk and performance uncertainties are identified and addressed.

Plants comprised of multiple reactor units consider event sequences that impact reactor units independently as well as those that credibly impact two or more reactor units concurrently.

3.3.3 PRA Scope Adequacy

The guidance in the ASME/ANS RA-S-1.4 is used to establish the scope and technical adequacy of the PRA. The scope and level of detail of the PRA models align with the state of definition of the design, the safety design approach, and systems design concepts. As the design matures and more design information becomes available for different types of risk evaluations, the scope of the PRA is broadened to address other plant conditions and progressively confirm the plant capability to meet safety objectives.

Given the simple systems, inherent characteristics, and minimal possible public health hazards, the PRA complexity necessary to support decision-making and an application for KP-FHR is much less complex than for operating LWR plants.

3.3.4 Safety Functions

A SF is a function by an SSC modeled in the PRA that is responsible for preventing or mitigating a release of radioactive material from a radioactive material source within the plant. Some of these SFs are further classified as RSFs if they are necessary to ensure that all the DBEs have doses that fall within the F-C Target and also to ensure that the doses for the DBAs meet the requirements of 10 CFR 50.34 using conservative assumptions. Once those RSFs are defined, SSCs that are available to support those functions on all the DBEs are identified. In addition, SSCs whose reliability needs to be assured to prevent high-consequence BDBEs from migrating up into the DBE region are also identified. From these sets of SSCs, a set of SR SSCs to perform each RSF is selected.

RSFs are defined starting with generic Fundamental Safety Functions (FSFs) defined by the International Atomic Energy Agency (IAEA) of control of the reactor power, removal of heat from the fuel, and confinement of radioactive materials in IAEA document, "*Proposal for a Technology-Neutral Safety Approach for New Reactor Designs* (Reference 5)." These are refined as necessary into reactor technology-specific SFs that reflect the reactor concept and unique characteristics of the reactors. This provides the foundation for reactor technology-specific SSCs selected to perform each function.

3.3.5 Risk Metrics for PRA Model Development

Overall Plant Risk Metrics

The KP-FHR PRA model is structured differently from the model for an LWR PRA, given that plant damage states will not involve an equivalent metric to the core damage state in an LWR PRA model. Frequencies of event sequences are individually identified and grouped into event sequence families having the same or similar plant response, and offsite radiological consequences are defined in terms of plant response, mechanistic source term, and offsite radionuclide consequences. Consequences are quantified in terms of offsite early and latent health effects and/or site boundary doses and are supported by mechanistic source terms. Risk metrics are defined in Section 3.2.2.

Reactor-specific risk metrics will be used to define the parameters of the PRA model. Requirements for the definition and use of these reactor-specific metrics are given in the Advanced Non-LWR PRA

Standard (Reference 4). The selection of PRA risk metrics addresses event sequences that involve one or more reactor units or non-reactor radionuclide sources. This is addressed by using the following approaches:

- The Initiating Events (IEs) and event sequences in the PRA delineate events involving each reactor unit and radionuclide source separately as well as events involving two or more reactor units or sources.
- Dependencies associated with shared systems and structures are explicitly modeled in an integrated fashion to support an integrated risk assessment of the entire plant where the plant may be comprised of two or more reactor units and non-core radionuclide sources.
- Treatment of human actions considers the unique performance-shaping factors associated with multi-reactor unit and multi-source event sequences.
- Treatment of common-cause failures delineates those that may impact multi-reactor units or non-reactor radiological sources.
- The frequency basis of the event sequence quantification is events per (multi-reactor unit/multi-source) plant-year.

Risk Significance Evaluations

There are two types of risk significance evaluations that are performed for the selection and evaluation of LBEs. The first type is an evaluation of the frequencies and consequence of each LBE, expressed in the form of mean values and uncertainty (at the 5th and 95th percentiles), against the F-C Target. In this evaluation, the frequencies and consequences of individual LBEs are compared against an F-C Target derived from regulatory requirements and NRC safety goal policy. The objective is to keep the LBE frequencies and consequences within the F-C Targets. An evaluation of the margins between the LBE risks and the F-C Target is one aspect of the RIPB evaluation of plant capability and DID adequacy. Figure 3-3 illustrates the use of the F-C Target to establish risk-significant LBEs.

Each LBE in this evaluation is defined as a family of event sequences modeled in the PRA that groups the individual modeled PRA event sequences according to the similarity of the following elements of the event sequence:

- Plant operating state (POS) at the time of the Initiating Event
- Initiating Events
- Plant response to the IE and any independent or consequential failures represented in the event sequence, including the nature of the challenge to the barriers and SSCs supporting each SF
- Event sequence end state
- Combination of reactor units and radionuclide sources affected by the sequence
- Mechanistic source term (MST) for sequences involving a radiological release

The event sequence frequencies are expressed in terms of events/plant-year where a plant may be comprised of two or more reactor units and sources of radioactive material.

In addition to evaluation of each individual LBE, an integrated risk evaluation of the entire plant is performed against the below criteria. For this evaluation, the integrated risk of the entire plant is evaluated against three cumulative risk targets:

- The total frequency of exceeding a site boundary dose of 100 mrem from all LBEs should not exceed 1/plant-year. This metric is introduced to ensure that the consequences from the entire range of LBEs from higher frequency, lower consequences to lower frequency, higher consequences are considered. The value of 100 mrem is selected from the annual exposure limits in 10 CFR 20.

- The risk to the average individual of early fatality within 1 mile of the EAB shall not exceed 5×10^{-7}/plant-year to ensure that the NRC safety goal QHO for early fatality risk is met.

- The risk to the average individual of latent cancer fatalities within 10 miles of the EAB shall not exceed 2×10^{-6}/plant-year to ensure that the NRC safety goal QHO for latent cancer fatality risk is met.

Risk-significant LBEs are those with frequencies within 1% of the F-C Target with site boundary doses exceeding 2.5 mrem (see crosshatched region of Figure 3-3). As discussed in Section 3.2.2, Task 7a, event sequences lower than the 5E-7/plant-year will also be evaluated to ensure that with uncertainty there are no cliff-edge effects. The PRA will also retain residual risk event sequences below the 5E-7/plant-year regardless of whether those sequences need to be analyzed as a BDBE. However, only LBEs (which have event sequence probabilities greater than 5E-7) can be considered risk-significant. To consider the effects of uncertainties, the upper 95th percentile estimates of both frequency and dose are used. The use of the 1% metric is consistent with the approach to defining risk-significant event sequences in the PRA standards. The 2.5 mrem cut-off is selected as this is approximately 10% of the dose that an average person at the site boundary would receive in 30 days due to background radiation.

3.3.6 Contributors to Risk and Risk Importance Measures

To derive useful risk insights from the results of a PRA, it is necessary to understand the principal contributors to each evaluated risk metric. This is achieved by rank ordering the PRA event sequences and sequence minimal cut-sets to identify their absolute contribution to each risk metric and to calculate the risk importance measures that evaluate contributions to basic events that are common to two or more sequences or cut-sets. For the integrated risk metrics, such as the QHOs, the absolute risk significance of an LBE is calculated as a percentage of the LBE risk (product of the LBE frequency and LBE consequence) to the risk target for each objective.

In order to evaluate the risk contributions from basic events that may appear in two or more event sequences or cut-sets, risk importance measures are used. The risk measures used to define risk significance for basic events are listed in Table 3-1 for the three integrated plant risk measure. In this table, the term R represents the total risk, *R(base)* is the risk of a given undesired outcome, with each basic event probability set to its base value, and the term x_i represents the probability of a basic event i (e.g., the event that a specific valve fails to perform its function). The risk reduction measure is compared to 1% of the risk target for each measure. The PRA will also include risk achievement importance measures for additional insights, but risk significance thresholds are only defined for the risk reduction measures.

The associated risk importance measures definitions are used with any of the risk metrics selected for the PRA using this process. These include:

- Frequency of a specific LBE
- Total risk (sum of the product of frequency and site boundary dose) of all the PRA modeled sequences, or individual risk of fatality in the plant vicinity
- Frequency of exceeding a specified site boundary dose
- Individual risk of prompt or latent fatality for comparison to NRC safety goal QHOs

The historical approach to evaluating risk importance produced only the relative importance of each basic event because the formulas are normalized against the total calculated risk for the plant, *R(base)*. For KP-FHR, the frequencies of events involving a release of radioactive material may be very small and those events with releases may involve very small source terms compared with releases from an LWR core damage event. This underlines the importance of using absolute vs. relative risk metrics to establish LBE and SSC risk significance. Hence, it is appropriate to evaluate risk significance not only on a relative basis but also on an absolute basis.

For this purpose, the risks are compared against the risk goals rather than the baseline risks. One example of the use of absolute risk metrics is the approach to defining risk-significant LBEs as illustrated in Figure 3-3. Another metric is used in establishing the risk significance of SSCs. For this metric, SSCs are risk-significant if any of the following criteria are met:

- A prevention or mitigation function of the SSC is necessary to meet the design objective of keeping all LBEs within the F-C Target. This is determined by assuming failure of the SSC in performing a prevention or mitigation function and checking how the resulting LBE risks compare with the F-C Target. The LBE is considered within the F-C Target when a point defined by the upper 95th percentile uncertainty of the LBE frequency and dose estimates is within the F-C Target.
- The SSC makes a significant contribution to one of the cumulative risk metrics used for evaluating the risk significance of LBEs. A significant contribution to each cumulative risk metric limit is satisfied when the total frequency of all LBEs with failure of the SSC exceeds 1% of the cumulative risk metric limit. This evaluation of SSC risk significance requires the aggregation of all the LBEs in which any basic event in the PRA model associated with the SSC is failed. There are normally different basic events for different SSC failure modes (e.g. failure to start, failure to run, etc.), unavailability for test or maintenance, or a common-cause basic event involving that SSC. When the total frequency of LBEs with all the basic events associated with the SSC exceeds the 1% criterion, the SSC is regarded as risk-significant. The cumulative risk metrics and limits include:

- The total frequency of exceeding a site boundary dose of 100 mrem < 1/plant-year (10 CFR 20)
- The risk to the average individual of early fatality within 1 mile of the EAB < 5×10^{-7}/plant-year (QHO)
- The risk to the average individual of latent cancer fatalities within 10 miles of the EAB should not exceed 2×10^{-6}/plant-year (QHO)

Table 3-1. Basic Event Risk-Significance Criteria for Cumulative Risk Measures

	Risk Reduction $R(base) - R(x_i = 0)$
Prompt Health Risk	$> 5 \cdot 10^{-9}$ (prompt fatalities/yr)
Latent Health Risk	$> 2 \cdot 10^{-8}$ (latent fatalities /yr)
100 mrem release risk	$> 10^{-2}$ (100 mrem release/yr)

Figure 3-1. Frequency-Consequence Target

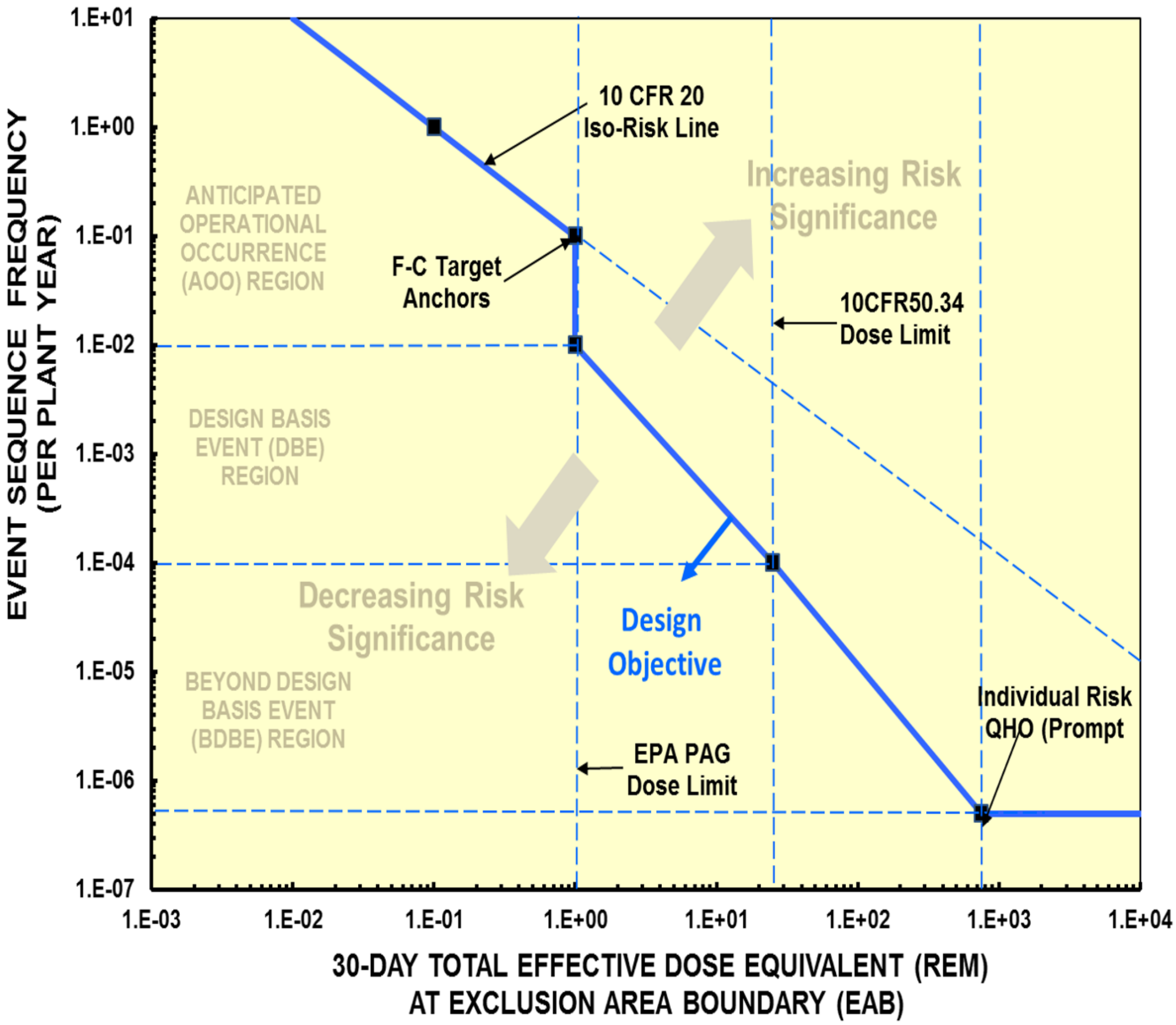


Figure 3-2. Process for Selecting and Evaluating Licensing Basis Events

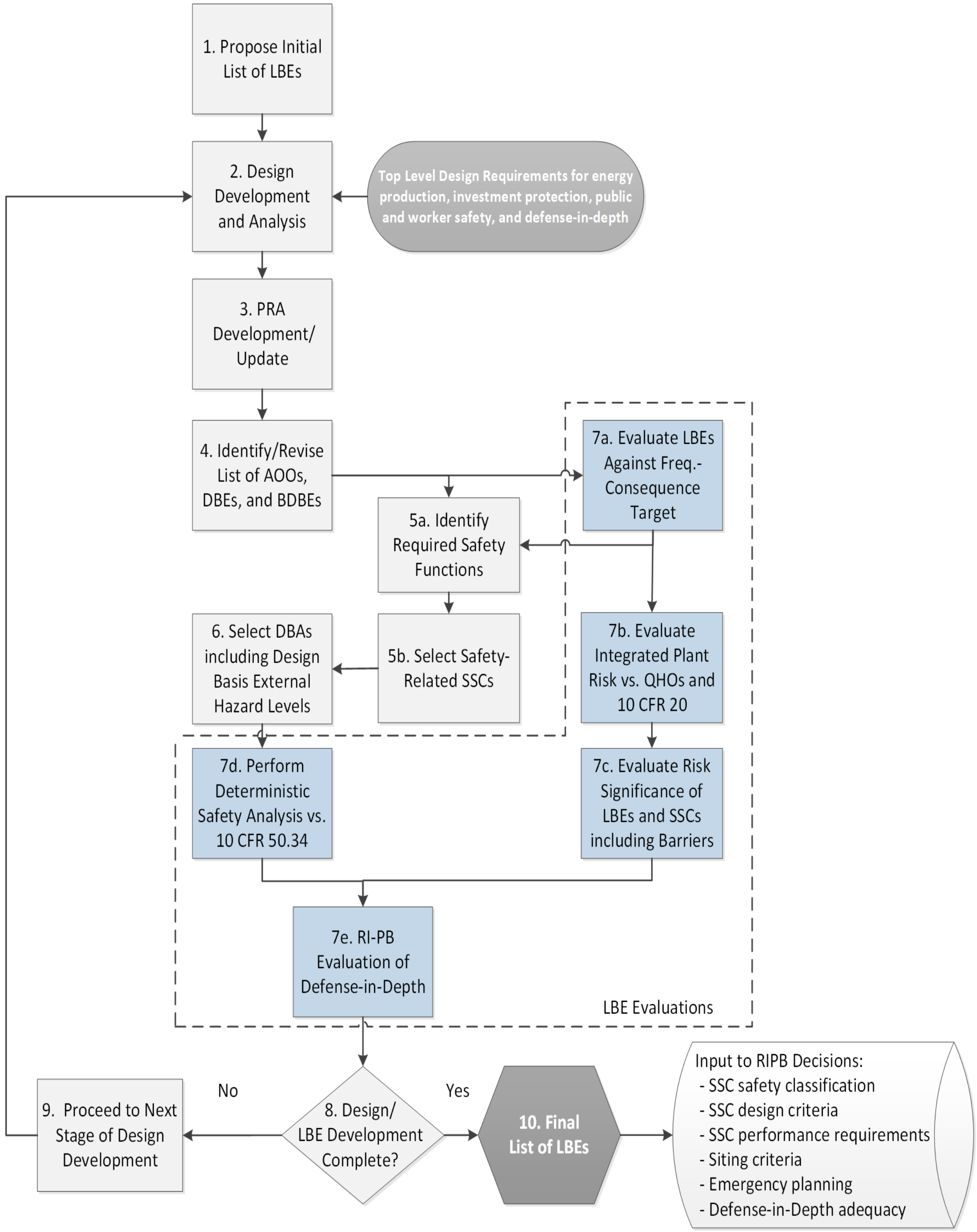
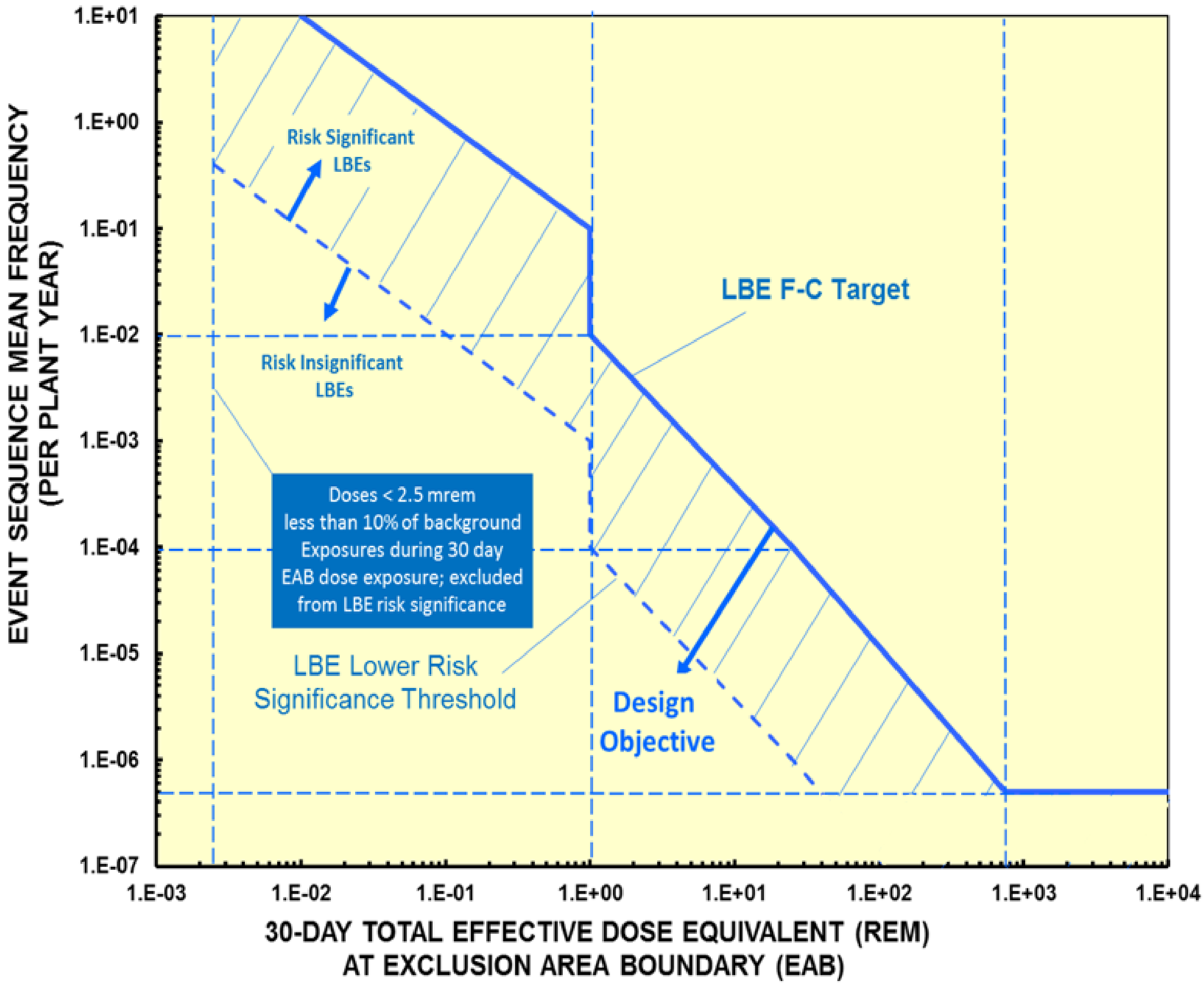


Figure 3-3. Use of the F-C Target to Define Risk-Significant LBEs



4 SAFETY CLASSIFICATION AND PERFORMANCE CRITERIA FOR STRUCTURES, SYSTEMS, AND COMPONENTS

The purpose of this section is to define the approach to SSC safety classification and the derivation of requirements necessary to support SSC performance of SFs in the prevention and mitigation of LBEs. Such requirements include those to provide the necessary capabilities to perform their mitigation functions and those to meet their reliability targets to prevent LBEs with more severe consequences. Use is made of relevant aspects of risk-informed SSC classification approaches that have been developed for existing and advanced LWRs and small modular reactors, including those developed for implementation of 10 CFR 50.69.

Safety classification categories are defined as follows:

- Safety-Related:
    - SSCs to perform the RSFs to mitigate the consequences of DBEs to within the LBE F-C Target, and to mitigate DBAs that only rely on the SR SSCs to meet the dose limits of 10 CFR 50.34 using conservative assumptions
    - SSCs relied on to perform RSFs to prevent the frequency of BDBE with consequences greater than the 10 CFR 50.34 dose limits from increasing into the DBE region and beyond the F-C Target
    - SSCs relied on to shut down the reactor and maintain it in a safe shutdown condition
- Nonsafety-related with Special Treatment (NSRST):
    - Nonsafety-related SSCs relied on to perform risk-significant functions. Risk-significant SSCs are those that perform functions that prevent or mitigate any LBE from exceeding the F-C Target or make significant contributions to the cumulative risk metrics selected for evaluating the total risk from all analyzed LBEs.
    - Nonsafety-related SSCs relied on to perform functions requiring special treatment for DID adequacy
- Nonsafety-related with No Special Treatment (NST):
    - All other SSCs (with no special treatment required)

Safety-significant SSCs include all those SSCs classified as SR or NSRST. None of the NST SSCs are classified as safety-significant.

There are design requirements to protect all SR SSCs from adverse impacts of DBEHLs. This includes design requirements to prevent adverse impacts from failure of an SSC classified as NST or NSRST that could otherwise prevent an SR SSC from performing its RSFs.

The RIPB SSC performance and special treatment requirements identified in this process for SR and NSRST SSCs are complimentary activities. The purpose of these requirements is to provide reasonable confidence in the SSC capabilities and reliabilities in performing functions identified in the LBEs consistent with the F-C Target and the regulatory dose limits for DBAs.

4.1 SSC SAFETY CLASSIFICATION APPROACH

The SSC safety classification process is described in Figure 4-1. This process classifies SSCs on the basis of the SSC SFs reflected in the LBEs. Although the SSCs are classified, the resulting performance and special treatment requirements are for the specific functions identified in the LBEs. This process is used with the process for selecting and evaluating LBEs. The information needed to support the SSC safety classification is available when Task 10 of the LBE selection and evaluation process is completed in each phase of the design process.

The SSC safety classification process is described below. This process is described as an SSC function classification process rather than an SSC classification process because only those SSC functions that prevent or mitigate events represented in the LBEs are of concern. A given SSC may perform other functions that are not relevant to LBE prevention or mitigation or functions with a different safety classification.

Task 1: Identify SSC Functions in the Prevention and Mitigation of LBEs

The purpose of this task is to review each of the LBEs, including those in the AOO, DBE, and BDBE regions to determine the function of each SSC in the prevention and mitigation of the LBE. Each LBE is comprised of an IE, a sequence of conditioning events, and an end state. The IEs may be associated with an internal event such as an SSC failure or human error, an internal plant hazard such as a fire or flood, or an external event such as a seismic event or external flood.

For those internal events caused by an equipment failure, the IE frequency is related to the unreliability of the SSC, i.e., SSCs with higher reliability serve to prevent the IE. Thus, higher levels of reliability result in a lower frequency of IEs. For SSCs that successfully mitigate the consequences of the IE, their capabilities and safety margins to respond to the IE are the focus of the safety classification process and resulting special treatment. For those SSCs that fail to respond along the LBE, their reliabilities, which serve to prevent the LBE by reducing its frequency, are the focus of the reliability targets derived from the classification and treatment process. The output of this task is the identification of the SSC prevention and mitigation functions for all the LBEs.

Task 2: Identify and Evaluate SSC Capabilities and Programs to Support Defense-in-Depth

The purpose of this task is to provide a feedback loop from the evaluation of DID adequacy. This evaluation includes an examination of the plant LBEs, identification of the SSCs responsible for the prevention and mitigation of events, and a set of criteria to evaluate the adequacy of DID. A result of this evaluation is the identification of SSC functions and the associated SSC reliabilities and capabilities that are deemed necessary for DID adequacy. Such SSCs and their associated functions are regarded as safety-significant, and this information is used to inform the SSC safety classification in subsequent tasks.

Task 3: Determine the Required and Safety-Significant Functions

The purpose of this task is to define the SFs necessary to meet the F-C Target for all the DBEs and the high-consequence BDBEs, i.e., the RSFs, as well as other SFs regarded as safety-significant. Safety-significant SSCs include those that perform risk-significant functions and those that perform functions that are necessary to meet DID criteria. The scope of the PRA includes all the plant SSCs that are responsible for preventing or mitigating the release of radioactive material. Hence, the LBEs analyzed by the PRA include all the relevant SSC prevention and mitigation functions.

As explained previously, there are some SFs classified as RSFs that must be fulfilled to meet the F-C Target for the DBEs using realistic assumptions and 10 CFR 50.34 dose requirements for the DBAs using conservative assumptions. In addition to these RSFs, there are additional functions that are classified as safety-significant when certain risk significance and DID criteria are met, as explained below. In most cases, there are several combinations of SSCs that can perform these RSFs. How individual SSC SFs are classified relative to these function categories is resolved in Tasks 4 and 5. The concepts used to classify SSC SFs as risk-significant and safety-significant are illustrated in Figure 4-2.

The following key points are used to define the different regions on the SSC Venn diagram:

- The PRA model does not include all the SSCs in the plant but does include any SSC that performs a prevention or mitigation function for the sources of radioactive material in the scope of the PRA.

- Safety-significant SSCs are within the scope of the PRA-modeled SSCs and include SSCs that perform a risk-significant function and those that are needed to meet DID criteria.

- Safety-Related SSCs may or may not be risk-significant depending on whether they meet the SSC risk significance criteria. While SR SSCs perform RSFs that are needed to keep one or more DBEs or high-consequence BDBEs within the F-C Target, if there is sufficient redundancy or diversity provided by other SSCs that perform these RSFs, a given SR SSC is not necessarily risk-significant. However, all SR SSCs contribute to the layers of defense in meeting the DID adequacy criteria, and all SR SSCs are classified as safety-significant.

Tasks 4 and 5: Evaluate and Classify SSC Functions

The purpose of Tasks 4 and 5 is to classify the SSC functions modeled in the PRA into one of three safety categories: SR, NSRST, and NST.

Tasks 4A and 5A

In Task 4A, each of the DBEs and high-consequence BDBEs (i.e., those with doses above 10 CFR 50.34 limits) are examined to determine which SSCs are available to perform the RSFs. One specific combination of available SSCs to perform each RSF that covers all the DBEs and high-consequence BDBEs is selected. These specific SSCs are classified as SR in Task 5A and are the only ones included in the analysis of the DBAs. All remaining SSCs are evaluated further in Tasks 4B and 4C.

Tasks 4B and 5B

In this task, each nonsafety-related SSC is evaluated for its risk significance. A risk-significant SSC function is one that is necessary to keep one or more LBEs within the F-C Target or is significant in relation to one of the LBE cumulative evaluation risk metric limits. Examples of the former category are SSCs needed to keep the consequences below the AOO limits in the F-C Target, and DBEs where the reliability of the SSCs should be controlled to prevent an increase of frequency into the AOO region with consequences greater than the F-C Target. If the SSC is classified as risk-significant and is not an SR SSC, it is classified as NSRST. SSC functions that are neither SR nor risk-significant are evaluated further in Task 4C.

Tasks 4C and 5C

In this task, a determination is made as to whether any of the remaining nonsafety-related and non-risk-significant SSC functions should be classified as requiring special treatment in order to meet criteria for DID adequacy. Those that meet these criteria are classified as NSRST in Task 5B and those remaining as NST in Task 5C. At the end of this task, all SSC functions reflected in the LBEs are placed in one of the three SSC function safety classes illustrated in Figure 4-3. Note that all SSC functions classified as either SR or NSRST are regarded as safety significant. All non-safety-significant SSC functions are classified as NST.

This approach uses the concept of SSC safety significance which includes all those SSCs that are SR or NSRST and also addresses the possibility that an SSC that is not SR nor risk-significant may be classified as safety-significant based on DID considerations. This approach to assigning risk significance uses the concept of evaluating the impact of the SSC function on the ability to meet the F-C Target, and also includes criteria based on risk significance metrics for the cumulative risk impacts of SSC functions across all the LBEs.

Task 6: SSC Reliability and Capability Targets

For each of the SSC functions classified in Task 4, the purpose of this task is to define the targets for reliabilities and capabilities for safety-significant SSCs modeled in the PRA. For SSCs classified as NSRST, these targets are used to develop specific design and special treatment requirements in Task 7.

In order to meet the risk targets (F-C Target and cumulative risk targets), SSCs that are relied upon meet reliability performance targets and demonstrate DID adequacy. Strategies to achieve design reliability targets include use of passive and inherent design features, redundancy, diversity, and defenses against common-cause failures. Programmatic actions are used to maintain performance within the design reliability targets.

Task 7: Determine SSC Specific Design Criteria and Special Treatment Requirements

The purpose of this task is to establish the specific design requirements for SSCs which include design criteria for SR classified SSCs, regulatory design and special treatment requirements for each of the safety-significant SSCs classified as SR or NSRST. The specific SSC requirements are tied to the SSC functions reflected in the LBEs and are determined utilizing the same integrated decision-making process used for evaluating DID adequacy.

For SSCs classified as SR, the design criteria are referred to as Safety-Related Design Criteria (SRDC). These are derived from the Required Functional Design Criteria (RFDC) that are in turn developed from the RSFs determined in the LBE selection process. RSFs are those SFs that are fulfilled to keep the DBEs or high-consequence BDBEs within the F-C Target. RFDCs are taken down to a lower level and form a transition to SSC-level criteria. RFDCs are defined to capture design-specific criteria that are used to supplement the Principal Design Criteria. RSFs and RFDCs are framed at the function level. After SR SSCs have been selected to perform the RSFs, the SRDCs are defined at the SSC level in a manner that assures meeting the RFDCs and the RSFs for the specific SSC selected to perform the RSFs.

NSRST SSCs are not directly associated with RFDC but are subject to special treatment as determined by the integrated decision-making process for evaluation of DID and for meeting the reliability and capability targets set in Task 6. The RFDC, SRDC, and special treatment requirements for SR and NSRST SSCs define safety-significant aspects of the descriptions of SSCs that are included in safety analysis reports.

The term “special treatment” is used in a manner consistent with Regulatory Guide 1.201 Revision 1, “*Guidelines for Categorizing SSCs in Nuclear Power Plants According to Their Safety Significance*,” where the following definition of special treatment is provided:

> *“…special treatment refers to those requirements that provide increased assurance beyond normal industrial practices that structures, systems, and components (SSCs) perform their design-basis functions.”*

In RIEP-NEI-16, “*Risk Informed engineering Programs (10CFR50.69)*” (Reference 6), a distinction is made between special treatment as applied to SR SSCs and alternative special treatment afforded by 10 CFR 50.69. Alternative treatment requirements are differentiated from special treatment requirements in the use of “reasonable confidence” versus “reasonable assurance,” which is a general conclusion in initial plant licensing. More details on the development of specific SSC design and performance requirements are provided in Section 4.4.

4.2 DEFINITION OF SAFETY-SIGNIFICANT AND RISK-SIGNIFICANT SSCS

4.2.1 Safety-Significant SSCs

The meaning of safety-significant SSC in this process is the same as that used in NRC regulations. The NRC glossary provides the following definition:

> *“When used to qualify an object, such as a system, structure, component, or accident sequence, this term identifies that object as having an impact on safety, whether determined through risk analysis or other means, that exceeds a predetermined significance criterion.”*

4.2.2 Risk-Significant SSCs

An SSC is classified as risk-significant if any of the following risk significance criteria are met for any SSC function included within the LBEs:

- A prevention or mitigation function of the SSC is necessary to meet the design objective of keeping all LBEs within the F-C Target. An LBE is considered within the F-C Target when a point defined by the upper 95th percentile uncertainty on both the LBE frequency and dose is within the F-C Target. In addition, some non-SR SSCs perform functions that may be necessary to keep AOOs or high-consequence DBEs within the F-C Target; these non-SR SSCs are also regarded as risk-significant and are classified as NSRST.

- The SSC makes a significant contribution to one of the cumulative risk metrics used for evaluating the risk significance of LBEs. A significant contribution to each cumulative risk metric limit is satisfied when total frequency of all LBEs with failure of the SSC exceeds 1% of the cumulative risk metric limit. This SSC risk significance criterion may be satisfied by an SSC whether or not it performs functions necessary to keep one or more LBEs within the F-C Target. The cumulative risk metrics and limits include:

    - The total frequency of exceeding a site boundary dose of 100 mrem should not exceed 1/plant-year to ensure that the annual exposure limits in 10 CFR 20 are not exceeded. An SSC makes a significant contribution to this cumulative risk metric if the total frequency of exceeding a site boundary dose of 100 mrem associated with LBEs with the SSC failed is greater than 10^{-2}/plant-year.

    - The risk to the average individual of early fatality within 1 mile of the EAB should not exceed 5×10^{-7}/plant-year to ensure that the NRC safety goal QHO for early fatality risk is met. An SSC makes a significant contribution to this cumulative metric if the individual risk of early fatalities associated with the LBEs with the SSC failed is greater than 5×10^{-9}/plant-year.

    - The risk to the average individual of latent cancer fatalities within 10 miles of the EAB should not exceed 2×10^{-6}/plant-year to ensure that the NRC safety goal QHO for latent cancer fatality risk is met. An SSC makes a significant contribution to this cumulative risk metric if the individual risk of latent cancer fatalities associated with the LBEs with the SSC failed is greater than 2×10^{-8}/plant-year.

The cumulative risk limit criteria in this SSC classification process address the situation in which an SSC may contribute to two or more LBEs that collectively may be risk-significant even though the individual LBEs may not be significant. All LBEs within the scope of the supporting PRA are included when evaluating the cumulative risk limits. In such cases, the reliability and availability of such SSCs are controlled to manage the total integrated risks over all the LBEs.

4.3 SSCS REQUIRED FOR DEFENSE-IN-DEPTH ADEQUACY

An integrated decision-making process is used to evaluate the design and risk-informed decision to ensure adequacy of design and DID. Any SSCs that do not meet the risk-significance criteria are classified as safety-significant if the integrated decision-making process determines that some form of special treatment is necessary to establish the adequacy of DID. The DID evaluation incorporates traditional engineering judgments made via an integrated decision-making panel, considers additional sources of uncertainty that are not fully resolved in the PRA. These include measures to enforce assumptions made in the PRA that may impact both frequencies and consequences and measures necessary to address considerations beyond the PRA. If a non-risk-significant SSC is classified as safety-significant, it means that some type of special treatment is applied to support the adequacy of DID.

As a result, safety-significant SSCs include both risk-significant SSCs as well as SSCs that perform functions where some form of special treatment is determined to be needed to meet DID adequacy criteria. All safety-significant SSCs are classified as SR or NSRST. NST SSCs are not safety-significant. This ensures a relationship between the SSC safety classification approach and the special treatment requirements for SR and NSRST SSCs.

4.4 DEVELOPMENT OF SSC DESIGN AND PERFORMANCE REQUIREMENTS

This section describes the approach for defining the design requirements for each of the three SSC safety categories: SR, NSRST, and NST. These design requirements begin with the identification of the SSC functions that are necessary to meet owner requirements for energy production, investment protection, worker and public safety, and licensing. SSC functions associated with the prevention and mitigation of release of radioactive material from the plant are modeled in the PRA and are represented in the LBEs. The first priority in establishing the design requirements for all the SSCs associated with the prevention and mitigation of release of radioactive material is to ensure that the capability and reliability of each SSC are sufficient for all the SSC functions represented in the LBEs, including the AOOs, DBEs, BDBEs, and DBAs. A related priority is to provide reasonable confidence that the reliability and capability of the SSCs are achieved and maintained throughout the lifetime of the plant.

Those SSCs that are classified as SR meet applicable regulatory requirements as well as reactor-specific and design-specific SRDC derived from the RFDC.

4.4.1 Required Functional Design Criteria for Safety-Related SSCs

SSCs classified as SR perform one or more SFs that are required to perform either of the following:

1. Mitigate DBEs within the F-C Target and DBAs within 10 CFR 50.34 dose limits
2. Prevent high-consequence BDBEs (those with doses exceeding 10 CFR 50.34 dose limits) from exceeding 10^{-4}/plant-year in frequency and thereby migrating into the DBE region of the F-C evaluation
3. Shut down the reactor and maintain it in a safe shutdown condition

These RSFs are used within this process to define a set of reactor-specific RFDCs from which SRDCs are derived. RFDCs are derived from the design, supported by the PRA, and related to a set of design specific RSFs. One purpose of the RFDCs is to form a bridge between the safety classification of SSCs and the derivation of SSC performance, special treatment requirements, and SRDCs.

The process for identifying the RSFs starts with a review of the SFs modeled in the PRA for the prevention and mitigation of LBEs and identifying which of those SFs, if not fulfilled, would likely increase the consequences of any of the DBEs beyond the F-C Target. This involves implementation of sensitivity analyses in which the performance of each SF that mitigates the consequences of each DBE is removed and consequences re-evaluated. This is just one example of the use of sensitivity analyses in this process. Sensitivity analyses are also performed in the development of the PRA and in the RIBP evaluation of DID as part of the approach to addressing uncertainties in the estimation of LBE frequencies and consequences, including uncertainties in the mechanistic source terms. Applicable standards for performing these analyses are covered in ASME/ANS-RA-S-1.4. Guidance for performing uncertainty analysis in the PRA is available in NUREG-1855. Insights from the uncertainty analysis are also an important input to the RIPB evaluation of DID.

From the RSFs, a top-down logical development is used to define the functional requirements that are fulfilled for the reactor design to meet each RSF. The RFDCs are viewed as functional criteria that are defined in the context of the specific reactor design features that are necessary and sufficient to meet the RSF. The corresponding SRDCs are developed from the RFDCs.

4.4.2 Design Requirements for Safety-Related SSCs

For each of the RFDCs, a set of SRDCs appropriate to the SR SSCs is assigned to perform the RSFs.

The design requirements are performance-based and tied to RSFs, derived from the LBEs, and used to systematically select the SR SSCs.

4.4.3 Evaluation of SSC Performance Against Design Requirements

Although the SR SSCs are derived from an evaluation of the RSFs to mitigate the DBEs and DBAs, the SR and nonsafety-related SSCs are evaluated against the full set of LBEs including the AOOs and BDBEs, at the plant level to ensure that the F-C Target is met. This leads to design requirements for both the SR and nonsafety-related SSCs across the full set of LBEs, including the DBAs.

4.4.4 Barrier Design Requirements

SSCs that provide functions that support the retention of radioactive material within barriers have associated regulatory design requirements that are derived from the evaluation of the LBE against the F-C Target and the RFDCs. These functions include barrier functions in which the SSC serves as a physical or functional barrier to the transport of radionuclides and indirect functions in which performance of an SSC function serves to protect one or more other SSCs that are classified as barriers. However, a more complete perspective on the role of barriers and the SSCs that protect each barrier considers the barrier response to each of the LBEs derived from the PRA. The LBEs delineate the barrier failure modes, the challenges to barrier integrity, and the interactions between SSCs that influence the effectiveness of each barrier within a given layer of defense and the extent of independence among layers of defense. The evaluation of mechanistic source terms that help determine the offsite doses provides another performance metric for evaluating the effectiveness of each barrier within a given layer of defense.

When viewed across all the LBEs, each barrier plays a specific role within a given layer of defense in the retention of radionuclides; however, those roles are different in different LBEs. A full picture of the synergistic roles that each of the SSCs that comprise these layers of defense plays considers the way in which the SSCs mutually support the FSF of radionuclide retention.

Some functional barriers are different from the physical barriers frequently employed in the past. The term “barrier” is used to denote any plant feature within a given layer of defense that is responsible for either prevention of radionuclide release or reduction in the quantity of radionuclide release during an event. It comprises physical barriers and any other features that are responsible for mitigating the quantity of material released, including time delays that permit radionuclide decay.

In summary, the definition of requirements for barriers cannot be fully developed simply by examining the capability of discrete physical barriers to retain radionuclides. It is important to assure that barriers and other contributions to layers of defense are functionally independent. The systematic development of SSC design requirements considers the full spectrum of barrier challenges, barrier interactions, and barrier dependencies within layers of defense. The full examination of the barrier challenges, interactions and dependencies includes the performance of a technically sound PRA. Hence, it is logical that the approach to formulating requirements for barriers and other SSCs be linked to a systematic identification and evaluation of LBEs supported by a PRA.

4.4.5 Special Treatment Requirements for SSCs

Purpose of Special Treatment

The purpose of special treatment is reflected in the Regulatory Guide 1.201 definition of this term:

> *"…special treatment refers to those requirements that provide increased assurance beyond normal industrial practices that structures, systems, and components (SSCs) perform their design-basis functions."*

In the context of this process, special treatment is realized by the measures taken to provide reasonable confidence that SSCs will perform their functions reflected in the LBEs. The applicable functions include those that are necessary to prevent IEs and event sequences and other functions needed to mitigate the impacts of IEs on the performance of SFs. Assurance is accomplished by achieving and monitoring the capabilities of the SSCs in the performance of their mitigation functions with adequate margins to address uncertainties. Assurance is further accomplished by monitoring the levels of reliability and availability that are assessed in the PRA and that are determined to be necessary to meet the LBE risk evaluation criteria. These measures are focused on the prevention functions of the SSCs. The relationships between SSC reliability and capability in the performance of functions that are needed to prevent and mitigate event sequences are defined further in the next section.

The activities above are a subpart of the overall set of programmatic activities included design, manufacturing, construction, and operations of the plant that provide greater assurance that the plant capabilities and performance outcomes remain within the design basis. The broader list of possible programmatic actions shown in Table 4-1 are evaluated as part of the DID adequacy evaluation described in Section 5. NEI 18-04 has a table summarizing special treatments for SSCs that includes regulatory guidance. That list of regulatory guidance was not included in Table 4-1 so that it would not be confused with regulatory commitment. The set of special treatments applied to a given SSC are determined on a case by case basis and are influenced by RIPB considerations described in the following sections.

Relationship Between SSC Capability, Reliability, Mitigation, and Prevention

The safety classification of SSCs is made in the context of how the SSCs perform specific SFs for each LBE in which they appear. The reliability of the SSC serves to prevent the occurrence of the LBE by lowering its frequency of occurrence. If the SSC function is successful along the event sequence, the SSC helps to mitigate the consequences of the LBE.

The safety classification process and the corresponding special treatments control the frequencies and consequences of the LBEs within the F-C Target and also ensure that the cumulative risk targets are not exceeded. The LBE frequencies are a function of the frequencies of Initiating Events resulting from internal events, internal hazards, and external hazards, as well as the reliabilities and capabilities of the SSCs (including the operator) to prevent and mitigate the LBE. The SSC capabilities include the ability to prevent an Initiating Event from progressing to an event sequence, to mitigate the consequences of an event sequence, or both. In some cases, the Initiating Events are failures of SSCs themselves, in which case the reliability of the SSC in question serves to limit the Initiating Event frequency. In other cases, the Initiating Events represent challenges to the SSC in question, in which case the reliability of the SSC to perform a SF in response to the Initiating Event is considered. Finally, there are other cases in which the challenge to the SSC in question is defined by the combination of an Initiating Event and combinations of successes and failures of other SSCs in response to the Initiating Event. All of these cases are included in the PRA and represent the set of challenges presented to a specific SSC.

Role of SSC Safety Margins

SSC safety margins play an important role in the development of SSC design requirements for reliability and performance capability. Acceptance of plant performance is demonstrated with safety margins to adverse consequences for all the LBEs in which the SSC performs a prevention or mitigation function. The magnitudes of the safety margins in performance are evaluated in the context of the uncertainties in performance, the nature of the associated LBEs, and criteria for adequate DID. The ability to achieve the acceptance criteria in turn reflects the design margins that are part of the SSC capability to mitigate the challenges reflected in the LBEs.

Safety margins are also used in the selection of reliability performance targets. The reliability targets are set to ensure that the underlying LBE frequencies and consequences meet the LBE evaluation criteria with sufficient margins. These safety margins are also assessed in the DID evaluation.

Safety margins are also used in the evaluation of margins between the frequencies and consequences of the LBEs and the F-C Target and the margins between the cumulative risk metrics and the cumulative risk targets used for LBE evaluation. These risk margins are assessed as part of the RIPB evaluation of DID.

Specific Special Treatment Requirements for SR and NSRST SSCs

The applicability of special treatment to the SSC safety categories is provided in Table 4-1. The applicability of special design requirements treatment to any SSC is evaluated on a case-by-case basis and in the context of the SSC functions in the prevention and mitigation of applicable LBEs.

The purpose of any special treatment requirement is to provide adequate assurance that the SSC will perform its functions in the prevention and mitigation of LBEs. Each requirement is intended to assure that the SSC has adequate reliability and capability to perform these functions.

Reliability Assurance for SSCs

All safety-significant SSCs, including those in the SR and NSRST categories, are included in a Reliability Assurance Program (RAP) similar to that described in SRP NUREG-0800, Section 17.4. The reliability and availability targets established in the RAP are used to focus the selection of special treatments that are necessary and sufficient to achieve these targets and to assure they are maintained for the life of the plant.

Capability Targets for SSCs

All safety-significant SSCs, including those in the SR and NSRST categories, have the capability to perform the SFs to mitigate the challenges reflected in the LBEs responsible for the safety classification. SR SSCs are capable of mitigating the DBAs within the 10 CFR 50.34 dose limits. These SR SSCs include appropriate RFDC for such functions. The guiding principle is that the requirements are performance-based and yield high confidence that the SSC functions are performed during the identified LBEs.

Capability and reliability targets for SR and NSRST SSCs refer back to the LBEs that challenge them, so through this path, some hazards, including area hazards such as pipe whip or spatial placement of a NSRST component above an SR component, may lead to specific special treatment requirements.

Table 4-1. Summary of Special Treatments for SR and NSRST SSCs

Special Treatment Category	Applicability[1]		
	SR SSC	NSR ST SSC	NST SSC
Requirements Associated with SSC Safety Classification			
Document basis for SSC categorization by Integrated Decision-Making Panel[4]	√	√	√
Document evaluation of adequacy of special treatment to support SSC categorization	√	√	
Change control process to monitor performance and manage SSC categorization changes	√	√	
Basic Requirements for all Safety-Significant SSCs			
Reliability Assurance Program including reliability and availability targets for SSCs in performance of SFs	√	√	
Design Requirements for SSC capability to mitigate challenges reflected in LBEs	√	√	
Maintenance Program that assures targets for SSC availability and effectiveness of maintenance to meet SSC reliability targets	√	√	
Licensee Event Reports	√	√	
10 CFR 50 Appendix B Quality Assurance Program	√		
KP-FHR Quality Assurance (QA) Program for nonsafety-related SSCs with special treatment		√	
Additional Special Treatment Requirements			
Required Functional Design Criteria	√		
Technical Specifications	√	[2]	
Seismic design basis	√	[3]	[3]
Seismic qualification testing	√		
Protection against design basis external events	√		
Equipment qualification testing	√		
Materials surveillance testing	√		
Pre-service and in-service inspections	√	[2]	
Pre-service and in-service testing	√	[2]	

[1] The applicability of each category of special treatment to any SSC is indicated by the check marks in this table. The specific requirements for each applicable category is evaluated on a case-by-case basis and in the context of the SSC functions in the prevention and mitigation of

Special Treatment Category	Applicability[1]		
	SR SSC	NSR ST SSC	NST SSC
applicable LBEs. This is determined in the design and confirmed via an integrated decision-making process. [2] The need for this special treatment for any NSRST is determined on a case-by-case basis, and when applicable, is applied to the specific functions to prevent and mitigate the applicable LBEs. This is determined via an integrated decision-making process. [3] SR-classified SSCs are required to perform their RSFs following a Safe Shutdown Earthquake; NSRST and NST SSCs required to meet Seismic II/I requirements (required not to interfere with the performance of SR SSC RSFs following a Safe Shutdown Earthquake). [4] Integrated Decision-Making Panels are discussed more fully in Section 5.3 and are similar to those described in NEI-00-04.			

Figure 4-1. SSC Function Safety Classification Process

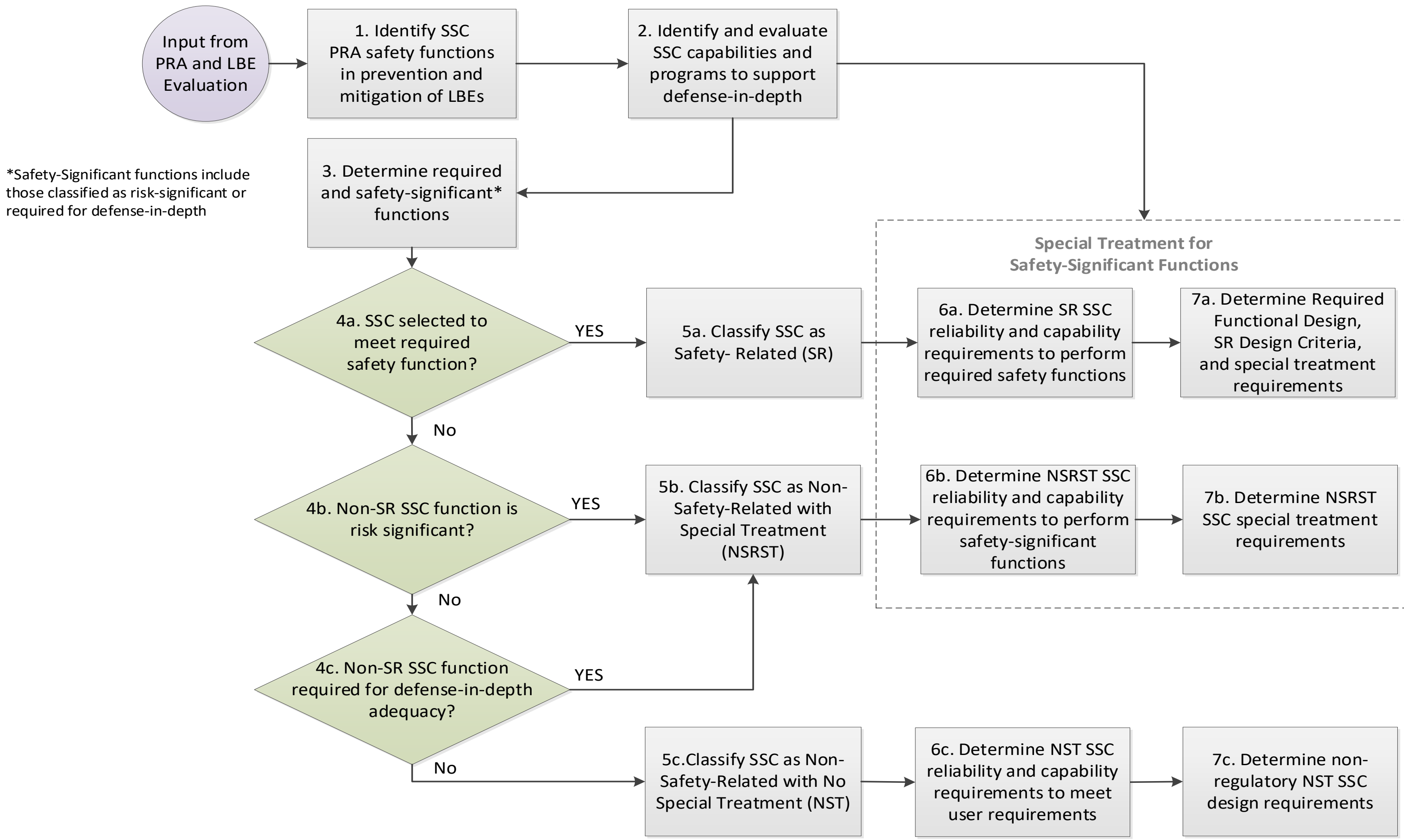


Figure 4-2. Relationship of Risk-Significant and Safety-Significant SSCs

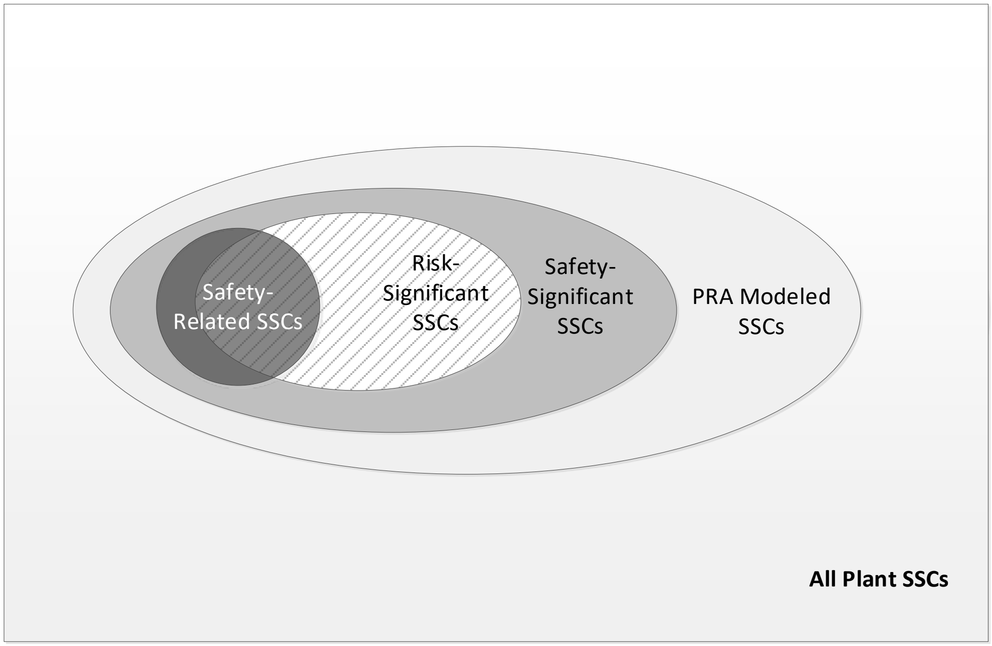
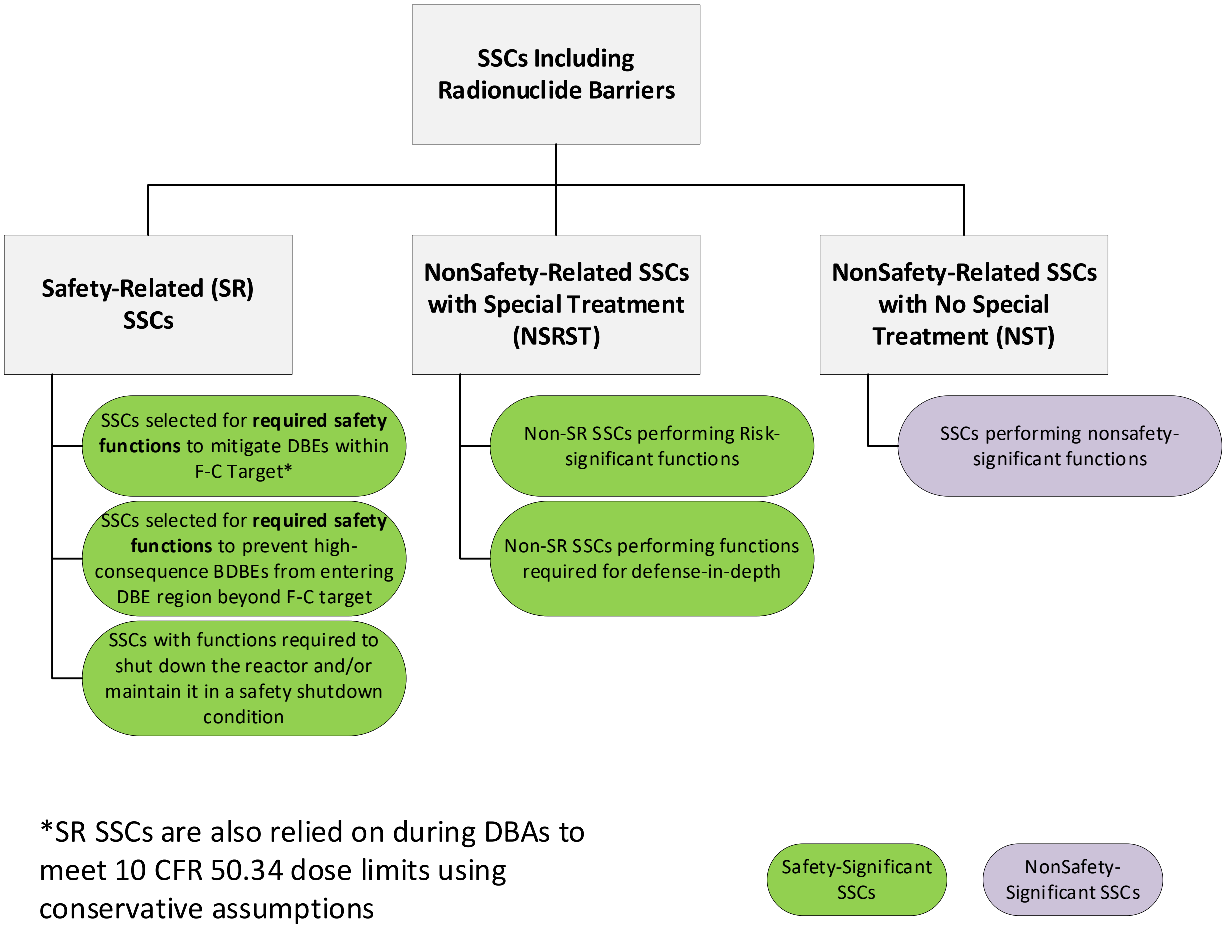


Figure 4-3. SSC Safety Categories



5 EVALUATION OF DEFENSE-IN-DEPTH ADEQUACY

The philosophy of defense-in-depth, multiple independent but complementary means for protecting the public from potential impacts from nuclear reactor operation, has historically been applied. The process described in this section provides an objective assessment of DID adequacy that permits the establishment of DID in design, construction, maintenance, and operation of nuclear facilities. Achievement of DID occurs when all stakeholders make clear and consistent decisions regarding DID adequacy as an integral part of the overall design process.

Establishing DID adequacy involves incorporating DID design features, operating and emergency procedures, and other programmatic elements. DID adequacy is evaluated by using a series of RIPB decisions regarding design, plant risk assessment, selection and evaluation of LBEs, safety classification of SSCs, specification of performance requirements for SSCs, and programs to ensure these performance requirements are maintained throughout the life of the plant.

5.1 DEFENSE-IN-DEPTH PHILOSOPHY

According to the NRC glossary, defense-in-depth is:

> *"…an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense in depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures."*

Figure 5-1 illustrates the concept of layers of defense embodied in this philosophy taken from NUREG/KM-0009 "*Historical Review and Observations of Defense-in-Depth*." This process is consistent with the "levels of defense" concept advanced by the 2005 IAEA Safety Report Series No. 46, "*Assessment of Defense in Depth for Nuclear Power Plants*" (Reference 8).

This process for establishing DID adequacy embraces the concept of layers of defense and uses these layers to identify and evaluate DID attributes.

5.2 FRAMEWORK FOR ESTABLISHING DID ADEQUACY

This process for evaluation of DID adequacy is outlined in Figure 5-2. The elements of the process are described below.

Plant Capability Defense-in-Depth

This element is used to select functions, SSCs, and their bounding design capabilities to assure safety adequacy. Additionally, excess capability, reflected in the design margins of individual SSC and the use of redundancy and diversity, is important to the analysis of beyond design basis conditions that could arise. This reserve capacity to perform in severe events is consistent with the DID philosophy for conservative design capabilities that enable successful outcomes for unexpected events should they occur. Plant capability DID is divided into the following categories:

- Plant Functional Capability DID—This capability is introduced through systems and features designed to prevent occurrence of undesired LBEs or mitigate the consequences of such events.

- Plant Physical Capability DID—This capability is introduced through SSC robustness and physical barriers to limit the hazard consequences.

These capabilities, when combined, create layers-of-defense responses to plant challenges.

Programmatic Defense-in-Depth

Programmatic DID is used to address uncertainties when evaluating plant capability DID as well as when programmatic protective strategies are defined. It provides a means to incorporate special treatment while designing, manufacturing, constructing, operating, maintaining, testing, and inspecting the plant and the associated processes to ensure there is reasonable assurance that the predicted performance can be achieved throughout the lifetime of the plant. According to Regulatory Guide 1.201, "…special treatment refers to those requirements that provide increased assurance beyond normal industrial practices that SSCs perform their design-basis functions". The use of performance-based measures, where practical, to monitor plant parameters and equipment performance that have a direct connection to risk management and to equipment and human reliability are considered essential.

Risk-Informed Evaluation of Defense-in-Depth

This element provides a systematic and comprehensive process for examining the DID adequacy achieved by the combination of plant capability and programmatic elements. This evaluation is performed by a risk-informed (RI) integrated decision-making process to assess sufficiency of DID and to enable consideration of different alternatives for achieving commensurate safety levels at reduced burdens. The outcome of the RI process also establishes a DID baseline for managing risk throughout the plant lifecycle.

The concept of using the layers of defense for performing the RIPB evaluation of plant capabilities and programs, which has been adapted from the IAEA "levels of defense" approach, is shown in Figure 5-3.

This framework sets the context to evaluate each LBE and to identify the DID attributes that have been incorporated into the design to prevent and mitigate event sequences and to ensure that they reflect adequate SSC reliability and capability. Those LBEs with the highest levels of risk significance are given greater attention in the evaluation process.

As explained more fully in the sections on PRA development, LBE selection and evaluation, and SSC safety classification, the PRA is used together with traditional deterministic safety approaches to affect a risk-informed process, as indicated in the center of Figure 5-2. The PRA is not employed simply to calculate numerical risk metrics, it is also used to develop risk insights into the design and to identify sources of uncertainty in the PRA models and supporting data that complement the deterministic elements of the process. The DID evaluation includes the identification of compensating protective measures to address the risk-significant sources of uncertainty in both the frequency and consequence estimates.

5.3 INTEGRATED FRAMEWORK FOR INCORPORATION AND EVALUATION OF DID

DID is considered and incorporated into all phases of defining the design requirements, developing the design, evaluating the design from both deterministic and probabilistic perspectives, and defining the programs to ensure adequate public protection. DID is achieved through the incorporation of DID features and programs in the design and in turn, conducting the evaluation that arrives at the decision of whether adequate DID has been achieved. The formation of an Integrated Decision-Making Panel (IDP) reviews the outputs of the overall design effort (including development of plant capability and programmatic DID features), conducts the DID adequacy evaluation of the resulting design, and ensures the DID baseline is documented.

The incorporation of DID in each component of this process is illustrated in Figure 5-4, and the key elements of each task in the figure are summarized below. Note that Figure 5-4 includes many actions described previously and does not imply that these steps are re-performed for the purpose of the DID adequacy evaluation. The color coding in the figure identifies elements that are probabilistic, deterministic, and risk-informed (i.e., having both probabilistic and deterministic aspects). The implementation of the process is not a series of discrete tasks but rather an iterative process. As shown by the ‘Triangle A’ icons in the figure, this iteration is expected to occur repeatedly and at different tasks in the overall process. Iteration through the tasks is expected to continue through the documentation of the DID baseline in Task 18, and then with subsequent DID baseline updates as the design progresses. The sequence of tasks reflects more an information logic than a step-by-step procedure. The execution of the DID elements is accomplished in the context of an integrated decision-making process throughout the plant design and operation lifecycle.

Under this process, the IDP is responsible for evaluating the adequacy of DID; similar to the processes used by currently operating plants to guide risk-informed changes to the licensing basis, such as risk-informed safety classification under 10 CFR 50.69. The Industry has developed procedures and guidelines for the makeup and responsibilities of such panels. These panels or teams have been found acceptable by the NRC in specific licensee 10 CFR 50.69 programs. The IDP is comprised of a team that is responsible for evaluating the DID adequacy of the integrated process tasks shown in Figure 5-4. This cross-functional team is staffed with expert, plant knowledgeable members whose expertise includes PRA, safety analysis, plant operation, design engineering, and system engineering.

Task 1: Establish Initial Design Capabilities

The process begins in Task 1 with available design information. Top-level requirements are formulated with input from all stakeholders, including owner requirements for such things as energy production, capital costs, operating and maintenance costs, safety, availability, investment protection, siting, and commercialization requirements. DID adequacy is given high priority early in the design.

Even though many of these requirements are not directly associated with meeting licensing requirements, they often contribute to DID. Owner requirements for plant availability and reliability contribute to protecting the first layer of defense of DID in Figure 5-4 by controlling plant disturbances and preventing some IEs and AOOs.

The inherent reactor characteristics for the design are determined by the early fundamental design decisions to address owner requirements, operating experience, studies of technology maturity, system engineering requirements, and safety objectives.

At an early stage of design, a comprehensive set of plant-level and system-level functional requirements are developed. This task includes the identification of systems and components and their functions, including energy production functions, maintenance functions, auxiliary functions, and SFs and an identification of hazards associated with these SSCs. This is a purely deterministic task that produces a definition of the design in sufficient detail to begin the PRA.

The selection of inherent reactor characteristics, primary heat transport system design parameters, and materials for SSCs dictates the safe, stable operating states for the reactor. Considerations of the need for periodic inspections and maintenance, Operations and Maintenance (O&M) procedures, methods for starting up, shutting down, load following, and mode transitions are used to make decisions about the modes and states that are considered to complete the functional design and to perform the subsequent evaluations.

As part of the pre-conceptual or conceptual design, a great deal of the DID capability is naturally established by addressing the fundamental top-level design requirements for operability, availability, maintainability, and investment protection features using conventional practices, industry codes and standards, etc. Additional plant capabilities as well as programs and compensating measures are added as a result of maturing probabilistic and deterministic evaluations of plant safety and DID in subsequent tasks.

Initially, decisions on the design and selection of codes and standards that influence design and some baseline level of special treatment are made. For example, certain parts of ASME design codes for certain SSCs which may be linked to ASME requirements for in-service inspection may be selected. Provisions are made in the design and the definition of modes and states to perform the required inspections. Final decisions on the frequency and extent of inspections are made in Task 14. The full extent of special treatment is defined following the evaluation of LBEs and the selection of SSC safety classes for each SSC. Hence, selection of codes and standards supports both the plant capabilities for DID and the activities that contribute to the programmatic DID.

As noted previously, establishing DID capabilities in the plant design is an iterative process. Some portions of the design advance earlier than others. As a result, some of the activities in Figure 5-4 are updated in parallel. Thus, the IDP process recurs more often than the serial picture shown in the figure as more and more of the design is completed and integrated evaluations of performance and DID become more robust.

Task 2: Establish F-C Target Based on Regulatory Objectives and QHOs

The F-C Target and QHOs (cumulative risk targets) are described in Section 3.

Task 3: Define SSC Safety Functions for PRA Modeling

The KP-FHR specific SFs are identified in Task 3. All reactors are designed to meet certain Fundamental Safety Functions such as retention of radioactive material, decay heat removal, and reactivity control (the term “Fundamental Safety Function” is used extensively in IAEA publications such

"*Proposal for a Technology-Neutral Safety Approach for New Reactor Designs,"* Technical Report IAEA-TECDOC-1570 (Reference 5). The functions listed are the ones regarded as fundamental and are applicable to all reactor technologies.) However, application of the reactor-specific safety design approach leads to a set of reactor-specific SFs that achieve the FSFs. During this process, the allocation of these SFs to both passive and active SSCs is confirmed. The top-level design criteria are also confirmed for all the SSCs selected to perform the reactor-specific SFs. As Task 3 is completed, the plant capabilities that support DID are largely determined. Adjustments are made to address the results of subsequent evaluations or design iterations that may expose weaknesses in design or operating assumptions or expose margin or other uncertainties that are relevant to demonstrate adequate levels of safety and sufficient DID.

Task 4: Define Scope of PRA for Current Design Phase

In the initial stages of the design, an evaluation is made to decide the scope of the PRA. This includes identifying the hazards, IEs, and event sequences to consider within the design basis and for designing specific measures to prevent and mitigate off-normal events and event sequences.

Task 5: Perform PRA

The performance of the current phase of the PRA is covered in this task consistent with the process described in Sections 3 and 4. Information from the PRA is used together with deterministic inputs to establish DID adequacy as part of the RIPB evaluation of DID depicted in Tasks 12 and 17. The PRA is used together with traditional deterministic safety approaches to affect a risk-informed process. The PRA is not employed simply to calculate numerical risk metrics, but also to develop risk insights into the design and to identify sources of uncertainty in the PRA models and supporting data that complement the deterministic elements of the process. The DID evaluation includes the identification of compensating protective measures to address the risk-significant sources of uncertainty in both LBE frequencies and consequences.

Task 6: Identify and Categorize LBEs as AOOs, DBEs, or BDBEs

The process for identifying and categorizing the LBEs in terms of AOOs, DBEs, and BDBEs is discussed in Section 3 of this document.

Task 7: Evaluate LBE Risks vs. F-C Target

An important input in evaluating DID adequacy is establishment of adequate margins between the risks of each LBE and the F-C Target. Such margins help demonstrate the level of satisfaction of the NRC's advanced reactor policy objective of achieving higher margins of safety. In this process, the most risk-significant LBEs are identified. These provide a systematic means to focus more attention on those events that contribute the most to the design risk profile.

Task 8: Evaluate Plant Risks vs. Cumulative Risk Targets

In addition to establishing adequate margins between the risks of individual LBEs and the F-C Targets, the evaluation of the margins against the cumulative risk metrics identified previously is also used to establish DID adequacy.

Task 9: Identify DID Layers Challenged by Each LBE

The layers of defense process in Table 5-3 are used in this task to evaluate each LBE with more attention given to risk-significant LBEs to identify and evaluate the DID attributes to support the capabilities in each layer and to minimize dependencies among the layers.

Task 10: Select Safety-Related SSCs and Define DBAs

The selection of SR SSCs is confirmed by examining each of the DBEs and high-consequence BDBEs and by performing sensitivity analyses to demonstrate that the RSFs modeled in these LBEs are necessary to perform their prevention or mitigation functions to keep the DBEs and high-consequence BDBEs inside the F-C Target. Those SFs are classified as RSFs. In general, there may be two or more different sets of SSCs that could provide these RSFs. Those functions specified by the design team (represented on the IDP) select the SSCs that can support the RSFs for all the DBEs and high-consequence BDBEs and designate them as SR. DBAs are then constructed, starting with each DBE, and then assuming that only the SR SSCs perform their associated RSFs. DID considerations are taken into account in the selection of SR SSCs by selecting those that yield high confidence in performing their functions with sufficient reliability to minimize uncertainties.

Task 11: Perform Safety Analysis of DBAs

Conservative deterministic safety analyses of the DBAs are performed in a manner that is analogous to that for current generation LWRs in this task. The conservative assumptions used in these analyses make use of insights from the PRA, which include an analysis of the uncertainties in the plant response to events, mechanistic source terms, and radiological consequences. Programmatic DID considerations are taken into account in the formulation of the conservative assumptions for these analyses which need to show that the site boundary doses meet 10 CFR 50.34 acceptance limits.

Task 12: Confirm Plant Capability DID Adequacy

At this task, there is sufficient information, even during conceptual design, to evaluate the adequacy of the plant capabilities for DID using information from the previous tasks and guidelines for establishing the DID adequacy. This task is supported by the results of the systematic evaluation of LBEs using the layers of defense process in Task 9. As part of the DID adequacy evaluation, each LBE is evaluated to confirm that risk targets are met without exclusive reliance on a single element of design, a single program, or a single DID attribute.

Task 13: Identify Nonsafety-related with Special Treatment SSCs

All the SSCs that participate in a layer of defense are generally not classified as SR. However, these SSCs are evaluated against criteria for establishing SSC risk significance and additional criteria for whether the SSC provides a function necessary for DID adequacy. Criteria for classifying SSCs as safety-significant based on DID considerations are presented in Section 4. SSCs not classified as SR or NSRST are classified as NST. None of the NST SSCs are regarded as safety-significant, even though they may contribute to the plant capability for DID. All of the safety-significant SSCs are classified as either SR or NSRST.

Task 14: Define and Evaluate Required Functional Design Criteria for SR SSCs

RFDC provide a bridge between the DBAs and the formulation of SRDC for the SR SSCs. DID attributes such as redundancy, diversity, and independence, and the use of passive and inherent means of fulfilling RSFs are used in the formulation of RFDCs.

Task 15: Evaluate Uncertainties and Margins

One of the primary motivations of employing DID attributes is to address uncertainties, including those that are reflected in the PRA estimates of frequencies and consequence as well as other uncertainties which are not sufficiently characterized for uncertainty quantification nor amenable to sensitivity analyses. The plant capability DID includes design margins that protect against uncertainties. The layers of defense within a design, including offsite response, are used to compensate for residual unknowns. The approach to identifying and evaluating uncertainties that are quantified in the PRA and used to establish protective measures reflected in the plant capability and programmatic elements of DID is described throughout Section 5.

Task 16: Specify Special Treatment Requirements for SR and NSRST SSCs

All safety-significant SSCs that are distributed between SR and NSRST are subject to special treatment requirements. These requirements include specific performance requirements to provide adequate assurance that the SSCs are capable of performing their SFs with significant margins and with appropriate degrees of reliability. Another consideration in the setting of SSC performance requirements is the need to assure that the results of the plant capability DID evaluation in Task 12 are achieved not just in the design, but in the as-built and as-operated and maintained plant throughout the life of the plant. The SSC performance targets are set in the design of the SSC and confirmed by the IDP that is responsible for establishing the adequacy of DID. In addition to these performance targets, further special treatments may be identified.

Task 17: Confirm Programmatic DID Adequacy

The adequacy of the programmatic measures for DID is driven by the selection of performance requirements for the safety-significant SSCs in Task 16. The programmatic measures are evaluated relative to the risk significance of the SSCs, the roles of SSCs in different layers of defense, and the effectiveness of special treatments in providing additional confidence that the risk-significant SSCs will perform as intended.

Task 18: DID Adequacy Established; Document/Update DID Baseline Evaluation

The RIPB evaluation of DID adequacy continues until the recurring evaluation of plant and programmatic DID associated with design and PRA update cycles no longer identifies risk-significant vulnerabilities where potential compensatory actions make a practical, significant improvement to the LBE risk profiles or risk significant reductions in the level of uncertainty in characterizing the LBE frequencies and consequences. At this point, a DID baseline is finalized to support the final design and operations the plant.

The successful outcomes of Tasks 12 and 17 establish DID adequacy. This determination is made by the IDP and documented initially in a DID integrated baseline evaluation report which is subsequently revised as the iterations through the design cycles and design evaluation evolve.

5.4 HOW MAJOR ELEMENTS OF THE RIPB FRAMEWORK ARE EMPLOYED TO ESTABLISH DID ADEQUACY

As shown in Table 5-1, there are important DID roles in each major element of the process. The IDP uses information and insights in each of these elements to support a risk-informed and performance-based evaluation of DID adequacy. As indicated in Figure 5-2, RIPB decisions that are made in this evaluation feedback any necessary changes to the DID attributes reflected in the plant capability and programmatic elements of DID.

5.5 RIPB COMPENSATORY ACTION SELECTION AND SUFFICIENCY

The DID evaluation, including compensatory action selection and sufficiency, is depicted as the more detailed process shown in Figure 5-2 using information as it is developed in the design process to adjust the plant capability features or programmatic actions as the state of DID knowledge improves with the design evolution.

5.6 ESTABLISHING THE ADEQUACY OF PLANT CAPABILITY DID

The RIPB evaluation of DID adequacy is complete when the recurring evaluation of plant capability and programmatic capability associated with design and PRA update cycles no longer identifies risk-significant vulnerabilities where potential compensatory actions make a practical, significant improvement to the LBE risk profiles or risk-significant reductions in the level of uncertainty in characterizing the LBE frequencies and consequences. The IDP is responsible for making the deliberate, affirmative decision that DID adequacy is achieved. This decision is recorded, including the bases for this decision, in a configuration-controlled document. At this point, the DID baseline is finalized to support the operational phase of the plant.

5.6.1 Guidelines for Plant Capability DID Adequacy

The process for establishing plant capability DID begins in the development of the safety design approach and is accomplished in the course of the iterative process tasks leading up to the selection and evaluation of LBEs. It is also impacted by SSC safety classification. Task 7e represents the task in the LBE evaluation in which the plant capability for DID is assessed. As discussed in the NRC documents that describe the DID philosophy, layers and DID attributes play a significant role in the approach to DID capability. However, there do not exist well-defined regulatory acceptance criteria for deciding the sufficiency of the DID for nuclear power plant licensing or operation.

To support the design and licensing of KP-FHR within this process, a set of DID adequacy guidelines is provided. The guidelines, presented in Table 5-2, are used as a basis for initially evaluating the adequacy of plant capability DID and are confirmed during the regulatory review as appropriate and sufficient.

5.6.2 DID Guidelines for Defining Safety-Significant SSCs

As discussed in Section 4, SSCs are classified as safety-significant if they perform one or more risk-significant functions or provide a function or functions that are necessary for DID adequacy. The guidelines in Table 5-2 require that two or more independent plant design or operational features are necessary to satisfy the requirements. For the inherent capabilities of passive functions, degradation of the passive function is considered, as opposed to complete failure (i.e., a physical non-existence of that function). As degradation or failure of plant design or operational features are analyzed against the frequency-based guidelines in Table 5-2, the analysis should be kept in the context of risk added from these plant disruptions (i.e., certain LBEs may exceed the frequency thresholds but not carry any consequence). In the case of design changes, where risk is not increased as a result of a frequency increase, additional requirements on SSC classification or other operational solutions may not be needed. The integrated design process may determine whether additional requirements on SSCs (e.g., elevating classification) or other operational programs are needed to meet the Table 5-2 guidelines. The integrated design process may also determine that no further design requirements or operational programs are needed, or that previously identified requirements and operational programs are no longer needed to assure DID adequacy as described in Section 5.9.

Non SR SSCs that perform a function or functions that are necessary for DID adequacy are classified as NSRST. Special treatment requirements for NSRST SSCs include the setting of performance requirements for SSC reliability, availability, and capability and any other treatments deemed necessary by the IDP responsible for guiding the integrated design process in Figure 5-4 and evaluating DID adequacy.

5.6.3 DID Attributes to Achieve Plant Capability DID Adequacy

The evaluation of plant capability DID adequacy focuses on the completeness, resiliency, and robustness of the plant design with respect to addressing hazards, responding to identified IEs, preventing and mitigating the progression of IEs through the availability of independent levels of protection, and achieving sufficient protection of public health and safety through the use of redundant and diverse means. Additionally, the evaluation determines whether a single feature is excessively relied upon to achieve public safety objectives, and if so, identifies options to reduce or eliminate such dependency. The completion of the evaluation supports an appropriate safety design adequacy determination and ultimate finding that a plant poses no undue risk to public health and safety.

Table 5-3 lists the plant capability DID attributes and principal evaluation focus areas included in the DID evaluation scope. The evaluation of plant capability involves the systematic evaluation of hazards over the spectrum of all modes and states including anticipated transients and potential event sequences within and beyond the design basis.

5.7 EVALUATION OF LBES AGAINST LAYERS OF DEFENSE

A central element of the RIPB evaluation of DID is a systematic review of the LBEs against the layers of defense. This review is necessary to evaluate the plant capabilities for DID and to identify programmatic DID measures that may be necessary for establishing DID adequacy. In meeting its objectives, the review performs the following:

- Confirms that plant capabilities for DID are deployed to prevent and mitigate each LBE at each layer of defense challenged by the LBE.
- Confirms that a balance between event prevention and mitigation is reflected in the layers of defense for risk-significant LBEs.

- Identifies the reliability/availability missions of SSCs that perform prevention and mitigation functions along each LBE and confirm that these missions can be accomplished. A reliability/availability mission is the set of targets related to the performance, reliability, and availability of an SSC function that adequately ensures the accomplishment of its task, as defined by the PRA or deterministic analysis.

- Confirms that adequate technical bases for classifying SSCs as SR or NSRST exist and their capabilities to execute the RSFs are defined.

- Confirms that the effectiveness of physical and functional barriers to retain radionuclides in preventing or limiting release is established.

- Reviews the technical bases for important characteristics of the LBEs with focus on the most risk-significant LBEs, and LBEs with relatively higher consequences (LBEs with site boundary doses exceeding 1 rem TEDE, the lower Environmental Protection Agency (EPA) Protective Action Guideline (PAG) dose, are regarded as having relatively high consequences for this purpose). The technical bases for relatively high-frequency LBEs that are found to have little or no release or radiological consequences are also a focus of the review.

- Confirms that risk-significant sources of uncertainty in both the frequency and consequence estimates that need to be addressed via programmatic and plant capability DID measures are adequately addressed.

An important consideration in the safety classification of SSCs and in the formulation of SSC performance requirements is the understanding of the roles of SSCs modeled in the PRA in the prevention and mitigation of IEs and event sequences. This understanding is the basis for the formulation of the SSC capability targets for mitigation of the challenges represented in the LBEs as well as the reliability targets to prevent LBEs with more severe consequences. This understanding is also important in recognizing how the plant capabilities for DID achieve an appropriate balance between event prevention and mitigation across different layers of defense, which permits an examination of the plant capabilities evaluation in the context of the layers of defense that are delineated in Figure 5-3.

NEI 18-04 contains some general guidance in Section 5.7 for defense in depth layers and source term that do not translate to specific actions or documentation for this process. Detail on the mechanistic source term approach for the KP-FHR will be provided as part of future licensing submittals.

5.7.1 Evaluation of LBE and Plant Risk Margins

This section explains how margins are established between the frequencies and consequences of individual LBEs and the F-C Target used to evaluate the risk significance of LBEs. These margins are established for the LBEs having the highest risk significance within each of the three LBE categories (AOOs, DBEs, and BDBEs).

Margins are developed in two forms. The margins to the F-C Target are measured based on mean values of the LBE frequencies and doses. In each case, margin is expressed as a ratio of the event's mean value (frequency and dose) to the corresponding F-C Target value (frequency and dose).

A more conservative evaluation of margins, similar to the first form mentioned above, uses the 95th percentile upper bound values for both LBE frequency and dose to calculate the margins. This process is repeated for each individual LBE, grouped by LBE category as part of the DID evaluation during the design development.

5.7.2 Integrated Decision-Making Panel Focus in LBE Review

The evaluation of LBEs by the IDP focuses on the following questions:

- Is the selection of IEs and event sequences reflected in the LBEs sufficiently complete? Are the uncertainties in the estimation of LBE frequency, plant response to events, mechanistic source terms, and dose well characterized? Are there sources of uncertainty not adequately addressed?
- Have all risk-significant LBEs and SSCs been identified?
- Has the PRA evaluation provided an adequate assessment of “cliff edge effects?”
- Is the technical basis for identifying the RSFs adequate?
- Is the selection of the SR SSCs to perform the RSFs appropriate?
- Have protective measures to manage the risks of multi-reactor unit and multi-radiological source event sequences been adequately defined?
- Have protective measures to manage the risks of all risk-significant LBEs been identified, especially those with relatively high consequences?
- Have protective measures to manage the risks for all risk-significant common-cause IEs such as support system faults, internal plant hazards such as fires and floods, and external hazards been identified?
- Is the risk benefit of all assigned protective measures well characterized, e.g., via sensitivity analyses?

If the evaluation identifies unacceptable answers to any of these questions, additional compensatory action are considered, depending on the risk significance of the LBE. With reference to Figure 5-4, the compensatory action takes on different forms including changes to design and operation, refinements to the PRA, revisions to the selection of LBEs and safety classification of SSCs, and enhancements to the programmatic elements of DID.

5.8 ESTABLISHING THE ADEQUACY OF PROGRAMMATIC DID

5.8.1 Guidelines for Programmatic DID Adequacy

The adequacy of programmatic DID is based on meeting the following objectives:

- Assuring that adequate margins exist between the assessed LBE risks relative to the F-C Target including quantified uncertainties
- Assuring that adequate margins exist between the assessed total plant risks relative to the cumulative risk targets
- Providing adequate assurance that the risk, reliability, and performance margins are maintained throughout the life of the plant in design and operational programs with adequate consideration of sources of significant uncertainties

These objectives differ slightly from the objectives stated in NEI 18-04. The Kairos Power approach to establishing programmatic DID adequacy focuses activities on assuring that frequency targets are maintained at the event sequence level. At the more detailed SSC level, the focus shifts to performance-based measures such as surveillance frequency and test success rates.

Unlike the plant capabilities for DID that are described in physical terms and are amenable to quantitative evaluation, the programmatic DID adequacy is established using engineering judgment by determining what package of DID attributes are sufficient to meet the above objectives. These judgments are confirmed by the IDP using the programmatic DID attributes and evaluation considerations in Table 5-4.

The attributes of programmatic DID complement each other and provide overlapping assurance that the desired plant capability is achieved in design, manufacturing, construction, and operations lifecycle phases. The evaluation focus items provided in Table 5-4 are addressed for each programmatic DID attribute for risk-significant LBEs to determine that the programmatic DID provides reasonable assurance of adequate protection of public health and safety based on the plant capability. The net result establishing and evaluating programmatic DID is the selection of special treatment programs for all safety-significant SSCs including those classified as SR or NSRST.

5.8.2 Application of Programmatic DID Guidelines

The considerations discussed below are used in the evaluation of programmatic DID using the attributes in Table 5-4 and the questions raised in Table 5-5.

Quality and Reliability

The initial quality of the design is developed through the application of proven practices and application of industry codes and standards. In cases where no approved codes and standards are available, conservative adaptation of existing practices from other industries or first principles derivations of repeatable practices may be applied. Conservatisms are applied in cases where common practices and codes are not available. The use of new practices is validated to the degree practical against physical tests or other operating experiences if risk-significant SSCs are involved. The PRA considers the uncertainties of unproven methods or standards for specific risk-significant functions. This topic is examined by the IDP.

The primary focus on reliability in the evaluation of DID is on the establishment of the functional reliability targets for SSCs that prevent or mitigate risk-significant LBEs as part of a layer of defense and associated monitoring of reliability performance against the targets. The reliability is achieved by some combination of inherent, passive, or active SSC capabilities. The appropriate use of redundancy and diversity to achieve the reliability targets set by the IDP together with the plant technical specifications is evaluated.

Margin Adequacy

At the plant level, performance margins to established design goals and regulatory limits are evaluated as part of DID adequacy. At the individual SSC level, properly designing SSCs to proven codes and standards provides an appropriate level of assurance that the SSC will perform reliably at its design conditions and normally include reserve margin for more demanding conditions. The DID evaluation includes a determination that the appropriate codes were applied to safety-significant SSCs (included in SR and NSRST safety categories) and that the most demanding normal operation, AOO, DBE, or DBA parameters for that component, conservatively estimated, are used for the design point. For SSCs that play a role in risk-significant BDBEs, the DID evaluation evaluates the inherent performance margins in SSCs against the potentially more severe conditions of BDBEs in the PRA.

Treatment of Uncertainty in Programmatic DID

In judging DID adequacy, at each stage of design and operations, personnel continually keep in mind that errors are possible, equipment can fail, and real events do not always mimic analytical events. For that reason, the three questions of the risk triplet (what can go wrong, how likely is it, what are the consequences?) are part of deciding how to manage residual risk and uncertainty. The primary means of addressing these residual risks is through effective Severe Accident Management Programs and effective emergency planning. Siting considerations and emergency planning zone programs take into account the known risks of a plant, siting the plant in less populated areas and incorporating proactive emergency planning programs that ensure precautionary actions are taken well before a serious threat to public health can arise.

Compensation for Unknowns

The layers-of-defense approach utilized in the DID evaluation process includes the need to define protective measures to address unknowns. Feedback from actual operating and maintenance experience to the PRA provides performance-based outcomes that are part of plant monitoring. Periodic PRA updates incorporate that information into reliability (system or human) estimates to determine whether significant LBE risks have changed or new events have emerged. Relevant, known nuclear industry sources of information are utilized for known, risk-significant LBEs.

Operator and management training programs contain appropriate requirements for dealing with each identified risk-significant BDBE and include provision for event management of potential events undefined in the PRA due to truncation or other limitations in modeling or scope for this phase of the design/PRA development. The evaluation of programmatic DID determines whether risk-significant LBEs are included in the routine training of operators and management.

Programmatic DID in Design

Programmatic activities developed during design and licensing phases that are integral to the design process include design-sensitive programs such as:

- Development of risk-informed plant technical specifications
- Tier 1 and inspections, tests, analyses, and acceptance criteria
- Operating procedures including those for DBEs, DBAs and BDBEs
- Maintenance programs for safety-significant SSCs (SR and NSRST)
- In-service inspection and in-service testing programs

The early consideration of the use of RIPB practices to establish the scope of these types of programmatic actions support the more efficient implementation of physical design features in a manner that minimizes the scope of programmatic regulatory compliance activities and related burdens in the operational phase of the plant lifecycle.

Examples of special treatment programs are listed in Table 5-6. The actual special treatments are established and/or confirmed by the IDP. Each of these programs and treatments are programmatic DID protective measures that benefit from RIPB insights early in their development cycles in optimizing their value as part of an integrated risk management approach.

There are other programmatic activities spread across a broader portion of the industry that provide additional levels of programmatic DID and contribute to assurance of public protection. The NRC, Institute of Nuclear Power Operations, American Nuclear Insurers, and ASME all play an important part of assuring public safety through independent oversight and monitoring of plant development and operations. Included in some of these oversight activities are self-reporting requirements that notify NRC and other external agencies of unexpected or inappropriate performance of SSCs or human activities.

5.9 RISK-INFORMED AND PERFORMANCE-BASED EVALUATION OF DID ADEQUACY

5.9.1 Purpose and Scope of Integrated Decision-Making Panel Activities

In this process, the IDP is responsible for evaluating and/or confirming DID adequacy. NEI 00-04 Revision 0 (Reference 7): "*10 CFR 50.69 SSC Categorization Guideline*," Sections 9 and 11 provide guidance on the composition of a panel (referred to as the Integrated Decision-Making Panel within NEI 00-04) and the associated output documentation. The decisions of the IDP are documented and retained as a quality record; this function is critical to future decision-making regarding plant changes which have the potential to affect DID.

For KR-FHP, the IDP is comprised of a team that is responsible for ensuring implementation of the integrated process tasks for evaluating DID shown in Figure 5-4, and for confirming DID is adequately implemented. The IDP includes those with expert, plant knowledgeable members whose expertise includes PRA, safety analysis, plant operation, design engineering, and system engineering.

5.9.2 Risk-Informed and Performance-Based Decision-Making Process

The IDP uses a risk-informed and performance-based integrated decision-making (RIPB-DM) process. Risk-informed decision-making is the structured, repeatable process by which decisions are made on significant nuclear safety matters including consideration of deterministic and probabilistic inputs. The process is also performance-based because it employs measurable and quantifiable performance metrics to guide the determination of DID adequacy. RIPB-DM plays a central role in designing and evaluating the DID layers of defense and establishing measures associated with each plant capability and programmatic DID attribute.

Table 5-7 lists the integrated decision-making attributes and principal evaluation focus areas included in the RIPB-DM DID evaluation scope. The RIPB-DM process is expected to be applied throughout the design process in conjunction with other integrated review processes executed during design development as described in Figure 5-4. Meeting the applicable portions of the ASME/ANS PRA Standard for Advanced non-LWRs, which includes the requirement for and completion of the appropriate PRA peer review process, is one means for development of the PRA in RIPB-DM processes.

The RIPB-DM process includes the following tasks regardless of the phase of design:

- Identification of the DID issue to be decided
- Identification of the combination of defined DID attributes important to address identified issues
- Comprehensive consideration of each of the defined attributes individually, incorporating insights from deterministic analyses, probabilistic insights, operating experience, engineering judgment, etc.
- A decision made collaboratively by knowledgeable, responsible individuals based on the defined attribute evaluation requirements
- If compensatory actions are needed, identification of potential plant capability and/or programmatic choices
- Implementation and closure of DID action items and documentation of the results of the RIPB-DM process

A concept in DID adequacy evaluation RIPB-DM is that a graded approach to RIPB-DM is prudently applied such that the decisions on LBEs with the greatest potential risk significance receive corresponding escalated cross-functional and managerial attention, while routine decisions are made at lower levels of the organization, consistent with their design control program.

Completing the evaluation of the DID adequacy of a design is not a one-time activity. The RIPB-DM process is used as often as necessary to minimize the potential for revisions late in the design process due to DID considerations. Integrated DID adequacy evaluations occurs in concert with major design iterations and additionally occurs in response to significant design changes or new risk-significant information at any phase of design or licensing.

5.9.3 IDP Actions to Confirm DID Adequacy

Adequacy of DID is confirmed when the following actions and decisions by the IDP are completed.

- Plant capability DID is deemed to be adequate.
  - Plant capability DID guidelines in Table 5-2 are satisfied.
  - Review of LBEs is completed with satisfactory results.
    - Risk margins against the F-C Target are sufficient.
    - Risk margins against cumulative risk targets are sufficient.
    - The role of SSCs in the prevention and mitigation at each layer of defense challenged by each LBE is understood.
    - Prevention/mitigation balance is sufficient.
    - Classification of SSCs into SR, NSRST, and NST is appropriate.
    - Risk significance classification of LBEs and SSCs are appropriate.
    - Independence among design features at each layer of defense is sufficient.
    - Design margins in plant capabilities are adequate to address uncertainties identified in the PRA.
- Programmatic DID is deemed to be adequate.
  - Performance targets for SSC reliability and capability are established.
  - Sources of uncertainty in selection and evaluation of LBE risks are identified.
    - Completeness in selection of IEs and event sequences is sufficient.
    - Uncertainties in the estimation of LBE frequencies are evaluated.
    - Uncertainties in the plant response to events are evaluated.
    - Uncertainties in the estimation of mechanistic source terms are evaluated.
    - Design margins in plant capabilities are adequate to address residual uncertainties.
  - Special treatment for all SR and NSRST SSCs is sufficient.

5.9.4 Evaluation of Changes to Defense-in-Depth

For each iteration of the design evaluation lifecycle in Figure 5-4, the DID evaluation from the baseline is re-evaluated based on a review to determine which programmatic or plant capability attributes have been affected for each layer of defense. Changes that impact the definition and evaluation of LBEs, safety classification of SSCs, or risk significance of LBEs or SSCs have their DID adequacy re-evaluated and the baseline updated as appropriate.

Table 5-1. Role of Major Elements of RIPB Framework in Establishing DID Adequacy

Elements of RIPB Framework	Role in Establishing DID Adequacy
Development of Safety Design Approach	Selection of inherent, active, and passive design features Selection of approach to radionuclide functional and physical barriers Definition of SFs to prevent and mitigate event sequences for inclusion into the PRA Selection of passive and active SSCs to perform SFs with consideration of the NRC Advanced Reactor Safety Policy to simplify designs, rely more on inherent and passive means to fulfill SFs Initial selection of DID attributes for plant capability and programmatic DID
Reactor-Specific PRA	Identification of challenges to each layer of DID and evaluation of the plant responses to them Identification of challenges to physical and functional barriers within layers of defense Characterization of the plant responses to IEs and identification of end states involving successful mitigation and associated success criteria, and unsuccessful mitigation with release of radioactive material from one or more reactor units or radionuclide sources Assessment of the effectiveness of barriers in retaining fission products via mechanistic source term development and assessment of offsite radiological consequences Assessment of IE frequencies, reliabilities, and availabilities of SSCs necessary to respond to those IEs Identification of dependencies and interactions among SSCs; evaluation of the layers of defense against common-cause failures and functional independence Grouping of event sequences into LBEs based on similarity of IE challenge, plant response, and end state Information for the evaluation of risk significance Identification of risk-significant sources of uncertainty in modeling event sequences and estimation of frequencies and consequences Quantification of the impact of uncertainties via uncertainty and sensitivity analyses Identification and documentation of scope, assumptions, and limitations of the PRA
Selection and Evaluation of LBEs	Identification of safety margins in comparing LBE risks against F-C Targets and cumulative risk criteria Evaluation of the risk significance of LBEs Confirmation of the RSFs Input to the selection of SR SSCs Input to the formulation of conservative assumptions for the deterministic safety analysis of DBAs
SSC Safety Classification and Performance Requirements	Classification of NSRST and NST SSCs Selection of SSC Required Functional Design Criteria Selection of design requirements for SR SSCs Selection of Performance Based (PB) reliability, availability, and capability targets for safety-significant SSCs Selection of Special Treatment Requirements for safety-significant SSCs
Risk-Informed Evaluation of DID Adequacy	Evaluation of DID attributes for DID Input to identification of safety-significant SSCs Input to the selection of SR SSCs

Elements of RIPB Framework	Role in Establishing DID Adequacy
	Evaluation of roles of SSCs in the prevention and mitigation of LBEs Evaluation of the LBEs to assure adequate functional independence of each layer of defense Evaluation of single features that have a high level of risk importance to assure no overdependence on that feature and appropriate special treatment to provide greater assurance of performance Input to SSC performance requirements for reliability and capability of risk-significant prevention and mitigation functions Input to SSC performance and special treatment requirements Integrated evaluation of the plant capability DID Integrated evaluation of programmatic measures for DID

Table 5-2. Guidelines for Establishing the Adequacy of Overall Plant Capability Defense-in-Depth

Layer[a]	Layer Guideline		Overall Guidelines	
	Quantitative	**Qualitative**	**Quantitative**	**Qualitative**
1) Prevent off-normal operation and AOOs	Maintain frequency of plant transients within designed cycles; meet owner requirements for plant reliability and availability[b]		Meet F-C Target for all LBEs and cumulative risk metric targets with sufficient[d] margins	No single design or operational feature,[c] no matter how robust, is exclusively relied upon to satisfy the five layers of defense
2) Control abnormal operation, detect failures, and prevent DBEs	Maintain frequency of all DBEs < 10^{-2}/plant-year	Minimize frequency of challenges to SR SSCs		
3) Control DBEs within the analyzed design basis conditions and prevent BDBEs	Maintain frequency of all BDBEs < 10^{-4}/plant-year	No single design or operational feature[c] relied upon to meet quantitative objective for all DBEs		
4) Control severe plant conditions and mitigate consequences of BDBEs	Maintain individual risks from all LBEs < QHOs with sufficient[d] margins	No single barrier[c] or plant feature relied upon to limit releases in achieving quantitative objectives for all BDBEs		
5) Deploy adequate offsite protective actions and prevent adverse impact on public health and safety				

Notes:

[a] The plant design and operational features and protective strategies employed to support each layer should be functionally independent.

[b] Non-regulatory owner requirements for plant reliability and availability and design targets for transient cycles limit the frequency of Initiating Events and transients and thereby contribute to the protective strategies for this layer of DID. Quantitative and qualitative targets for these parameters are design specific.

[c] This criterion implies no excessive reliance on programmatic activities or human actions and that at least two independent means are provided to meet this objective.

[d] The level of margins between the LBE risks and the QHOs provides objective evidence of the plant capabilities for DID. Sufficiency is decided by the IDP.

Table 5-3. Plant Capability Defense-In-Depth Attributes

Attribute	Evaluation Focus
Initiating Event and Event Sequence Completeness	PRA Documentation of Initiating Event Selection and Event Sequence Modeling
	Insights from reactor operating experience, system engineering evaluations, expert judgment
Layers of Defense	Multiple Layers of Defense
	Extent of Layer Functional Independence
	Functional Barriers
	Physical Barriers
Functional Reliability	Inherent Reactor Features that contribute to performing SFs
	Passive and Active SSCs performing SFs
	Redundant Functional Capabilities
	Diverse Functional Capabilities
Prevention and Mitigation Balance	SSCs performing prevention functions
	SSCs performing mitigation functions
	No Single Layer / Feature Exclusively Relied Upon

Table 5-4. Programmatic DID Attributes

Attribute	Evaluation Focus
Quality / Reliability	Performance targets for SSC reliability and capability
	Design, manufacturing, construction, O&M features, or special treatment sufficient to meet performance targets
Compensation for Uncertainties	Compensation for human errors
	Compensation for mechanical errors
	Compensation for unknowns (performance variability)
	Compensation for unknowns (knowledge uncertainty)
Offsite Response	Emergency response capability

Table 5-5. Evaluation Considerations for Evaluating Programmatic DID Attributes

Evaluation Focus	Implementation Strategies	Evaluation Considerations
Quality / Reliability Attribute		
Design Testing Manufacturing Construction O&M	Conservatism with Bias to Prevention Equipment Codes and Standards Equipment Qualification Performance Testing	1. Is there appropriate bias to prevention of AOOs progressing to postulated event sequences? 2. Has appropriate conservatism been applied in bounding deterministic safety analysis of more risk-significant LBEs? 3. Is there reasonable agreement between the deterministic safety analysis of DBAs and the upper bound consequences of risk-informed DBA included in the LBE set? 4. Have the most limiting design conditions for SSCs in plant safety and risk analysis been used for selection of safety–related SSC design criteria? 5. Are the reliability of functions within systems relied on for safety overly dependent on a single inherent or passive feature for risk-significant LBEs? 6. Is the reliability of active functions relied upon in risk-significant LBEs achieved with appropriate redundancy or diversity within a layer of defense? 7. Have the identified SR SSCs been properly classified for special treatment consistent with their risk significance?
Compensation for Uncertainties Attribute		
Compensation for Human Errors	Operational Command and Control Practices Training and Qualification Plant Simulators Independent Oversight and Inspection Programs Reactor Oversight Program	1. Have the insights from the Human Factors Engineering program been included in the PRA appropriately? 2. Have plant system control designs minimized the reliance on human performance as part of risk-significant LBE scenarios? 3. Have plant protection functions been automated with highly reliable systems for all DBAs? 4. Are there adequate indications of plant state and transient performance for operators to effectively monitor all risk-significant LBEs? 5. Are the risk-significant LBEs all properly modeled on the plant reference simulator and adequately confirmed by deterministic safety analysis?

Evaluation Focus	Implementation Strategies	Evaluation Considerations
		6. Are all LBEs for all modes and states capable of being demonstrated on the plant reference simulator for training purposes?
Compensation for Mechanical Errors	Operational Technical Specifications Allowable Outage Times Part 21 Reporting Maintenance Rule Scope	1. Are all risk-significant LBE limiting condition for operation reflected in plant Operating Technical Specifications? 2. Are Allowable Outage Times in Technical Specifications consistent with assumed functional reliability levels for risk-significant LBEs? 3. Are all risk-significant SSCs properly included in the Maintenance Program?
Compensation for Unknowns (Performance Variability)	Operational Technical Specifications In-Service Monitoring Programs	1. Are the Technical Specifications for risk-significant SSCs consistent with achieving the necessary safety function outcomes for the risk-significant LBEs? 2. Are the in-service monitoring programs aligned with the risk-significant SSC identified through the RIPB SSC Classification process?
Compensation for Unknowns (Knowledge Uncertainty)	Site Selection Phenomena Identification and Ranking Table (PIRT)/ Technical Readiness Levels Integral Systems Tests / Separate Effects Tests	1. Have the uncertainties identified in PIRT or similar evaluation processes been satisfactorily addressed with respect to their impact on plant capability and associated safety analyses? 2. Has physical testing been done to confirm risk-significant SSC performance within the assumed bounds of the risk and safety assessments? 3. Have plant siting requirements been conservatively established based on the risk from severe events identified in the PRA? 4. Has the PRA been peer reviewed in accordance with applicable industry standards and regulatory guidance? 5. Are hazards not included in the PRA low risk to the public based on bounding deterministic analysis?
Offsite Response Attribute		
Emergency Response Capability	Layers of Response Strategies Emergency Planning Zone Location	1. Are functional response features appropriately considered in the design and emergency operational response capabilities for severe events as a means of providing additional DID for undefined event conditions?

Evaluation Focus	Implementation Strategies	Evaluation Considerations
	Emergency Planning Programs Public Notification Capability	2. Is the emergency planning zone appropriate for the full set of DBEs and BDBEs identified in the LBE selection process? 3. Is the time sufficient to execute emergency planning protective actions for risk-significant LBEs consistent with the event timelines in the LBEs?

Table 5-6. Examples of Special Treatments Considered for Programmatic DID

Programs	Elements
Engineering Assurance Programs	Special treatment specifications
	Independent design reviews
	Physical testing and validation including integrated and separate effects tests
Organizational and Human Factors Programs	Plant simulation and human factors engineering
	Training and qualification of personnel
	Emergency operating procedures
	Severe Accident Management Guidelines
Technical Specifications	Limiting conditions for operation
	Surveillance testing requirements
	Allowable outage (completion) times
Plant Construction and Start-Up Programs	Equipment fabrication oversight
	Construction oversight
	Factory testing and qualification
	Start-up testing
Maintenance and Monitoring of SSC Performance Programs	Operation
	In-service testing
	In-service inspection
	Maintenance of SSCs
	Monitoring of performance against reliability and capability performance indicators
Quality Assurance Program	Inspections and audits
	Procurement
	Independent reviews
	Software verification and validation
Corrective Action Programs	Event trending
	Cause analysis
	Closure effectiveness
Independent Oversight and Monitoring Programs	Owner-directed independent reviews and performance monitoring programs
Equipment Qualification	Seismic qualification
	Adverse environment qualification
	Physical protection
Emergency Planning	Periodic drills Emergency response equipment maintenance programs

Table 5-7. Risk-Informed and Performance-Based Decision-Making Attributes

Attribute	Evaluation Focus
Use of Risk Triplet Beyond PRA	What can go wrong?
	How likely is it?
	What are the consequences?
Knowledge Level	Plant Simulation and Modeling of LBEs
	State of Knowledge
	Margin to Performance-Based Targets and Limits
Uncertainty Management	Magnitude and Sources of Uncertainties
Action Refinement	Implementation Practicality and Effectiveness
	Cost/Risk/Benefit Considerations

Table 5-8. Evaluation Summary – Qualitative Evaluation of Plant Capability DID

LBE IE Series Name	Functional			Physical	
	Margin Adequacy	**Multiple Protective Measures**	**Prevention and Mitigation Balance**	**Functional Reliability**	**No Single Feature Relied Upon**
Normal Operation	√	√		√	
AOOs	√	√		√	
DBEs	√	√	√	√	√
BDBEs	√	√	√	√	√
DBAs	√	√	√	√	√

Table 5-9. Evaluation Summary – Qualitative Evaluation of Programmatic DID

LBE IE Series Name	Quality/Reliability: Design, Manufacturing, Construction, O&M	Compensation for Uncertainties			Emergency Response Capability
		Human Errors	Mechanical Failures	Unknowns	
Normal Operation	√	√	√	√	
AOOs	√	√	√	√	
DBEs	√	√	√	√	√
BDBEs	√	√	√	√	√
DBAs	√	√	√	√	√

Figure 5-1. U.S. Nuclear Regulatory Commission's Defense-in-Depth Concept

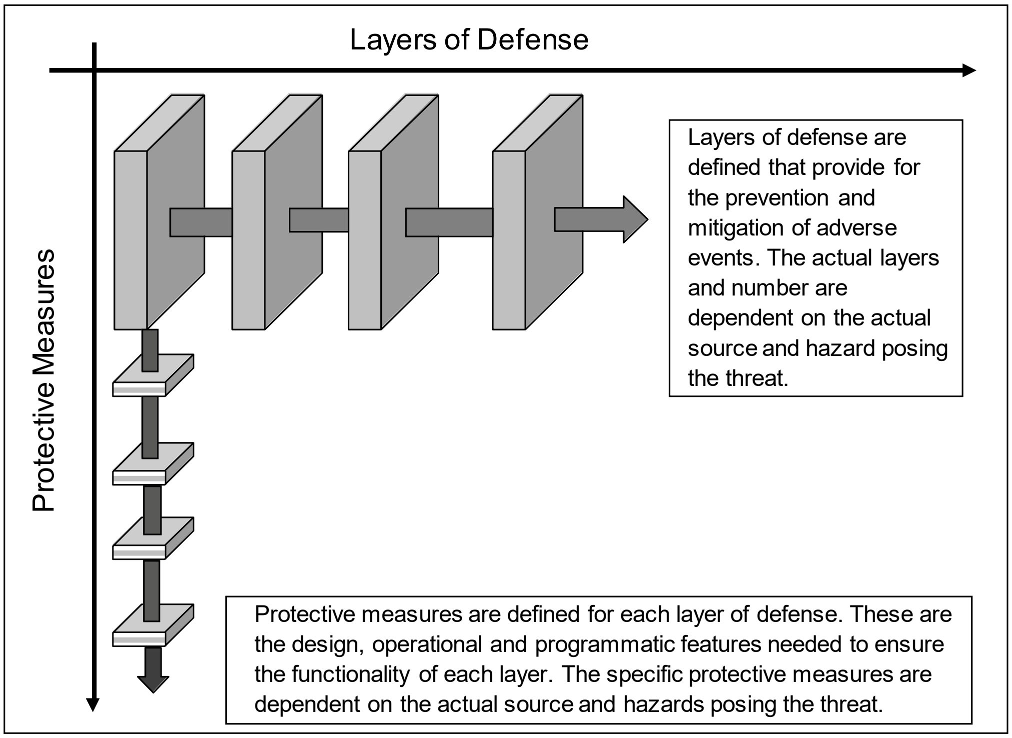


Figure 5-2. Framework for Establishing DID Adequacy

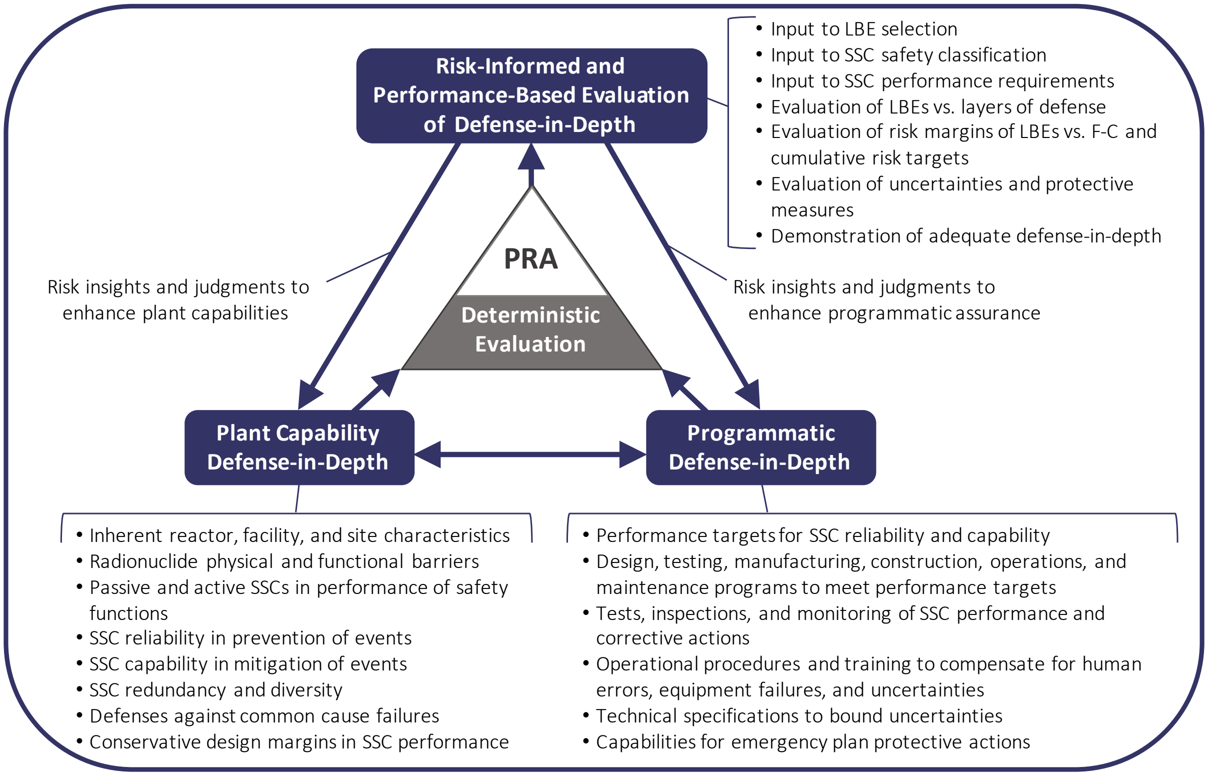


Figure 5-3. Framework for Evaluating LBEs Using Layers of Defense Concept Adapted from IAEA

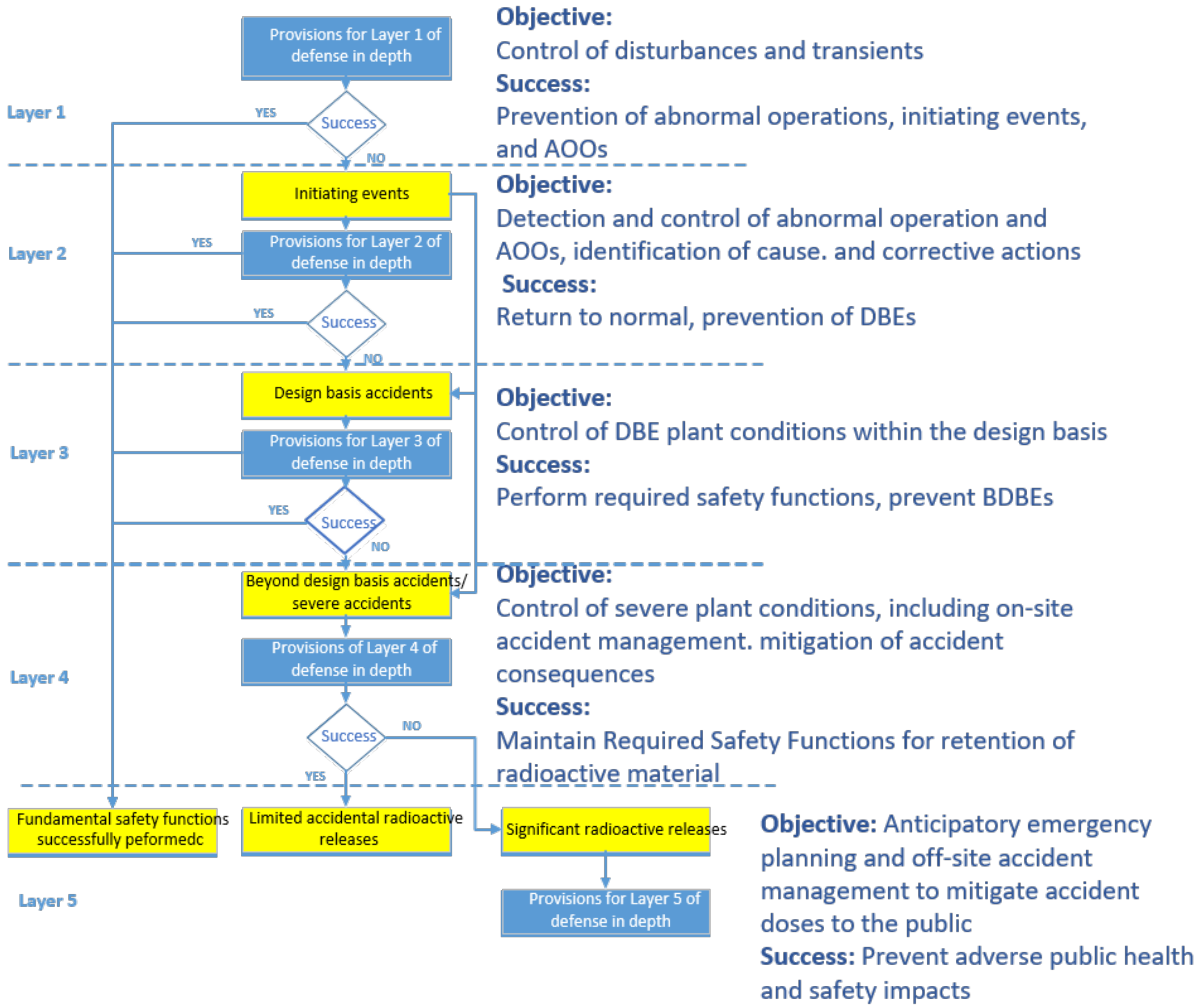
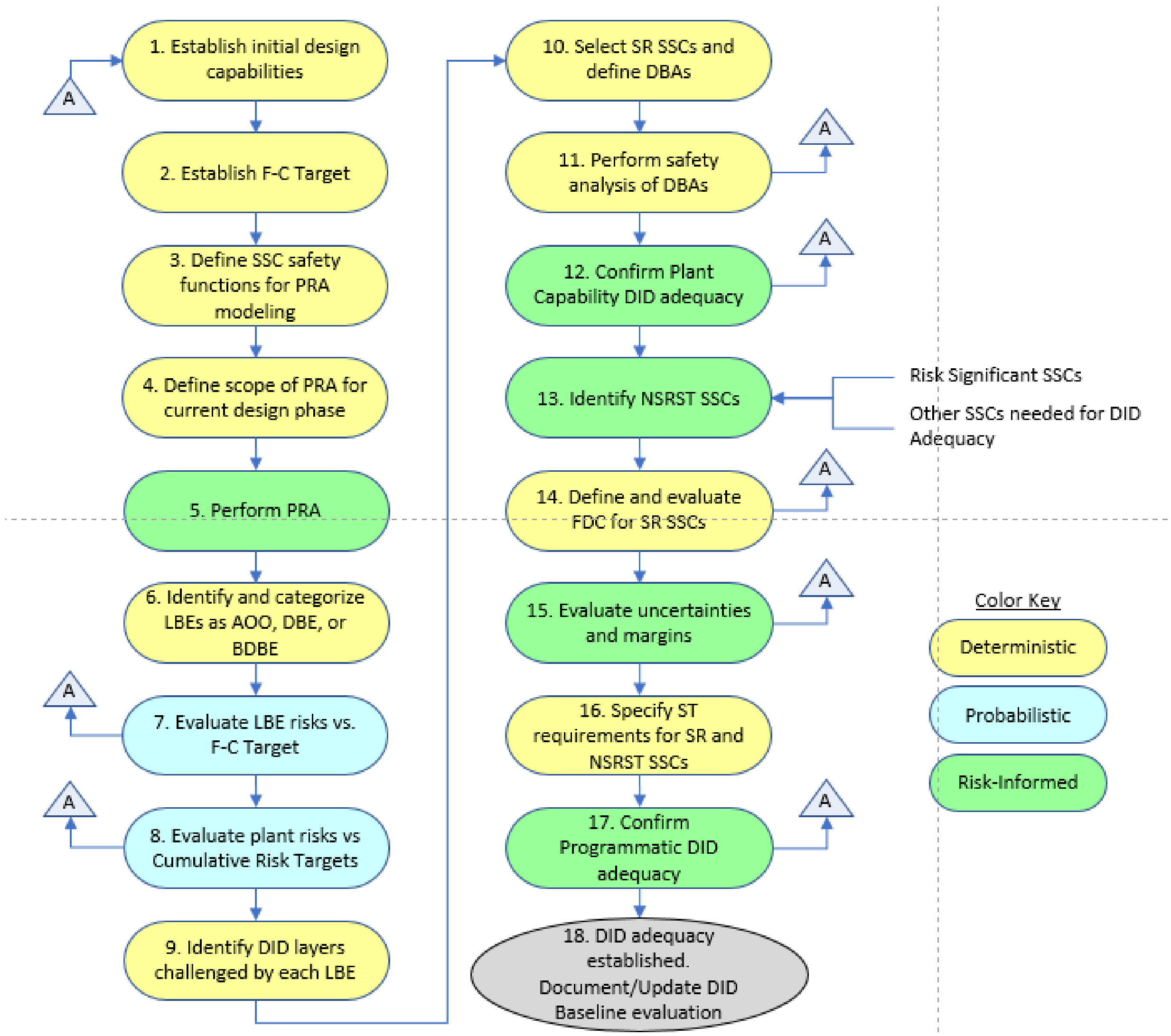


Figure 5-4. Integrated Process for Incorporation and Evaluation of Defense-in-Depth



6 CONCLUSION

This report presents a risk-informed, performance-based methodology developed through the licensing modernization project to define, categorize and evaluate licensing basis events (LBEs), provide safety classifications for structures, systems, and components (SSCs), and ensure the defense-in-depth adequacy of the KP-FHR. This topical reproduces the NEI 18-04 content with minor technology-specific changes to the risk-informed, performance-based guidance, to assert the methodology as applicable to the KP-FHR.

Kairos Power is requesting U.S. Nuclear Regulatory Commission (NRC) review and approval to use the methodology presented in this report to define the licensing basis events, to classify the SSCs, and to ensure the defense-in-depth (DID) adequacy of the KP-FHR as part of safety analysis reports required to be submitted to meet the associated requirements for content of licensing applications required in 10 CFR 50.34(a), 10 CFR 50.34(b), 10 CFR 52.47, 10 CFR 52.79, 10 CFR 52.137, and 10 CFR 52.157. There is a sample licensing basis event (LBE) evaluation is provided in Appendix B to illustrate the methodology. This sample LBE does not represent final KP-FHR design information and is only intended to be an illustration of the methodology in application. Kairos Power is not requesting NRC approval of the design information presented in Appendix B.

7 REFERENCES

1. Kairos Power LLC, “Design Overview of the Kairos Power Fluoride Salt Cooled, High Temperature Reactor (KP-FHR)”, KP-TR-001, November 2018.
2. Kairos Power LLC, “Testing and Development Program Overview for the Kairos Power Fluoride Salt Cooled, High Temperature Reactor”, KP-TR-002, November 2018.
3. NEI 18-04, Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development, Draft Report Revision 1, NEI Technical Report, August 2019.
4. Non-LWR PRA Standard, American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS) RA-S-1.4-2013.
5. IAEA-TECDOC-1570, Proposal for a Technology-Neutral Safety Approach for New Reactor Designs, Technical Report, 2007.
6. RIEP-NEI-16 Revision 0, Risk Informed Engineering Programs (10CFR50.69), Nuclear Energy Institute, November 2016.
7. NEI 00-04 Revision 0, 10CFR50.69 SSC Categorization Guideline, Nuclear Energy Institute, July 2005.
8. IAEA Safety Report Series No. 46, Assessment of Defense in Depth for Nuclear Power Plants, International Atomic Energy Agency, 2005.
9. Reference Not Used.
10. Kairos Power LLC, “Principal Design Criteria for the Kairos Power Fluoride Salt-Cooled High Temperature Reactor,” KP-TR-003, December 2018.
11. Kairos Power LLC, “Regulatory Analysis for the Kairos Power Fluoride Salt-Cooled, High Temperature Reactor”, KP-TR-004, January 2019.

APPENDIX A. GLOSSARY OF TERMS

Term	Acronym	Definition
Anticipated Operational Occurrence	AOO	Anticipated event sequences expected to occur one or more times during the life of a nuclear power plant, which may include one or more reactor units. Event sequences with mean frequencies of 10^{-2}/plant-year and greater are classified as AOOs. AOOs take into account the expected response of all SSCs within the plant, regardless of safety classification.
Beyond Design Basis Event	BDBE	Rare event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor units, but are less likely than a DBE. Event sequences with frequencies of 5×10^{-7}/plant-year to 10^{-4}/plant -year are classified as BDBEs. BDBEs take into account the expected response of all SSCs within the plant regardless of safety classification.
Defense-in-Depth	DID	"An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key SFs, and emergency response measures."
Design Basis Accident	DBA	Postulated accidents that are used to set design criteria and performance objectives for the design of Safety-Related SSCs. DBAs are derived from DBEs based on the capabilities and reliabilities of Safety-Related SSCs needed to mitigate and prevent accidents, respectively. DBAs are derived from the DBEs by prescriptively assuming that only SR SSCs classified are available to mitigate postulated accident consequences to within the 10 CFR 50.34 dose limits.
Design Basis Event	DBE	Infrequent event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor units, but are less likely than AOOs. Event sequences with mean frequencies of 10^{-4}/plant-year to 10^{-2}/plant-year are classified as DBEs. DBEs take into account the expected response of all SSCs within the plant regardless of safety classification.
Design Basis External Hazard Level	DBEHL	A design specification of the level of severity or intensity of an external hazard for which the Safety-Related SSCs are designed to withstand with no adverse impact on their capability to perform their RSFs
End State	--	The set of conditions at the end of an Event Sequence that characterizes the impact of the sequence on the plant or the

Term	Acronym	Definition
		environment. In most PRAs, end states typically include success states (i.e., those states with negligible impact) and Release Categories.
Event Sequence	ES	A representation of a scenario in terms of an Initiating Event defined for a set of initial plant conditions (characterized by a specified POS) followed by a sequence of system, safety function, and operator failures or successes, with sequence termination with a specified end state (e.g., prevention of release of radioactive material or release in one of the reactor-specific release categories. An event sequence may contain many unique variations of events (minimal cut sets) that are similar in terms of how they impact the performance of SFs along the event sequence.
Event Sequence Family	-	A grouping of event sequences with a common or similar POS, Initiating Event, hazard group, challenges to the plant SFs, response of the plant in the performance of each safety function, response of each radionuclide transport barrier, and end state. An event sequence family may involve a single event sequence or several event sequences grouped together. Each release category may include one or more event sequence families. Event sequence families are not required to be explicitly modeled in a PRA. Each event sequence family involving a release is associated with one and only one release category.
Frequency-Consequence Target	F-C Target	A target line on a frequency-consequence chart that is used to evaluate the risk significance of LBEs and to evaluate risk margins that contribute to evidence of adequate defense-in-depth
Fundamental Safety Function	FSF	SFs common to all reactor technologies and designs; includes control of the reactor power, removal of heat from the fuel, and confinement of radioactive materials
Initiating Event	IE	A perturbation to the plant during a POS that challenges plant control and safety systems whose failure could potentially lead to an undesirable end state and/or radioactive material release. An Initiating Event could degrade the reliability of a normally operating system, cause a standby mitigating system to be challenged, or require that the plant operators respond in order to mitigate the event or to limit the extent of plant damage caused by the Initiating Event. These events include human-caused perturbations and failure of equipment from either internal plant causes (such as hardware faults, floods, or fires) or external plant causes (such as earthquakes or high winds). An Initiating Event is defined in terms of the change in plant status that results in a condition requiring shutdown or a reactor trip

Term	Acronym	Definition
		(e.g., loss of main feedwater system, small reactor coolant pressure boundary [RCPB] breach) when the plant is at power, or the loss of a key safety function (e.g., decay heat removal system) for non-power modes of operation. A specific type of Initiating Event may be identified as originating from a specific cause as defined in terms such as “flood-induced transient” or “seismically-induced RCPB breach.”
Layers of Defense	--	Layers of defense are those plant capabilities and programmatic elements that provide, collectively, independent means for the prevention and mitigation of adverse events. The actual layers and number are dependent on the actual source and hazard posing the threat. See Defense-in-Depth.
Licensing Basis Event	LBE	The entire collection of event sequences considered in the design and licensing basis of the plant, which may include one or more reactor units. LBEs include AOOs, DBEs, BDBEs, and DBAs.
Mechanistic Source Term	MST	A source term that is calculated using models and supporting scientific data that simulate the physical and chemical processes that describe the radionuclide inventories and the time-dependent radionuclide transport mechanisms that are necessary and sufficient to predict the source term.
Mitigation Function	--	An SSC function that, if fulfilled, will eliminate or reduce the consequences of an event in which the SSC function is challenged. The capability of the SSC in the performance of such functions serves to eliminate or reduce any adverse consequences that would occur if the function were not fulfilled.
Multi-Reactor Unit Plant	--	A plant comprising multiple reactor units that are designed and constructed using a modular design approach. Modular design means a nuclear power plant that consists of two or more essentially identical nuclear reactors (units) and each reactor unit is a separate nuclear reactor capable of being operated independent of the state of completion or operating condition of any other reactor unit co-located on the same site, even though the nuclear power plant may have some shared or common systems.
Nonsafety-related with No Special Treatment SSCs	NST SSCs	All SSCs within a plant that are neither Safety-Related SSCs nor Nonsafety-related SSCs with Special Treatment SSCs.
Nonsafety-related with Special Treatment SSCs	NSRST SSCs	Nonsafety-related SSCs that perform risk-significant functions or perform functions that are necessary for defense-in-depth adequacy
Performance-Based	PB	An approach to decision-making that focuses on desired objective, calculable or measurable, observable outcomes,

Term	Acronym	Definition
		rather than prescriptive processes, techniques, or procedures. Performance-based decisions lead to defined results without specific direction regarding how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives and flexibility for licensees to improve safety without formal regulatory intervention by the agency.
Plant	--	The collection of site, buildings, radionuclide sources, and SSCs seeking a single design certification or one or more operating licenses. The plant may include a single reactor unit or multiple reactor units as well as non-reactor radionuclide sources.
Plant Operating State	POS	A standard arrangement of the plant during which the plant conditions are relatively constant, are modeled as constant, and are distinct from other configurations in ways that impact risk. Examples of such plant conditions include core decay heat level, primary coolant level, primary temperature, primary vent status, reactor building status, and decay heat removal mechanisms. Examples of risk impacts that are dependent on POS definition include the selection of Initiating Events, Initiating Event frequencies, definition of accident sequences, success criteria, and accident sequence quantification.
Safety Function	SF	Reactor design specific SSC functions that serve to prevent and/or mitigate a release of radioactive material or to protect one or more barriers to release.
PRA Technical Adequacy	--	A set of attributes that define the technical suitability of a PRA capability to provide fit-for-purpose insights to risk-informed decision-making. It includes consideration of realism, completeness, transparency, PRA model-to-plant as-designed and as-built fidelity state, and identification and evaluation of uncertainties relative to risk levels. Strategies to achieve technical adequacy include conformance to consensus PRA standards, performance of PRA peer reviews, and structured processes for PRA model configuration control, maintenance and updates, and incorporation of new evidence that comprises the state of knowledge reflected in the PRA model development and its quantification.
Prevention Function	--	An SSC function that, if fulfilled, will preclude the occurrence of an adverse state. The reliability of the SSC in the performance of such functions serves to reduce the probability of the adverse state.
Required	RFDC	Reactor design-specific functional criteria that are necessary and

Term	Acronym	Definition
Functional Design Criteria		sufficient to meet the RSFs
Required Safety Function	RSF	An SF that is required to be fulfilled to maintain the consequence of one or more DBEs or the frequency of one or more high-consequence BDBEs inside the F-C Target
Risk-Informed	RI	An approach to decision-making in which insights from probabilistic risk assessments are considered with other sources of insights
Risk-Informed and Performance-Based Integrated Decision-Making	RIPB-DM	The union of risk information and performance information to achieve performance-based objectives
Risk-Significant LBE	--	An LBE whose frequency and consequence meet a specified risk significance criterion. An AOO, DBE, or BDBE is regarded as risk-significant if the combination of the upper bound estimates of the frequency and consequence of the LBE are within 1% of the F-C Target AND the upper bound 30-day TEDE dose at the EAB exceeds 2.5 mrem.
Risk-Significant Function	--	An SF is regarded as risk-significant if is: a) required to keep one or more LBEs inside the F-C Target based on mean frequencies and consequences; or b) if the total frequency LBEs that involve failure of the SSC SF contributes at least 1% to any of the cumulative risk targets. The cumulative risk targets include: (i) maintaining the frequency of exceeding 100 mrem to less than 1/plant-year; (ii) meeting the NRC safety goal QHO for individual risk of early fatality; and (iii) meeting the NRC safety goal QHO for individual risk of latent cancer fatality.
Risk-Significant SSC	--	An SSC that performs an SF that is risk-significant.
Safety Design Approach	--	The strategies that are implemented in the design of a nuclear power plant that are intended to support safe operation of the plant and control the risks associated with unplanned releases of radioactive material and protection of the public and plant workers. These strategies normally include the use of robust barriers, multiple layers of defense, redundancy, and diversity, and the use of inherent and passive design features to perform SFs.
Safety-Related Design Criteria	SRDC	Design criteria for SR SSCs that are necessary and sufficient to fulfill the RFDCs for those SSCs selected to perform the RSFs
Safety-Related SSCs	SR SSCs	SSCs that are credited in the fulfillment of RSFs and are capable to perform their RSFs in response to any Design Basis External Hazard Level as well as any SSCs that are credited to shut down

Term	Acronym	Definition
		the reactor and maintain it in a safe shut down condition.
Safety-Significant Function	--	An SF whose performance is necessary to achieve adequate defense-in-depth or is classified as Risk-Significant (see Risk-Significant SSC).
Safety-Significant SSC	--	An SSC that performs an SF that is safety-significant

APPENDIX B. KP-FHR SAMPLE APPLICATION OF METHODOLOGY

B.1 Introduction

This appendix illustrates the application of the methodology provided in this topical report to an example KP-FHR LBE. This LBE is only intended to be used as an example and does not reflect final design information. The information in this appendix is informational and Kairos Power is not seeking NRC approval of this Appendix.

B.2 Selecting and Evaluating the Loss-of-Flow Event

The example LBE provided for this exercise is the loss-of-flow event. The results of this exercise will be documented in the tasks provided in Figure 3-2 of this report for consistency. Additional discussion is provided in the appropriate steps to inform or demonstrate the additional steps required in the SSC classification and DID adequacy portions of the methodology.

B.2.1 Task 1: Propose Initial List of LBEs

During design development, it is necessary to select an initial set of LBEs which may not be complete but are necessary to develop the basic elements of the safety design. As discussed in Section 3, there are multiple ways to select or identify an initial list of LBEs. For this example, the Loss-of-Flow initiating event is chosen as the LBE to exercise the methodology presented in this topical report.

B.2.2 Task 2: Design Development and Analysis

The KP-FHR design process includes various phases (e.g., pre-conceptual, conceptual, preliminary, and final) and iterations between phases. An overview of the KP-FHR design has been provided in Section 1.3 to provide context for this example LBE.

B.2.3 Task 3: PRA Development/Update

The PRA is introduced early in the design process for KP-FHR and updated as appropriate throughout the design process. For the purposes of this example, a PRA with the following scope is used to provide results:

- The at-power plant operating state is the initial focus of the risk assessment. This includes plant challenges possible during power-delivery.
- Internal events, including mechanical, human, fire, and flood hazards are included. These hazards are studied at the plant-level and lean heavily on screening based on equipment separation requirements.
- System reliability is modeled by incorporating design reliability targets for individual and common mode failures. Wide probability distributions are used to ensure that the uncertainty is reflected in results.
- Success criteria, source term, and radiological consequences are defined in terms of retention requirements for radionuclide barriers. Similar to the system reliability figures, the uncertainty is treated with wide probability distributions.

The probabilistic risk assessment uses initiating event groups to treat initiators that have common challenges to reactor systems. The loss of forced core flow initiating event group subsumes all initiating event causes which cause core flow to be reduced during at-power operation. This group specifically excludes events that are associated with physical loss of primary coolant. The loss of core flow event could potentially challenge temperature limits on the TRISO fuel by dramatically increasing the power-to-flow ratio within the core. Additionally, this event may present challenges to the vessel structure due to a rapid thermal transient. Finally, the loss of core flow may also result in reduced heat removal capability from the primary salt. The increase in primary salt temperature is a challenge to the fission product solubility of the salt as a radionuclide barrier.

The sequences that follow the loss of forced core flow initiating event are visualized in the event tree shown in Figure B-1. Event Sequence families are defined in the risk assessment to group event sequences having similar plant response characteristics.

The first event sequence family is named AOO-1. It contains a single sequence and represents the detection of the initiating event and automatic reactor trip by the nonsafety-related reactivity control system. This is followed by successful operation of the front-line decay heat removal system, a nonsafety-related system responsible for delivering residual reactor heat to the ultimate heat sink during anticipated transients.

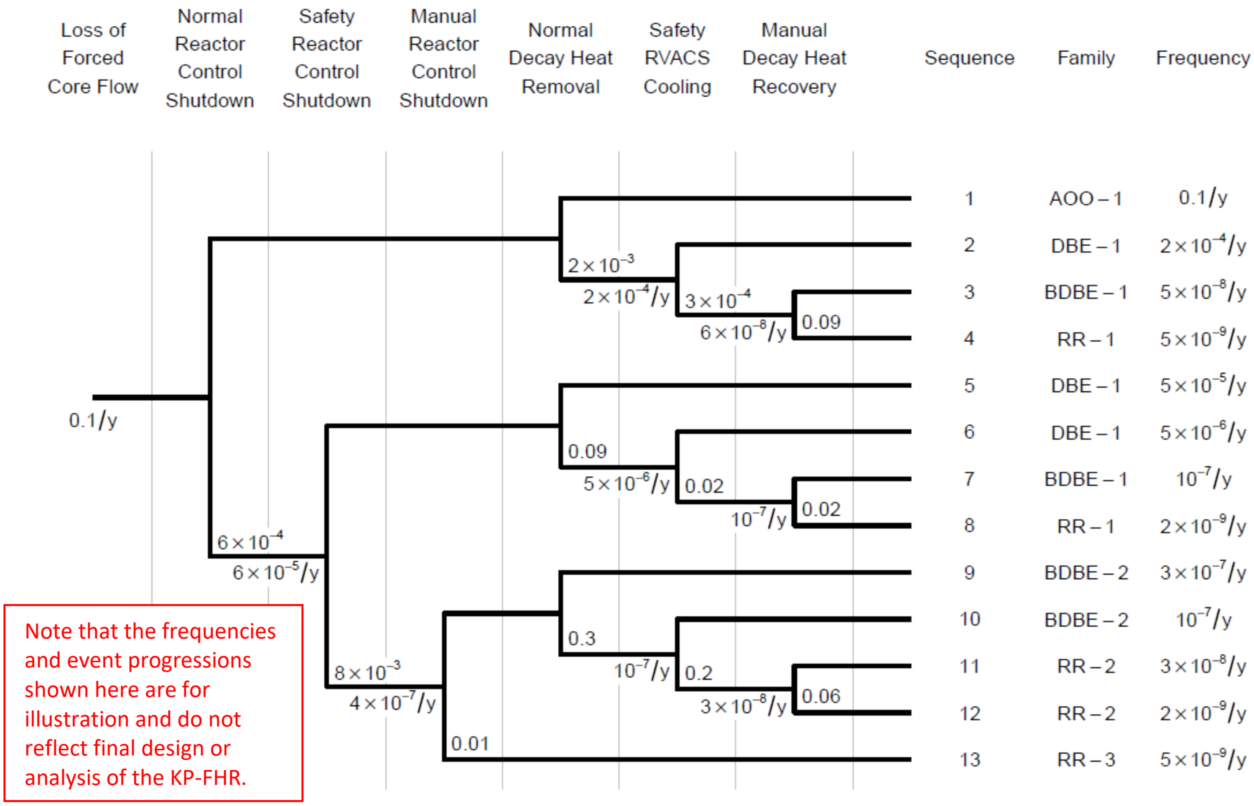
The second event sequence family is named DBE-1. It groups three event sequences where either or both of the nonsafety-related systems operating in AOO-1 are not available to perform their function. This family is bounded by the event sequence where both the non-safety reactor trip and the non-safety decay heat removal are unavailable. This event is a demand on both the back-up reactor trip by the safety-related reactor protection system and the safety-related decay heat removal system. For the illustration provided in this appendix the safety-related decay heat removal system is called reactor auxiliary cooling system (RVACS).

The third event sequence family is named BDBE-1. This family groups two event sequences where reactivity is controlled by either the nonsafety-related or safety-related systems, but decay heat removal from safety-related RVACS capability has been degraded by conditions either internal or external to the plant. This event sequence family is a demand for the beyond design basis response where either RVACS or normal shutdown cooling are recovered in an extended transient.

The fourth event sequence family is named BDBE-2. While BDBE-1 was an illustration of beyond design basis response for decay heat removal, BDBE-2 is a demand on beyond design basis reactivity control given the unavailability of both the nonsafety-related and safety-related control systems to shut down the reactor. This event sequence family relies on inherent reactivity feedback mechanisms of the core to automatically reduce thermal power on high temperature in the short-term and on long-term actions to get control elements inserted into the core for subcriticality.

The remaining event sequence families are labelled RR-1, RR-2, and RR-3. These are residual risk families that are retained in the PRA to identify cliff-edge effects.

Figure B-1. Loss of Forced Flow Event Tree



B.2.4 Task 4: Identify/Revise List of AOOs, DBEs, and BDBEs

The event sequences modeled and evaluated in the PRA are grouped into accident families each having a similar initiating event, challenge to the SFs, plant response, end state, and mechanistic source term if there is a radiological release. Each of these families is assigned to an LBE category based on mean event sequence frequency of occurrence per plant-year summed over all the event sequences in the LBE family.

The event sequence families from the PRA are described in the sections below. They are labeled with the event classification that matches both the product goals and the following frequency criteria from NEI 18-04.

- Anticipated operational occurrences have frequencies exceeding 10^{-2}/plant-year.
- Design basis events have frequencies that do not exceed 10^{-2}/plant-year to ensure that they are not anticipated in the lifetime of a single plant.
- Beyond design basis events have frequencies that do not exceed 10^{-4}/plant-year to ensure that they are not anticipated in the lifetime of a fleet of plants.
- Residual risk events are excluded from the list of licensing basis events and have frequencies that do not exceed 5×10^{-7}/plant-year.

Loss of Flow AOO-1 Event Sequence Family

The event sequence family AOO-1 matches the anticipated loss of flow licensing basis event described above. AOO-1 is a family containing a single event, Sequence 1.

The loss of forced flow initiating event is a challenge to reactor temperatures, requiring an immediate reduction in core power and removal of residual decay heat. This is a demand on the normal reactor shutdown and decay heat removal systems. In this event sequence family, both the systems successfully operate and fulfill the fundamental safety functions for the plant.

Loss of Flow DBE-1 Event Sequence Family

The event sequence family DBE-1 matches the design basis loss of flow licensing basis event described above. DBE-1 is a family containing three events, Sequences 2, 5, and 6.

Sequence 2 features a failure or unavailability of normal decay heat removal, with a demand on the safety decay heat removal through RVACS. Sequence 5 features a failure or unavailability of the normal reactor shutdown function, but a successful demand on the safety back-up that triggers insertion of the safety control elements. Sequence 6 is the same as sequence 5 but includes failure of both normal reactor shutdown and decay heat removal, and successful operation of both the safety shutdown and RVACS decay heat removal functions.

Loss of Flow BDBE-1 and BDBE-2 Event Sequence Families

Sequences 3 and 7 are in a family called BDBE-1.

Sequence 3 defines the beyond design basis conditions for a decay heat removal scenario. In this sequence, the normal decay heat removal system is failed or unavailable and the RVACS is degraded. Degraded RVACS conditions might be associated with an external event. In this sequence RVACS is not completely unavailable but provides its function in such a way that design basis criteria on release are not met.

Sequence 7 is similar to sequence 3, but the starting conditions of the decay heat removal scenario feature the failure or unavailability of the normal reactor trip. This may result in additional core heat added to the system before the safety scram actuates and may be a more bounding challenge to structural temperatures.

This sequence may involve operator actions to enhance RVACS heat removal capability or to realign normal decay heat removal.

Sequences 9 and 10 are in a family called BDBE-2.

Sequence 9 defines the beyond design basis conditions for a reactivity control scenario. In this sequence, the normal reactor shutdown system is failed or unavailable and the automatic safety control elements are also failed or delayed in inserting. This sequence relies on a combination of the performance of inherent reactivity feedback mechanisms of the core to reduce power on increasing temperature, as well as manual operator actions to recover the control elements.

Sequence 10 is similar to Sequence 9, but with the additional failure of normal decay heat removal. It is a challenge of operator actions to insert control elements and of RVACS to remove decay heat.

Figure B-2. AOO-1 Event Sequence Family Frequency

Note that the frequencies and event progression shown here are for illustration and do not reflect final design or analysis of the KP-FHR.

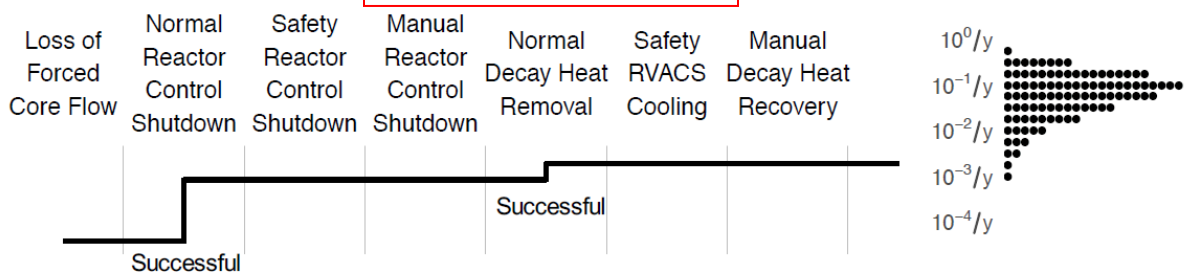


Figure B-3. DBE-1 Event Sequence Family Frequency

Note that the frequencies and event progressions shown here are for illustration and do not reflect final design or analysis of the KP-FHR.

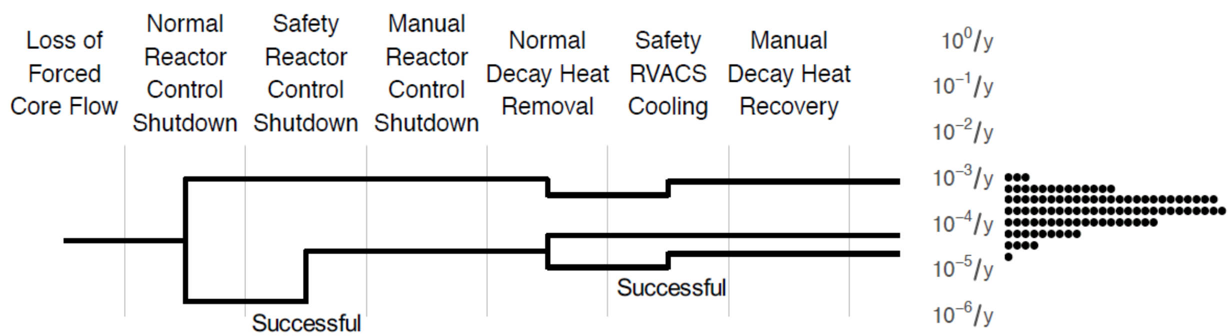
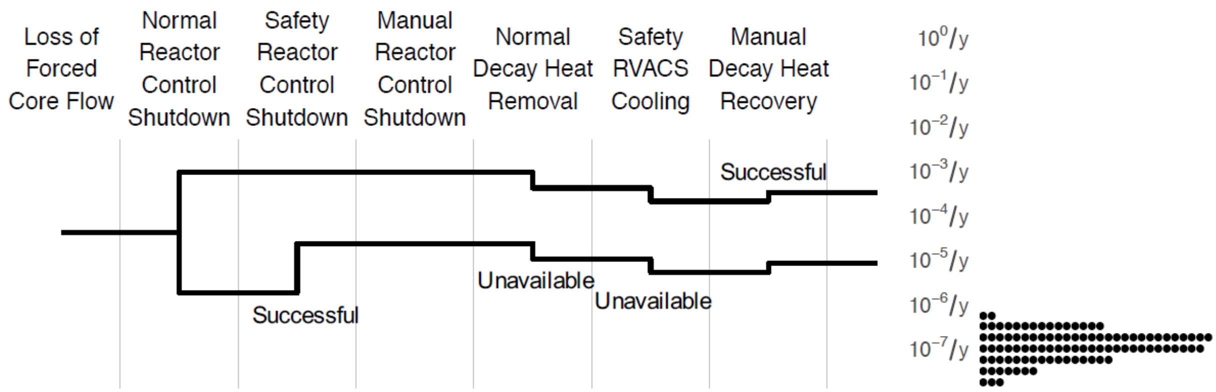


Figure B-4. BDBE-1 Event Sequence Family Frequency

Note that the frequencies and event progression shown here are for illustration and do not reflect final design or analysis of the KP-FHR.



B.2.5 Task 5a: Identify Required Safety Functions

The design basis event sequence family, DBE-1 uses the following SFs to prevent radiological consequences from exceeding the 10 CFR 50.34 dose requirements:

- Safety reactor shutdown system initiates a reactor scram if the normal reactor shutdown does not function
- Safety RVACS removes decay heat if the normal shutdown cooling system fails to do so

Although not explicitly modeled in the event tree, two other functions are performed:

- Maintain TRISO integrity to prevent release of radioactive material
- Maintain vessel integrity to keep TRISO particles covered and to enable decay heat removal

B.2.6 Task 5b: Select/Revise Safety-Related SSCs

Any SSC that is required to function to successfully fulfill the RSFs in Task 5a should be classified as safety-related.

The following SSCs are classified as safety-related and will be available to automatically shutdown the reactor following a loss of forced core flow DBE:

- Reactor shutdown rods
- Shutdown rod release and drive mechanisms
- SSCs required to maintain control rod insertability
- Instrumentation to detect the need for reactor shutdown (i.e. thermocouples, transducers)
- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the shutdown rods and drives

The success of this fundamental safety function is measured by the subcriticality of the reactor and timing. This function also satisfies the safe shutdown criterion of safety-related SSCs in 10 CFR 50.2

The following SSCs are classified as safety-related and will be available to remove core decay heat following a loss of forced core flow DBE:

- RVACS, including physical water storage tanks, cooling panels, valves and associated equipment

- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to open water valves and activate RVACS
- Structural supports for cooling panels
- Support systems that ensure the availability of RVACS to provide a passive decay heat removal function
- Air/water heat exchanger in RVACS stacks
- Physical RVACS chimneys
- Air intake structures
- Free-standing supports separate from the reactor building

The success of this fundamental safety function is measured by salt temperature limits which are defined based on qualification temperatures of the TRISO fuel particles.

The following SSCs are classified as safety-related and will be available in addition to the RVACS equipment identified above to maintain vessel integrity following a loss of forced flow DBE

- Vessel supports stabilizing the vessel in the cavity
- Cavity seals preventing water ingress into the reactor cavity

The success of this fundamental safety function is measured by temperature limits, stress limits, and environmental qualification conditions set by the design life constraints of the reactor vessel.

The following SSCs are classified as safety-related and will be available to ensure TRISO integrity is maintained following a loss of forced flow DBE:

- Instrumentation to detect the radionuclide inventory of the reactor cover gas space
- Instrumentation to detect the radionuclide inventory of the circulating salt coolant
- Instrumentation to detect unexpected transient failures from fuel pebbles circulating in the pebble handling system

The success of this fundamental safety function is measured by assurance that conditions exceeding the analysis assumptions for pre-transient damage to TRISO particles are avoided during normal operation.

B.2.7 Task 6: Select Deterministic DBAs and Design Basis External Hazard Levels

For each design basis event identified in Task 4, a deterministic design basis accident is defined that includes the Required Safety Function challenges represented in the event but assumes that the RSFs are performed exclusively by safety-related SSCs and that the nonsafety-related SSCs are assumed to be unavailable to mitigate the consequences of the event. These design basis accidents are used in transient analysis of the licensing application for supporting the conservative deterministic safety analysis.

For this example, the Loss of Flow design basis event identified above corresponds to a design basis accident. The following are assumptions and characteristics of the loss of flow design basis accident:

- The reactor is operating at the most bounding conditions with respect to the reactor power, pressure, and fluid temperature and flow steady-state condition before the onset of the transient.
- The burnup of the core is at the most limiting condition (likely end of life) for maximizing decay heat generation.
- The event begins with the most bounding loss of flow event – such as a pump seizure.
- The safety-related reactor protection system detects the need to insert safety control elements through temperature or flow measurements within enough time to give margin to TRISO fuel temperature limits and vessel structural temperature limits.
- The safety-related RVACS eventually initiates according to the safety-related sensors and logic. This may include a delay timer depending on the final design of the RVACS. The timing and capacity of RVACS will give margin to TRISO fuel temperature limits and vessel structural temperature limits.
- A safe, stable state is reached when the reactor is subcritical and vessel temperatures have reached the threshold defined for safe shutdown.

A set of Design Basis External Hazard Levels are selected to form an important part of the design and licensing basis. This determines the design basis seismic events and other external events that the safety related SSCs will be required to withstand.

All safety-related structures, systems, and components (including the set that is credited in this example) are evaluated to ensure that they can perform their safety function in the conditions presented by any of the design basis external hazard levels.

B.2.8 Task 7a: Evaluate LBEs Against Frequency-Consequence Target (Event Evaluation)

The LBEs identified in Task 4 must be plotted on the frequency-consequence curve to evaluate risk-significance. For this example, a conservative assumption for radioactive consequence will be used for demonstration of the method. There are three regions on the frequency-consequence curve, as demonstrated in Figure 3-3: non risk-significant region, risk-significant region, and outside of target.

When plotted on the frequency-consequence chart with uncertainties, none of the licensing basis events identified in Task 4 are characterized as risk-significant.

Anticipated Loss of Flow (AOO-1)

The anticipated loss of flow event is not risk-significant based on the frequency-consequence targets, as shown in Figure B-5.

The system performance targets for nonsafety-related reactor shutdown and normal decay heat removal are defined such that for AOO-1, dose consequences can be calculated with high confidence to be less than 2.5 mrem.

For this example, an upper-bound consequence of 2.5 mrem is assigned for demonstration. This is conservative value given that performance requirements for the nonsafety-related will likely be set such that effectively no release results from this event.

Design Basis Loss of Flow (DBE-1)

The design basis loss of flow event is not risk-significant based on the frequency-consequence targets, as shown in Figure B-6.

The system performance targets for safety-related reactor shutdown and RVACS are defined such that for LOF-DBE-1, dose consequences can be calculated with high confidence to be less than 100 mrem.

For this example, an upper-bound consequence of 100 mrem 30-day dose is set, which could translate to a capability requirement for both safety-related functions.

LOF-DBE-1 is shown to be less than 10^{-2}/yr in frequency with high confidence. This relies on the following system reliabilities. Both of these systems have safety-significance, but not risk-significance, due to their role in keeping the design basis event frequency rare.

- The reliability of the normal reactor shutdown system to detect the loss of flow and insert control elements, avoiding a safety-related reactor trip
- The reliability of the normal decay heat removal system to actuate and remove decay heat, avoiding a demand on safety-related RVACS

Beyond Design Basis Loss of Flow (BDBE-1, BDBE-2)

The two beyond design basis events are not risk-significant based on the frequency-consequence targets as shown in Figure B-7 and Figure B-8.

The operation actions and equipment design supporting both beyond design basis events are given performance targets with success criteria such that safety systems failed to maintain doses within 100 mrem, but successful plant contingencies are capable of maintaining consequences less than 1 rem. As with the other events this upper bound was assumed to be the consequence result for demonstration.

BDBE-1 is shown to be less than 10^{-4}/yr in frequency with high confidence. This relies on the following system reliabilities. Because of this, both systems have safety significance.

- The reliability of the normal decay heat removal system to actuate and remove decay heat
- The reliability of safety-related RVACS to operate given the unavailability of normal decay heat removal

BDBE-2 is also shown to be less than 10^{-4}/yr in frequency with high confidence. This relies on the following system reliabilities. Again, both systems have safety significance due to their role in maintaining the low BDBE frequency.

- The reliability of the normal reactivity control shutdown
- The reliability of the safety reactivity control shutdown

Figure B-5. Anticipated Loss of Flow (AOO-1) Plotted with Uncertainty on the Frequency-Consequence Chart

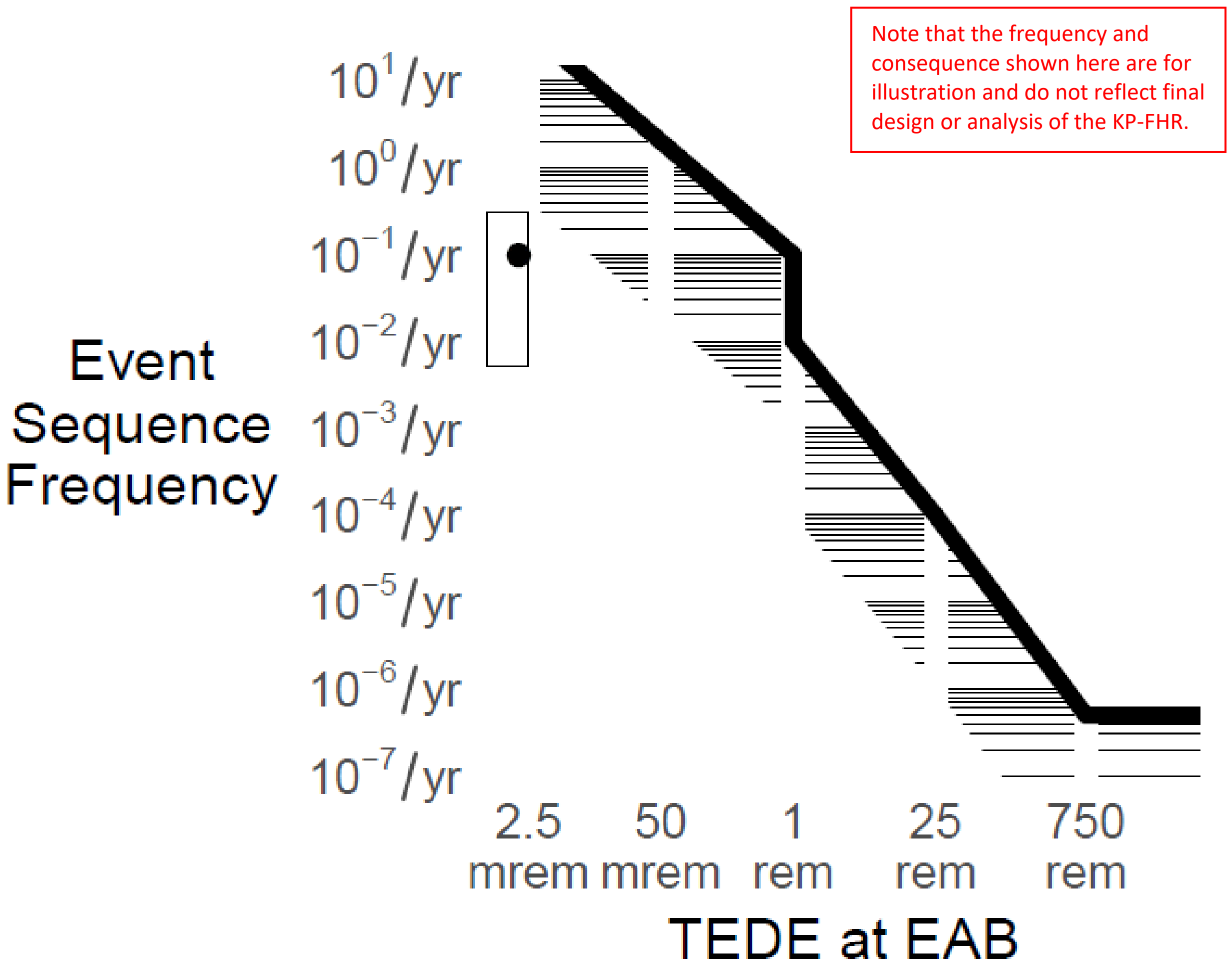


Figure B-6. Design Basis Loss of Flow (DBE-1) Plotted with Uncertainty on the Frequency-Consequence Chart

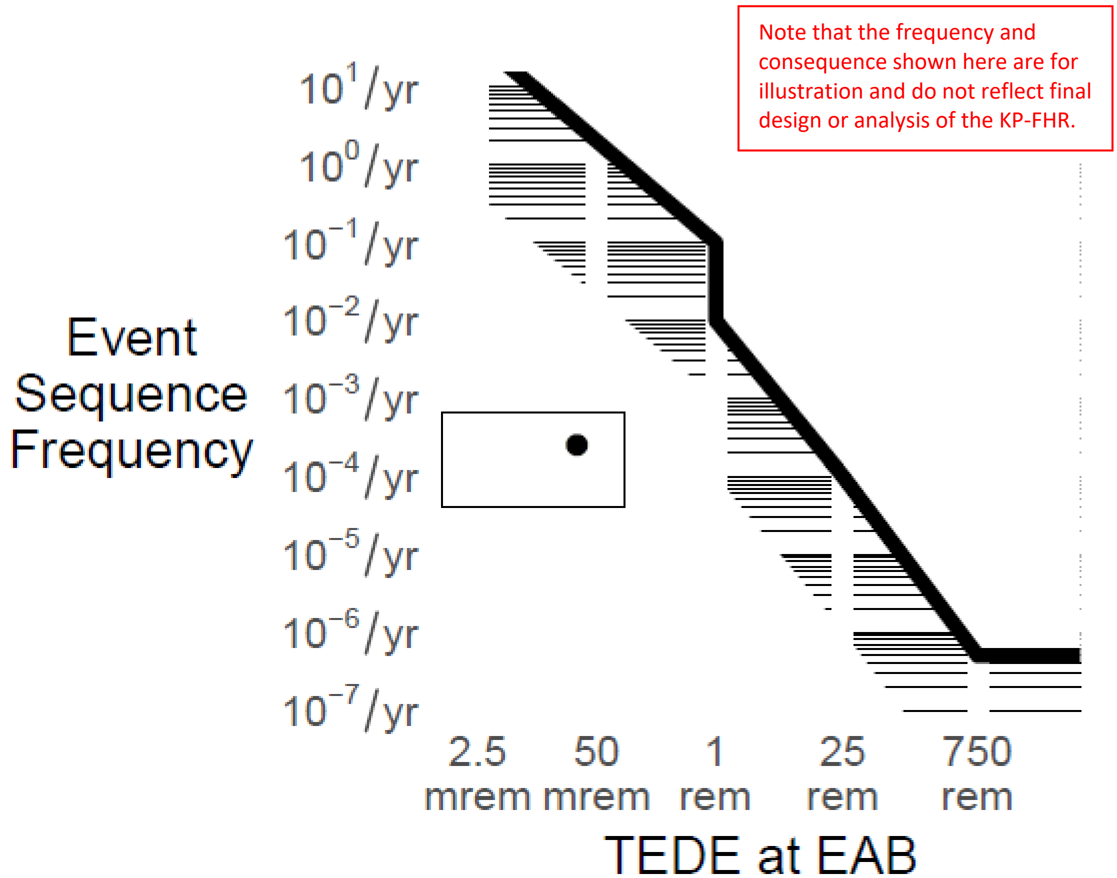


Figure B-7. Beyond Design Basis Loss of Flow (BDBE-1)Plotted with Uncertainty on the Frequency-Consequence Chart

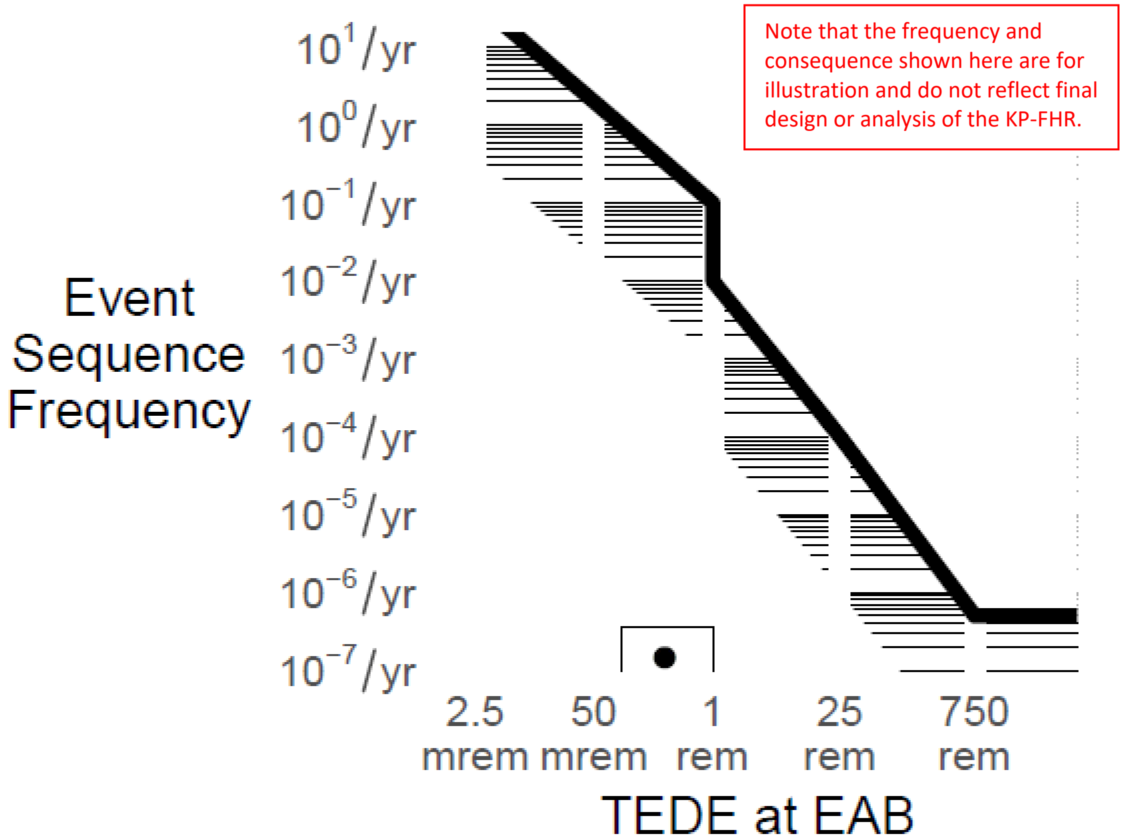
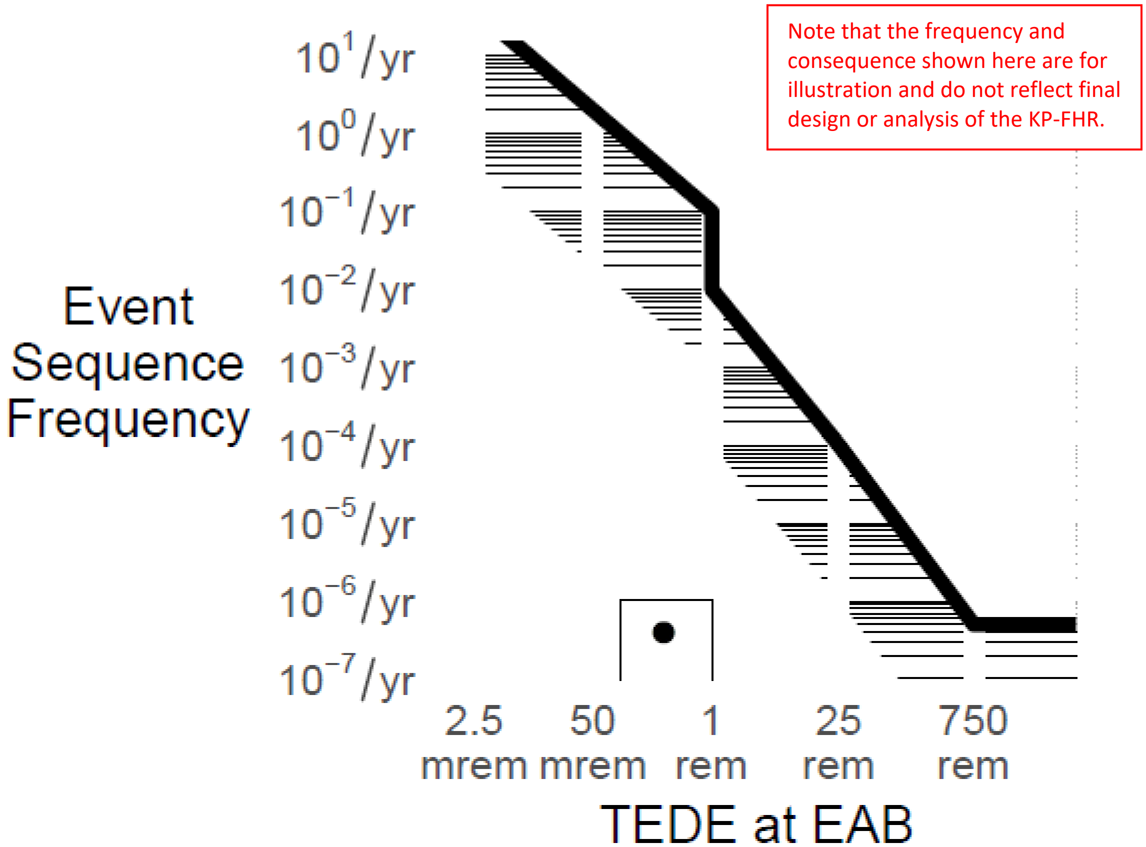


Figure B-8. Beyond Design Basis Loss of Flow (BDBE-2) Plotted with Uncertainty on the Frequency-Consequence Chart



B.2.9 Task 7b: Evaluate Integrated Plant Risk Against QHOs and 10 CFR 20

In this task, the integrated risk of the entire plant including all the LBEs is evaluated against three cumulative risk targets including:

- The risk to the average individual of early fatality within 1 mile of the Exclusion Area Boundary (EAB) from all LBEs should not exceed 5×10^{-7}/plant-year to ensure that the NRC Safety Goal QHO for early fatality risk is met.
- The risk to the average individual of latent cancer fatalities within 10 miles of the EAB from all LBEs should not exceed 2×10^{-6}/plant-year to ensure that the NRC safety goal QHO for latent cancer fatality risk is met.
- The total frequency of exceeding a site boundary dose of 100 mrem from all LBEs should not exceed 1/plant-year. This metric is introduced to ensure that the consequences from the entire range of LBEs from higher frequency, lower consequences to lower frequency, higher consequences are considered.

The probabilistic risk assessment provides distributions for consequences that provides measures of both prompt and latent health risk. The distributions in each direction are sized reflecting a combination of the level of model uncertainty, design uncertainty, and data parametric uncertainty.

To demonstrate the acceptability of the cumulative risk, the events from Task 4 are assigned upper consequence limits and plotted on a frequency-consequence curve along with each limit as demonstrated in Figure B-9. The anticipated loss of flow has acceptable risk based on the quantitative health objective targets, as shown in Figure B-10. For this example, an upper-bound consequence of 10^{-8} prompt risk/event and 3×10^{-8} latent risk/event are assigned for demonstration.

The design basis loss of flow event has acceptable risk based on the quantitative health objective targets, as shown in Figure B-11. For this example, an upper-bound consequence of 10^{-8} prompt risk/event and 3×10^{-8} latent risk/event are set.

The two beyond design basis loss of flow events have acceptable risk based on the quantitative health objective targets as shown in Figure B-12 and Figure B-13.

The evaluation of 10 CFR 20 is completed with a PRA that includes a complete set of event sequences, operating states, and hazard groups.

Figure B-9. Example of Prompt Health Risk of Licensing Basis Event Against a Target

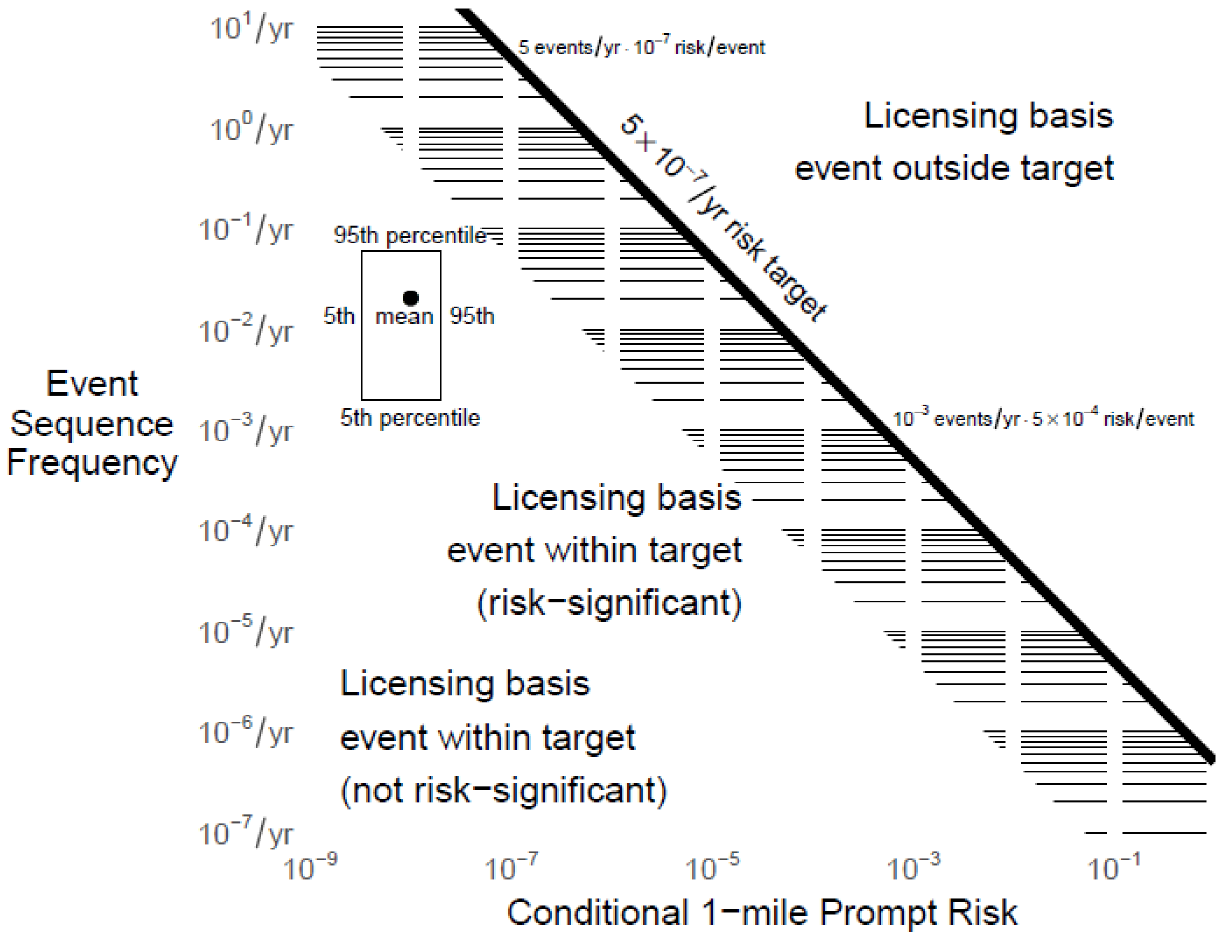


Figure B-10. Quantitative Health Risk for AOO Loss of Flow

Note that the frequencies and health risk results shown here are for illustration and do not reflect final design or analysis of the KP-FHR.

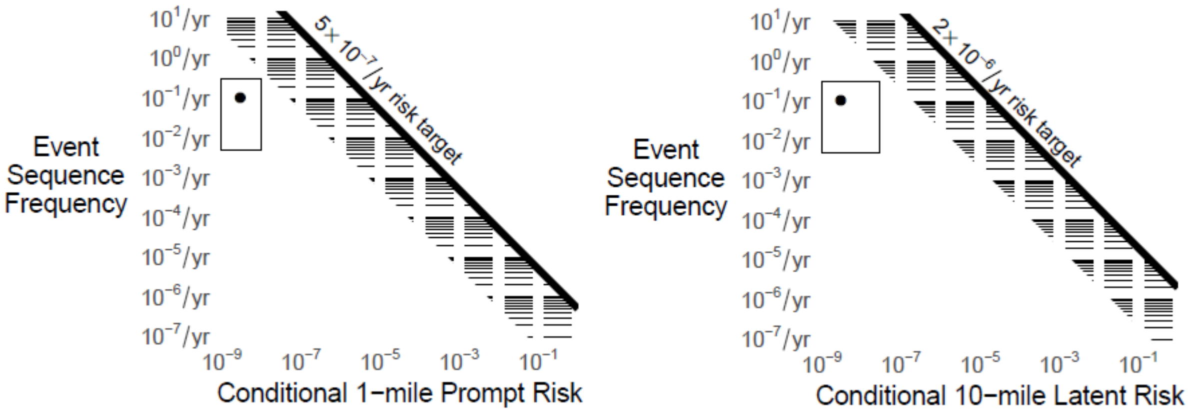


Figure B-11. Quantitative Health Risk for DBE Loss of Flow

Note that the frequencies and health risk results shown here are for illustration and do not reflect final design or analysis of the KP-FHR.

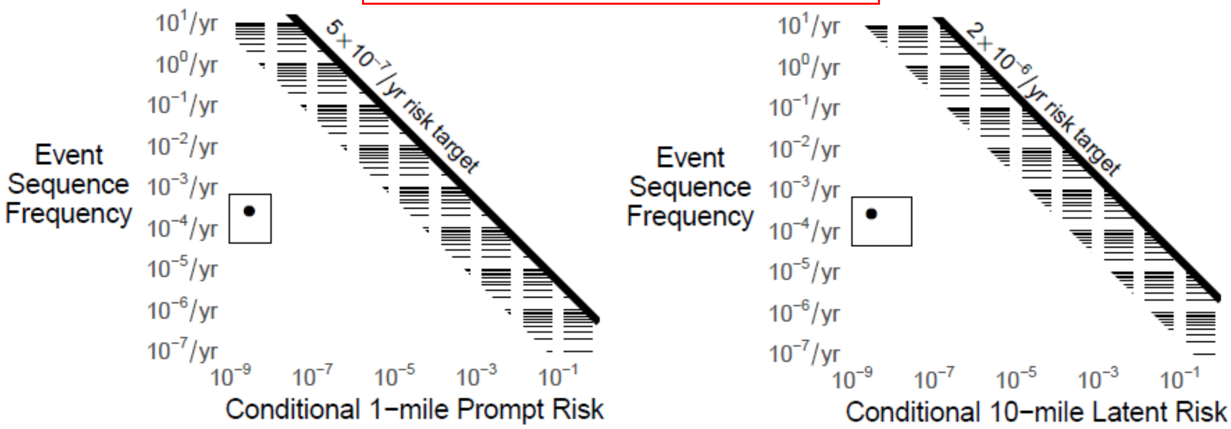


Figure B-12. Quantitative Health Risk for BDBE-1 Loss of Flow

Note that the frequencies and health risk results shown here are for illustration and do not reflect final design or analysis of the KP-FHR.

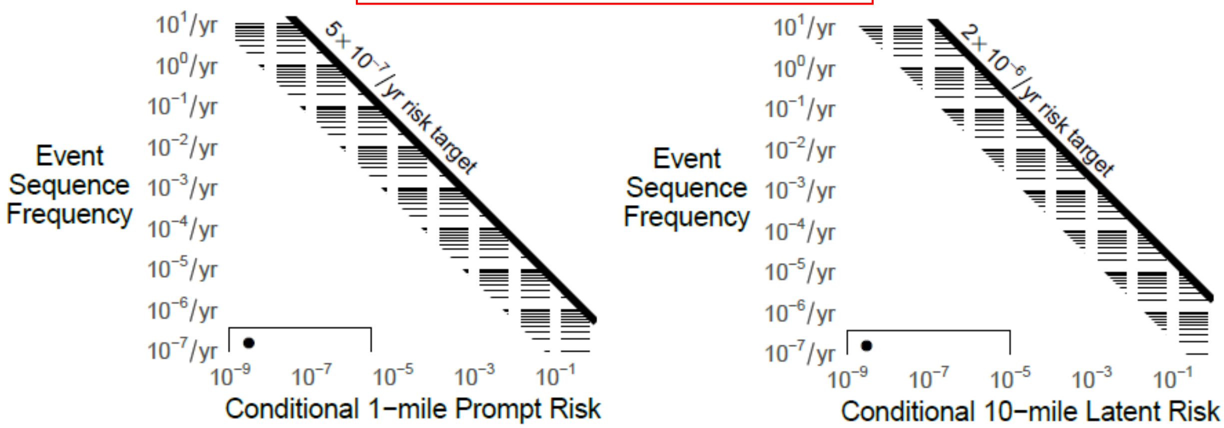
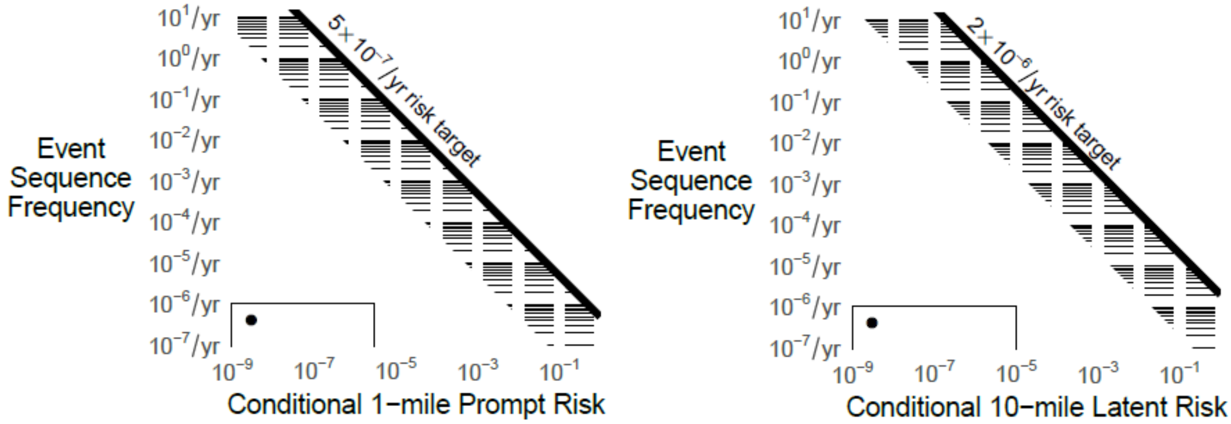


Figure B-13. Quantitative Health Risk for BDBE-2 Loss of Flow

Note that the frequencies and health risk results shown here are for illustration and do not reflect final design or analysis of the KP-FHR.



B.2.10 Task 7c: Evaluate Risk Significance of LBEs and SSCs Including Barriers

In this task, the details of the definition and quantification of each of the licensing basis events in Task 7a and the integrated risk evaluations of Task 7b are used to define the risk significance of individual licensing basis events and SSCs which include radionuclide barriers. These evaluations include the use of PRA risk importance metrics, where applicable, and the examination of the effectiveness of each of the layers of defense in retaining radionuclides. Licensing basis events are classified as risk significant if the licensing basis event site boundary dose exceeds a small fraction of background radiation exposure and the frequency of the dose is within 1% of the frequency-consequence target. SSCs are classified as risk significant if the SSC function is necessary to keep any licensing basis events inside the frequency consequence target, or if the total frequency of licensing basis events with the SSC failed is within 1% of any of the three cumulative risk targets identified in Task 7b. This information is used to provide risk insights, to identify safety significant SSCs, and to support the risk-informed performance-based evaluation of defense-in-depth in Task 7e.

Risk significance of Licensing Basis Events

Based on the figures provided in support of Task 7a above, each licensing basis event is evaluated against its proximity to the frequency-consequence target line. Any licensing basis event with a 95th percentile frequency or 30-day dose that falls within a factor of one hundred of the target line is considered risk-significant. Using these criteria, the loss of flow events are not risk-significant.

Based on the figures provided in support of Task 7b above, each licensing basis event is evaluated against its proximity to the prompt and latent quantitative health objective risk targets. Any licensing basis event with a 95th percentile frequency or conditional risk that falls within a factor of one hundred of the target line is considered risk-significant. Using these criteria, the loss of flow events are not risk-significant to prompt or latent health.

Similar to the quantitative health objectives, the risk to release of exceeding a dose of 100 mrem release is evaluated in support of Task 7b. Any licensing basis event with a 95th percentile frequency that is within 1% of the target risk is considered risk-significant. None of the loss of flow events match this criterion.

Risk-Significance of SSCs

An SSC is classified as risk-significant if the risk significance criteria are met for any SSC function included within the licensing basis events. There are two sources of risk criteria.

One criterion is if the SSC is necessary to keep an LBE within the F-C target. The risk-significance of a function performed by a structure, or component is depicted graphically by plotting on the frequency-consequence chart the licensing basis event or events where a given system is successful, then plotting the same LBE assuming the SSC is not functioning, as shown in Figure B-14. To assess the risk-significance of the system, the hybrid point on the frequency-consequence chart is marked where the upper bound frequency of the event with system success is matched with the upper bound consequence of the event where the system is unavailable. If that point is beyond the frequency-consequence target, then that system was significant in keeping the licensing basis event group within the target and is therefore risk-significant. If the hybrid point connecting system success frequency to system failure consequence falls beneath the frequency-consequence target, then that system is not risk-significant according to this criterion. There are additional defense in depth considerations that could cause the system to be risk-significant even if the hybrid point falls below the frequency-consequence target in this exercise based upon the cumulative risk of all LBEs.

The second source of risk significance criteria is in the cumulative risk metrics for the plant. A significant contribution to each cumulative risk metric limit is satisfied when total frequency of all LBEs with failure of the SSC exceeds 1% of the cumulative risk metric limit. This SSC risk significance criterion may be satisfied by an SSC whether or not it performs functions necessary to keep one or more LBEs within the F-C Target. The cumulative risk metrics and limits include:

- The total frequency of exceeding a site boundary dose of 100 mrem should not exceed 1/plant-year to ensure that the annual exposure limits in 10 CFR 20 are not exceeded. An SSC makes a significant contribution to this cumulative risk metric if the total frequency of exceeding a site boundary dose of 100 mrem associated with LBEs with the SSC failed is greater than 10^{-2}/plant-year.

- The average individual risk of early fatality within 1 mile of the EAB should not exceed 5×10^{-7}/plant-year to ensure that the NRC safety goal QHO for early fatality risk is met. An SSC makes a significant contribution to this cumulative metric if the individual risk of early fatalities associated with the LBEs with the SSC failed is greater than 5×10^{-9}/plant-year.

- The average individual risk of latent cancer fatalities within 10 miles of the EAB should not exceed 2×10^{-6}/plant-year to ensure that the NRC safety goal QHO for latent cancer fatality risk is met. An SSC makes a significant contribution to this cumulative risk metric if the individual risk of latent cancer fatalities associated with the LBEs with the SSC failed is greater than 2×10^{-8}/plant-year.

The cumulative risk limit criteria in this SSC classification process are provided to address the situation in which an SSC may contribute to two or more LBEs that collectively may be risk-significant even though the individual LBEs may not be significant. All LBEs within the scope of the supporting PRA should be included when evaluating these cumulative risk limits. In such cases, the reliability and availability of such SSCs may need to be controlled to manage the total integrated risks over all the LBEs.

Risk-Significance of NonSafety-Related Reactivity Control and Decay Heat Removal Systems

Nonsafety-related reactivity control structures, systems, and components are not risk-significant based on the frequency-consequence target. Additionally, nonsafety-related normal shutdown cooling structures, systems, and components are not risk-significant based on the frequency-consequence target as shown in Figure B-15. The nonsafety-related reactivity control equipment includes the following:

- Non-safety reactivity control elements

- Control element release and drive mechanisms

- Instrumentation to detect the need for reactivity control (i.e. thermocouples, transducers)
- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the control elements and drives

The nonsafety-related normal shutdown cooling equipment includes the following:

- Normal shutdown cooling piping, heat exchangers, and ultimate heat sink equipment
- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to actuate normal shutdown cooling
- Structural supports for piping, heat exchangers, and ultimate heat sink equipment
- Support systems that ensure the availability of normal shutdown cooling to provide the decay heat removal function

Risk-Significance of Safety-Related Reactivity Control

Safety-related reactivity control structures, systems, and components are not risk-significant based on the frequency-consequence target as shown in Figure B-16. The safety-related equipment for the reactivity control function includes:

- Safety-related reactor shutdown rods
- Shutdown rod release and drive mechanisms
- Instrumentation to detect the need for reactor shutdown (i.e. thermocouples, transducers)
- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the shutdown rods and drives

Risk-Significance of Safety-Related RVACS decay heat removal

Safety-related RVACS structures, systems, and components are not risk-significant based on the frequency-consequence target as shown in Figure B-17. The safety-related equipment for the decay heat removal function include:

- RVACS piping, including physical water storage tanks, cooling panels, valves and associated equipment
- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to open water valves and activate RVACS
- Structural supports for cooling panels
- Support systems that ensure the availability of RVACS to provide a passive decay heat removal function
- Air/water heat exchanger in RVACS stacks
- Physical RVACS chimneys
- Air intake structures
- Free-standing supports separate RVACS from the reactor building

Risk-Significance of Beyond Design Basis Reactivity control

Beyond design basis reactivity control structures, systems, and components are not risk-significant based on the frequency-consequence target as shown in Figure B-18. The beyond design basis equipment for the reactivity control function includes:

- Control room or reactor building equipment used by operators to manually recover from a failure to scram automatically
- Structures that protect manways or operator access to critical control element equipment to perform beyond design basis repair procedure actions
- Instrumentation and control systems that are critical to diagnosing failures

Risk-Significance of Beyond Design Basis Decay Heat Removal

Beyond design basis decay heat removal structures, systems, and components are not risk-significant based on the frequency-consequence target as shown in Figure B-19. The beyond design basis equipment for decay heat removal function include:

- Structures that protect manways or operator access to critical RVACS equipment to perform beyond design basis repair procedure actions

- Instrumentation and control systems that are critical to diagnosing failures

Risk-Significance of Components Separating Nonsafety-related and Safety-Related Reactivity control

Any structures, systems, or components that can lead to the concurrent unavailability of nonsafety-related reactivity control as well as safety-related reactivity control are risk-significant based on the frequency-consequence target as shown in Figure B-20. Examples of equipment that fits this description may include:

- Structures that separate the nonsafety-related instrumentation and control equipment from safety-related equipment

- Engineered solutions that separate nonsafety-related control element insertion equipment from safety control element insertion equipment

Risk-Significance of Components Separating Safety-Related From Beyond Design Basis Decay Heat Removal

Any structures, systems, or components that can lead to the concurrent unavailability of safety-related RVACS as well as beyond design basis decay heat removal are risk-significant based on the frequency-consequence target as shown in Figure B-21. Examples of equipment that fits this description may include:

- Ex-vessel structures that can collapse and impair the RVACS cooling capability function beyond repair

- In-vessel structures that can impair natural circulation of salt coolant and prevent long-term heat transfer to RVACS

SSC Significance Evaluation Summary

Table B-1 provides a summary of each of the major functions described in this sample LBE with the result of the significance evaluations performed in this process.

Table B-1. Summary of SSC Function Classifications

Function Type	SSC Function	Risk-Significant	Safety-Significant	Safety-Related
Reactivity Control	Nonsafety-Related Reactivity Control	No	Yes	No
	Safety-related reactivity control	No	Yes	Yes
	SSCs separating non-safety from safety-related reactivity control	Yes	Yes	Yes
	SSCs separating safety-related from beyond design basis reactivity control capability	Yes	Yes	Yes
	Beyond design basis reactivity control	No	Yes	No
Decay Heat Removal	Nonsafety-related decay heat removal	No	Yes	No
	Safety-related RVACS decay heat removal	No	Yes	Yes
	SSCs separating non-safety from safety-related decay heat removal	Yes	Yes	Yes
	SSCs separating safety-related from beyond design basis decay heat removal capability	Yes	Yes	Yes
	Beyond design basis decay heat removal	No	Yes	No

Figure B-14. Example Determination of Risk-Significance Against Frequency-Consequence Curve

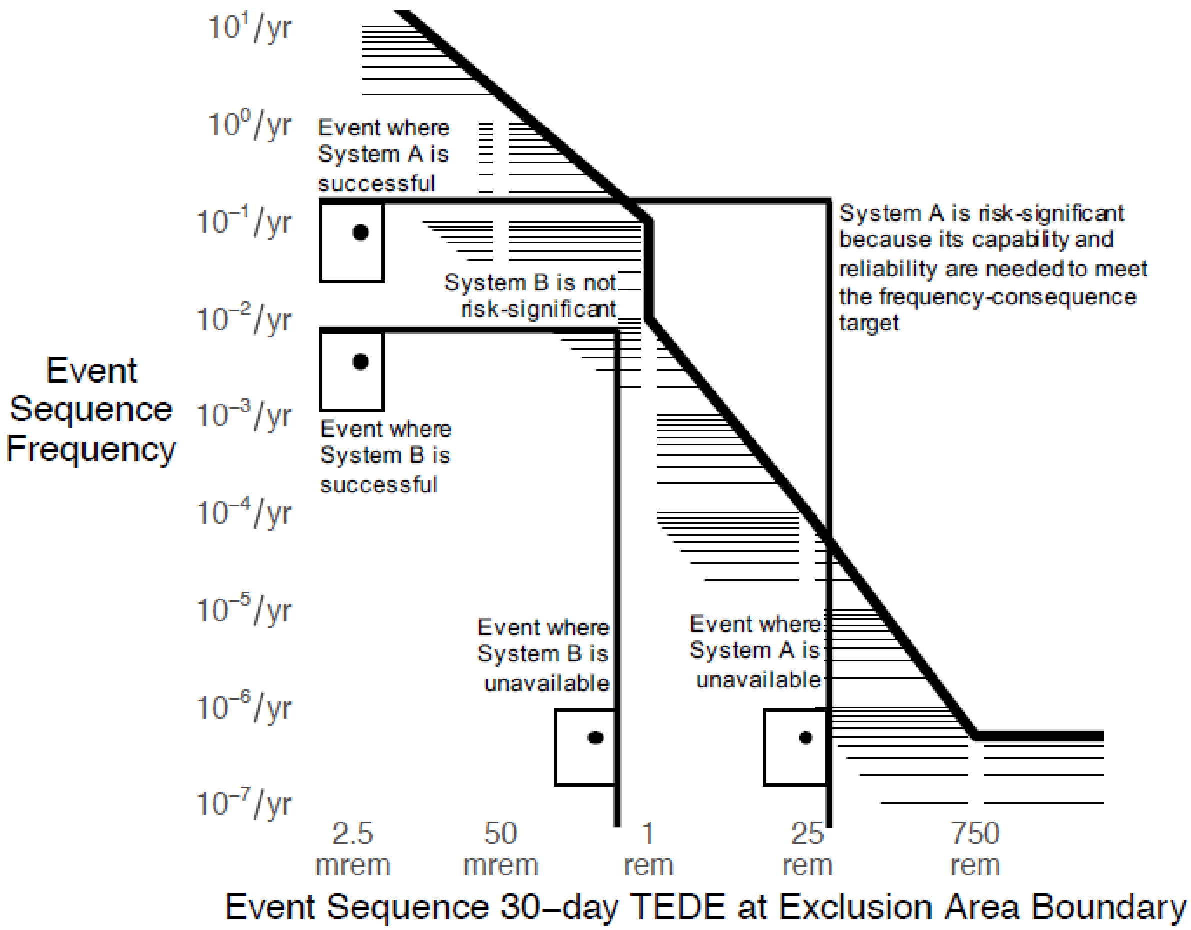


Figure B-15. SSCs Performing Nonsafety-Related Rector Control and NonSafety-Related Decay Heat Removal Functions Control the Anticipated Loss of Flow and Prevent the Design Basis Loss of Flow

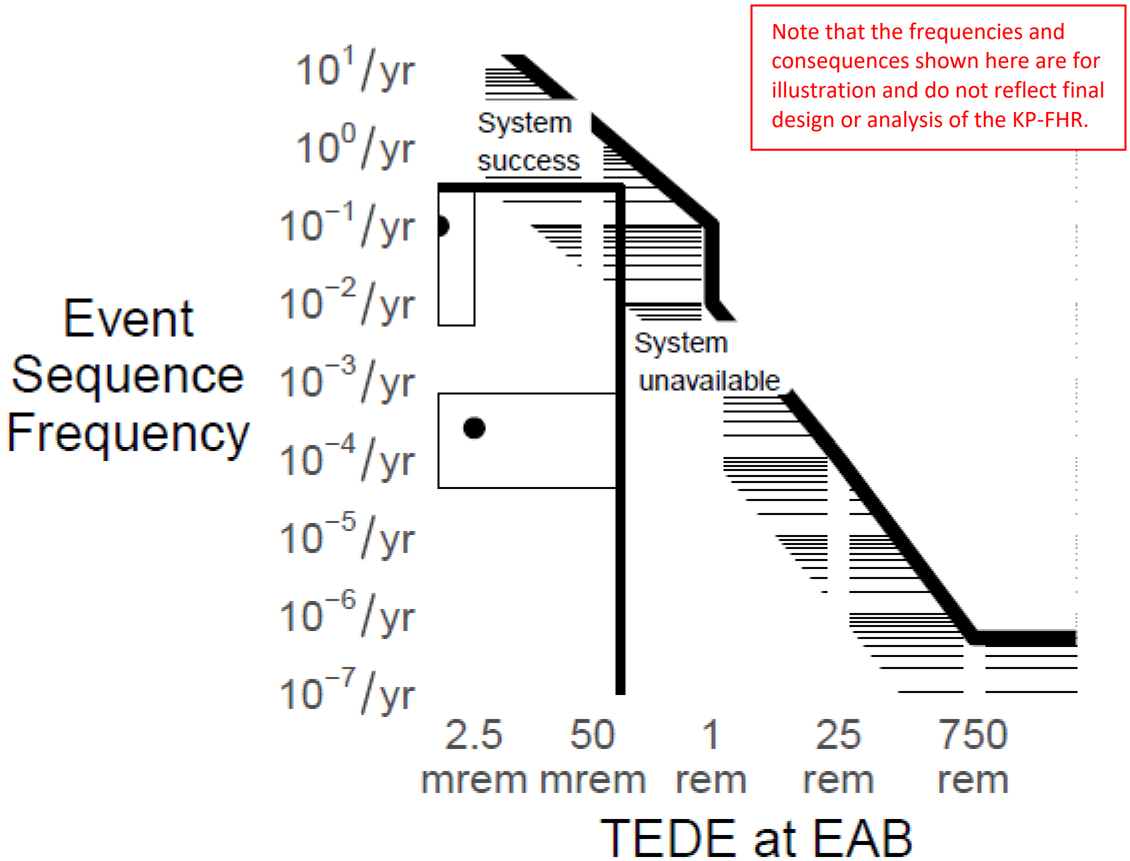


Figure B-16. SSCs Performing Safety-Related Reactivity control Function Control the Design Basis Loss of Flow and Prevent a Beyond Design Basis Loss of Flow

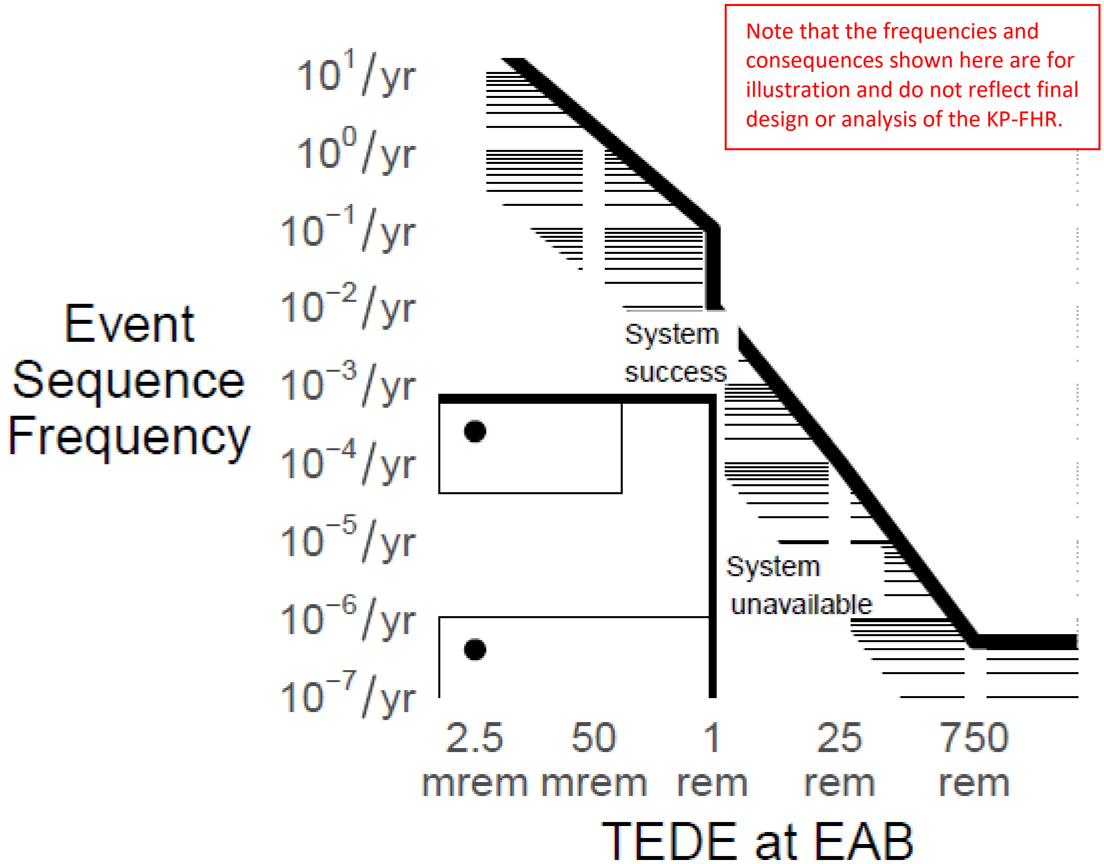


Figure B-17. SSCs Performing Safety-Related Decay Heat Removal Function Control the Design Basis Loss of Flow and Prevent the Beyond Design Basis Loss of Flow

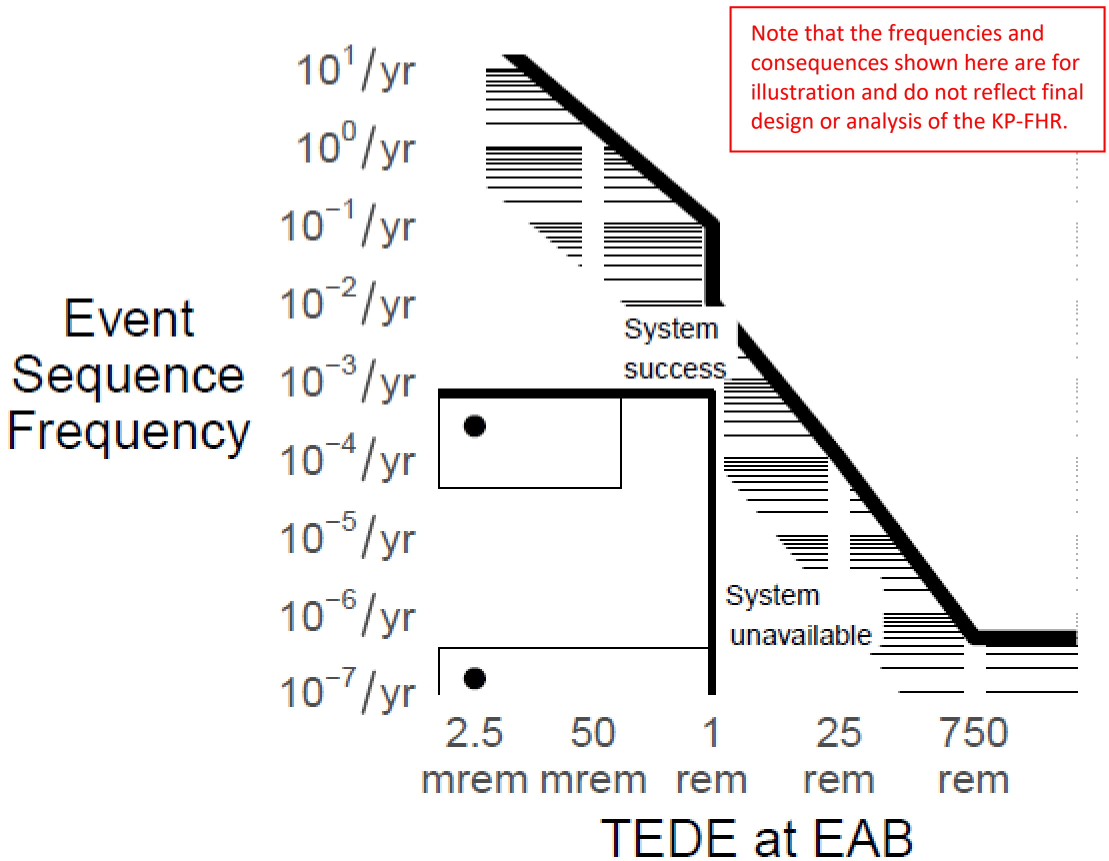


Figure B-18. SSCs Performing Beyond Design Basis Reactivity control Functions Mitigate a Beyond Design Basis Loss of Flow to Within Quantitative Health Objectives

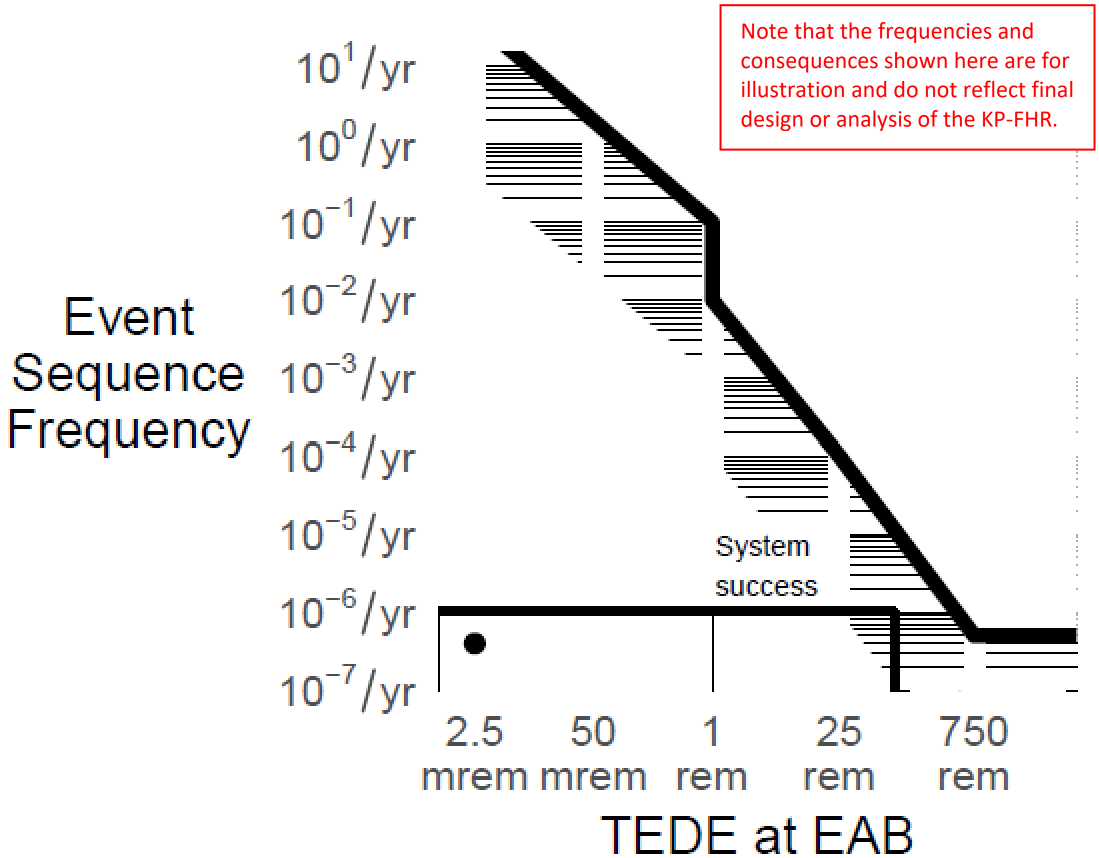


Figure B-19. SSCs Performing Beyond Design Basis Decay Heat Removal Function Mitigate Beyond Design Basis Loss of Flow Events to Within Quantitative Health Objectives

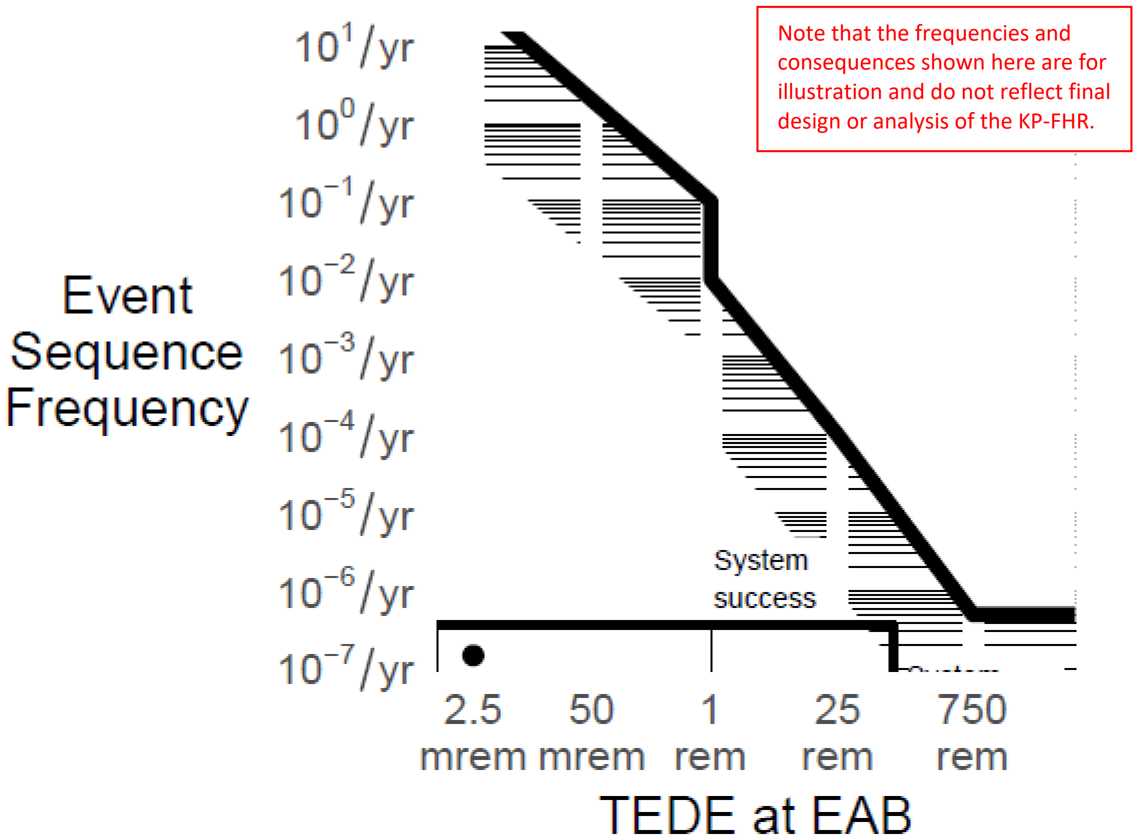


Figure B-20. SSCs That Separate NonSafety-Related and Safety-Related Reactivity control Function are Risk Significant on the Frequency-Consequence Chart

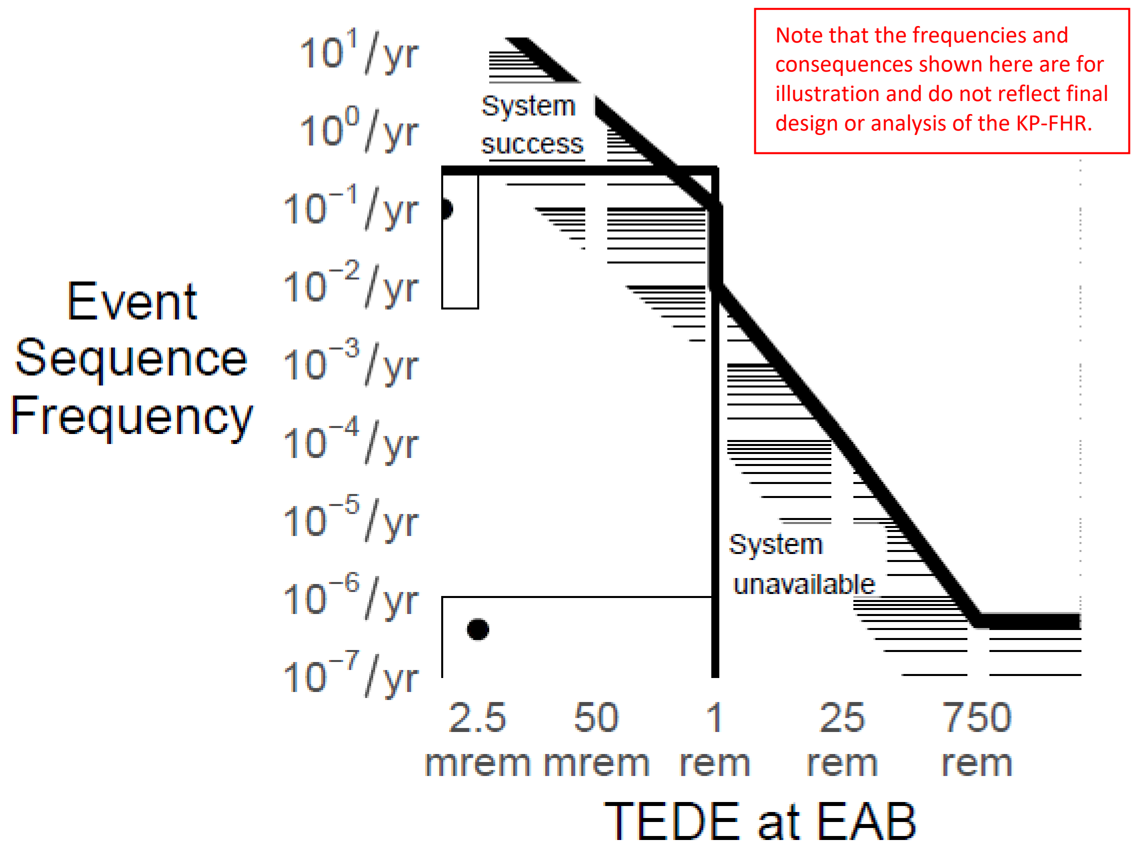
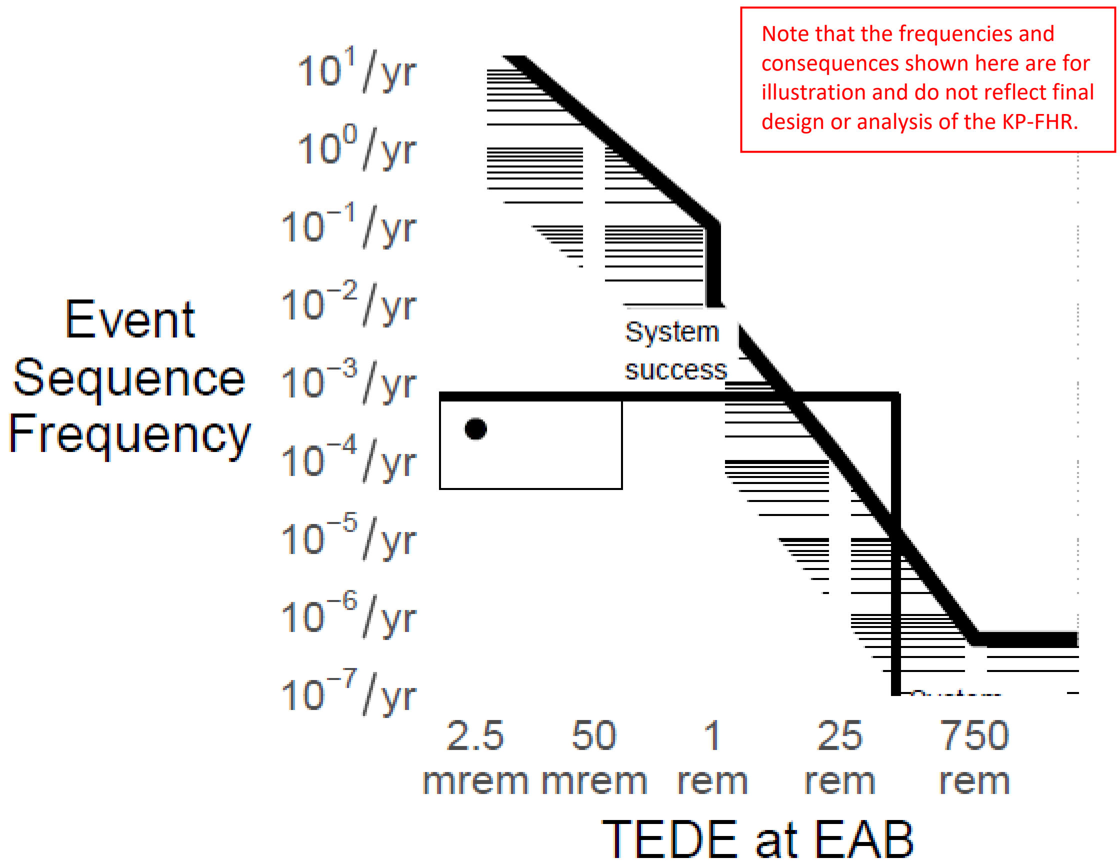


Figure B-21. SSCs That Separate Safety-Related and Beyond Design Basis Decay Heat Removal Functions are Significant on the Frequency-Consequence Chart



B.2.11 Task 7d: Perform Deterministic Safety Analyses Against 10 CFR 50.34

This task corresponds to the traditional deterministic safety analysis that is found in the transient analysis of the licensing application. It is performed on the Design Basis Accidents using conservative assumptions. The uncertainty analyses in the mechanistic source terms and radiological doses that are part of the PRA are available to inform the conservative assumptions used in this analysis and to avoid the arbitrary stacking of conservative assumptions.

The deterministic safety analysis uses the following high-level criteria from 10 CFR 50.34 for design basis accident calculations:

- An individual located at any point on the boundary of the exclusion area for any 2 hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).

- An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).

The description of the evaluation model and results will be provided in separate licensing application submittals.

B.2.12 Task 7e: Risk-Informed, Performance-Based Evaluation of Defense-in-Depth

Quantitative Defense-In-Depth

For the example event presented in this Appendix, demonstrative uncertainties were accounted for. All values driving the quantitative risk evaluation are treated with wide uncertainty distributions that represent the limits of design knowledge that was utilized as input to the sample event.

The complete risk assessment that supports the design will likely result in lower uncertainty and even wider margin to the targets described in Task 7.

Qualitative Defense-In-Depth

A detailed assessment of defense-in-depth adequacy is the scope of a separate evaluation. For this evaluation, it is important to note that qualitative defense-in-depth has been built into the selection of licensing basis events.

The design of plant response to various initiators is subdivided into a classical layers-of-defense paradigm, as shown in Figure B-22.

The first layer of defense is represented by the [[plant's normal resilience to upset conditions through inherent and active control features. For a loss of flow event, the ability of the primary core circulation pumps to maintain a flow rate in steady-state is the first line of defense against release.

The second layer of defense is represented by the plant's response to a failure of the first layer of defense. This presents the initiating event that is referred to in this work as the anticipated loss of flow. This event presents a challenge to the nonsafety-related front-line systems that are responsible for guaranteeing that the plant can be placed in a safe and stable condition following the initiating event. The nonsafety-related equipment includes nonsafety-related reactivity control and nonsafety-related decay heat removal. The nonsafety-related reactivity control equipment includes the following:

- Non-safety reactivity control rods
- Control rod release and drive mechanisms
- Instrumentation to detect the need for reactivity control (i.e. thermocouples, transducers)
- Logic equipment to translate instrument readings to shutdown signals
- Actuation equipment to release rods and/or drive rods into the core
- Support systems that ensure the availability of above
- Physical supports that secure the control rods and drives

The nonsafety-related normal shutdown cooling equipment includes the following:

- Normal shutdown cooling piping, heat exchangers, and ultimate heat sink equipment
- Instrumentation to detect the need for decay heat removal (i.e. thermocouples)
- Logic equipment to translate instrument readings to actuation signals
- Actuation equipment to actuate normal shutdown cooling
- Structural supports for piping, heat exchangers, and ultimate heat sink equipment
- Support systems that ensure the availability of normal shutdown cooling to provide the decay heat removal function

The third layer of defense is represented by the failures of layer 1 (initiating loss of flow) and layer 2 (unavailability of one of the front-line systems). This is a challenge to one or more safety-related systems.

Either the safety control elements are demanded to make the reactor subcritical, or the safety-related RVACS system is actuated to remove decay heat. The end state of successful layer 3 operation is a safe and stable condition.

The fourth layer of defense treats the rare case of concurrent failures of layer 1 (initiator), layer 2 (nonsafety-related equipment), and layer 3 (safety-related equipment). This is a beyond design basis event that is a challenge to systems and operator actions to recover failed functions under extreme conditions. The result of these events is not necessarily a safe and stable condition but is measured by the mitigation of radionuclide release. The beyond design basis equipment for the reactivity control function includes:

- Control room or reactor building equipment used by operators to manually recover from a failure to scram automatically

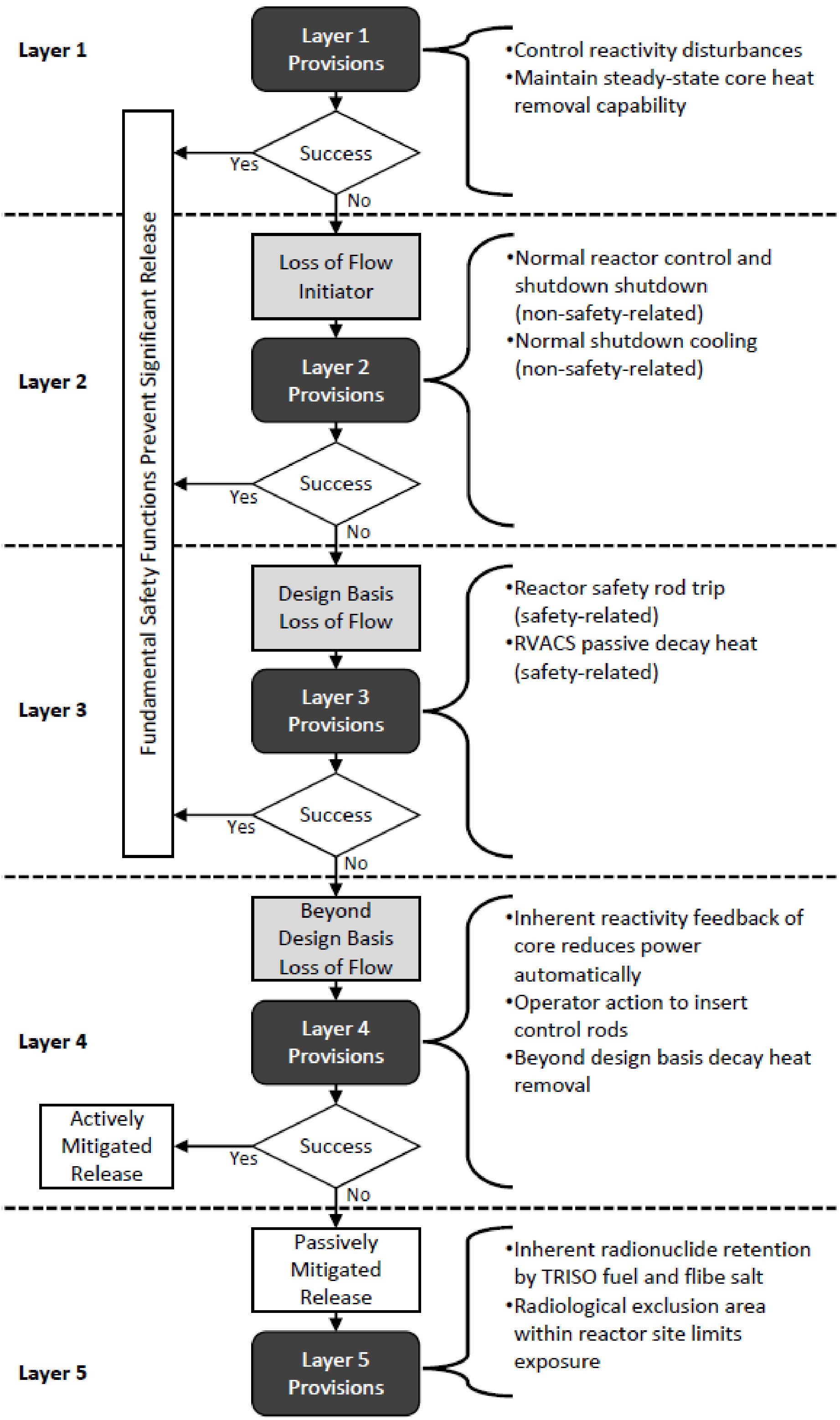
- Structures that protect manways or operator access to critical control rod equipment to perform beyond design basis repair procedure actions
- Instrumentation and control systems that are critical to diagnosing failures

The beyond design basis equipment for decay heat removal function include:

- Structures that protect manways or operator access to critical RVACS equipment to perform beyond design basis repair procedure actions
- Instrumentation and control systems that are critical to diagnosing failures

The fifth and final layer of defense considers the failure of systems and operator actions to recover from failures of safety-related systems. These events may end in a release that is not actively mitigated but is still passively mitigated by the inherent features of the plant. Such features include the low operating pressure which will limit the transmission of a source term, as well as the high-retention TRISO fuel and the radionuclide solvency of the primary coolant salt (Flibe).

Figure B-22. Layers of Defense for Loss of Flow Initiating Event Group



B.2.13 Task 8 – 10: Decide on Completion of Design/LBE Development, Proceed to Next Stage of Design Development, and Finalize List of LBEs and Safety-Related SSCs

The remaining tasks focus on characterizing the maturity of the design and finalizing the LBEs and SSC classifications. These tasks are beyond the scope of this illustrative example of a single LBE but are a part of the overall LBE methodology that are used in defining the final set of LBEs that will be presented in other licensing application submittals.