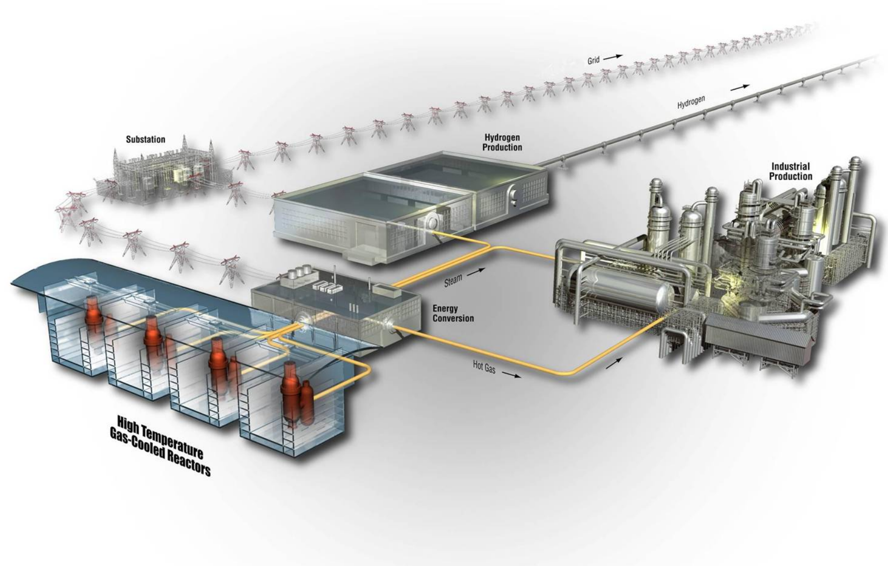
INL/EXT-11-21270

Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper

September 2011



The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Idaho National Laboratory

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXT-11-21270

Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper

September 2011

Idaho National Laboratory
Next Generation Nuclear Plant Project
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Next Generation Nuclear Plant Project

Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper

INL/EXT-11-21270

September 2011

Approved by:

Mark Holbrook NGNP Regulatory Affairs	9/19/11 Date
Jim Kinsey NGNP Regulatory Affairs Director	9-19-11 Date
S.C. Gladson for Phillip Mills PER TELECON NGNP Engineering Director	9/19/11 Date
Greg Gibbs NGNP Project Director	9/19/11 Date

ABSTRACT

This paper outlines the approach that will be followed to develop a Probabilistic Risk Assessment (PRA) for the Next Generation Nuclear Plant (NGNP) Project and subsequent high temperature gas-cooled reactors (HTGRs) in order to support a specific set of PRA applications that include:

- Evaluation of design alternatives and incorporation of risk insights into the design
- Input to the selection of licensing basis events (LBEs)
- Input to the safety classification of systems, structures and components (SSCs)
- Risk-informed evaluation of defense-in-depth.

The NGNP Combined License Application (COLA) will include an HTGR design-specific PRA. This paper outlines the relevant regulatory policy and guidance for this HTGR PRA, describes the approach being followed for the development of the PRA, and sets forth certain issues for review and discussion in order to facilitate preparation of the NGNP COLA.

Key elements discussed in this paper include the scope and objectives for the HTGR PRA, regulatory guidance used in the formulation of these objectives, and how the objectives have been factored into the PRA framework. The focus of the paper is to identify potential issues related to the performance of the PRA for use in the development of the NGNP design, selection of LBEs, safety classification of SSCs, and the risk informed evaluation of defense-in-depth.

The PRA approach that will be used to support the NGNP COLA will first be applied to a single reactor module plant defined in the NGNP COLA with the capability to extend later to multi-module designs to be certified for a range of sites. The PRA will be introduced at an early stage in the design, and will be upgraded at various design and licensing stages as the design matures and the design details are defined. This will provide an opportunity to optimize the design relative to safety and licensing by using the PRA to define the required capability and reliability of SSCs to prevent and to mitigate accidents.

CONTENTS

FIGURES

TABLES

ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
ANS	American Nuclear Society
AOO	anticipated operational occurrence
ASME	American Society of Mechanical Engineers
BDBE	beyond design basis event
CCDF	Complementary Cumulative Distribution Function
CDF	core damage frequency
CFR	Code of Federal Regulations
COLA	Combined Licence Application
DBA	Design Basis Accident
DBE	Design Basis Event
DOE	Department of Energy
EPA	Environmental Protection Agency
EPBE	Emergency Planning Basis Event
ESD	Event Sequence Diagram
GCR	gas-cooled reactor
HPB	helium pressure boundary
HPS	helium purification system
HRA	human reliability analysis
HTGR	high temperature gas-cooled reactor
HVAC	heating, ventilation, and air-conditioning
LBE	licensing basis event
LERF	large early release frequency
LOCA	loss of coolant accident
LWR	light water reactor
MHTGR	modular high temperature gas-cooled reactor
MPS	main power system
NGNP	Next Generation Nuclear Plant
NRC	Nuclear Regulatory Commission
OCS	operational plant control system
PAG	Protective Action Guide
PBMR	pebble bed modular reactor
PCU	power conversion unit

PDS	plant damage state
PRA	Probabilistic Risk Assessment
QHO	quantitative health objective
RCCS	reactor cavity cooling system
RIM	Reliability and Integrity Management
RPS	reactor protection system
RTNSS	regulatory treatment of non-safety systems
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan
SSC	structures, systems, and components

Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper

1. INTRODUCTION

1.1 Purpose

This paper outlines the approach that will be followed to develop a Probabilistic Risk Assessment (PRA) for the Next Generation Nuclear Plant (NGNP) Project and subsequent high temperature gas-cooled reactors (HTGRs) in order to support a specific set of PRA applications that include:

- Evaluation of design alternatives and incorporation of risk insights into the design
- Input to the selection of licensing basis events (LBEs)
- Input to the safety classification of structures, systems, and components (SSCs)
- Risk-informed evaluation of defense-in-depth.

The NGNP Combined License Application (COLA) will include an NGNP design-specific PRA. This paper outlines the relevant regulatory policy and guidance for this HTGR PRA, describes the approach being followed for the development of the PRA, and sets forth certain issues for review and discussion in order to facilitate preparation of the NGNP COLA.

Key elements discussed in this paper include the scope and objectives for the HTGR PRA, regulatory guidance used in the formulation of these objectives, and how the objectives have been factored into the PRA framework. The focus of the paper is to identify potential issues related to the performance of the PRA for use in the NGNP COLA.

A risk-informed approach to supporting licensing that, by definition, uses both deterministic and probabilistic elements is appropriate to introduce at an early stage in the NGNP Project's design and licensing processes. Within the context of the NGNP white papers, a "deterministic" process is defined as an approach that evaluates predetermined fixed scenarios based on physical principles. A deterministic process is prescriptive (in that elements of it may be imposed) and may incorporate bounding assumptions, criteria, or regulations which are imposed to compensate for related uncertainties. A "probabilistic" element is associated with an evaluation that explicitly accounts for the likelihood and consequences of possible accident sequences in an integrated fashion.

Risk insights to be developed from the PRA are viewed as essential to developing a design that is optimized in meeting safety objectives and in interpreting the applicability of the existing requirements to the safety design approach of the NGNP HTGR. Results and insights from the PRA will be needed to assure the safety of the design when compared to the Nuclear Regulatory Commission's (NRC's) Safety Goals and other Top Level Regulatory Criteria.

The HTGR PRA approach will be applied to a single reactor module NGNP defined in the COLA with the capability to extend later to multi-module plant designs to be certified for a range of sites. The PRA will be introduced at an early stage in the design, and will be upgraded at various design and licensing stages as the design matures and the design details are defined. This will provide an opportunity to optimize the design relative to safety and licensing requirements.

1.2 Objectives

The objectives of this paper are to:

- Summarize the regulatory requirements for performance of a PRA to support the NGNP COLA, and describe how the PRA approach will be used to meet these requirements.
- Identify the similarities and differences between the NGNP approach to PRA and the approach that has been followed for light water reactors (LWRs).
- Identify the key technical issues that will need to be resolved for the successful application of the PRA to the NGNP design.
- Describe the approach for using available guides, standards, and peer review processes to assure the technical adequacy of the PRA.
- Define the approach to developing the PRA so that it can be used to provide input to the selection of LBEs, information to select the safety classification of SSCs, the formulation of special treatment requirements, and to perform a risk-informed evaluation of defense-in-depth.
- Describe the approach to the PRA treatment of the integrated risk from operation of a multi-module plant.

1.3 Scope

The PRA approach described herein applies to all HTGR plant designs being considered for the NGNP and is intended to be generic for the various HTGR commercialization strategies being considered. The PRA methodology described in this white paper is intended for use on the NGNP and subsequent multi-module HTGR designs, and it is intended to be applied at various discrete points along the entire NGNP's design-operation life cycle.

1.4 Summary of Outcome Objectives

The NGNP Project is seeking (1) NRC's general concurrences and/or comments on the adequacy of the planned approach to performing the HTGR PRA and (2) to obtain feedback from the NRC on any issues that have the potential to significantly impact the effort and schedule to prepare a license application for a first-of-a-kind HTGR plant. The NGNP project is seeking agreement on its HTGR PRA approach for the following specific areas:

1. The scope of the HTGR PRA outlined in this paper is appropriate for the intended uses of the PRA in the NGNP COLA for the HTGR facility. These uses include input to:
    - Evaluation of design alternatives and incorporation of risk insights into the design
    - Input to the selection of LBEs
    - Input to the safety classification of SSCs
    - Risk-informed evaluation of defense-in-depth.
2. The approaches to initiating event selection, event sequence development, end state definition, and definition of risk metrics are appropriate.
3. The approach to the treatment of inherent characteristics and passive SSCs outlined in this paper is reasonable and consistent with current state-of-the-art PRAs.
4. The approach to the use of deterministic engineering analyses to provide the technical basis for predicting the plant response to initiating events and event sequences, success criteria, and mechanistic source terms yields an appropriate blend of deterministic and probabilistic inputs to support NGNP licensing.

5. The approach to the development of a PRA database outlined in this paper, including the use of applicable data from LWRs, use of expert opinion, and treatment of uncertainty, is a reasonable approach for the PRA.
6. The process for representing uncertainties and the quantification of mechanistic source terms in the PRA (as outlined in a companion paper on Mechanistic Source Terms[4]) is a reasonable approach for the purpose of developing and analyzing the results of the PRA.
7. The approach for the PRA treatment of single and multiple reactor accidents is sufficient to support licensing of a basic single HTGR module and for multi-module configurations.
8. The approach to using available guides and standards for PRA quality and independent peer review is an acceptable approach for determining the adequacy of the PRA for its intended uses outlined above.
9. The PRA approach to treatment of uncertainties is adequate for the intended PRA applications.
10. The PRA approach used to support the risk-informed evaluation of defense-in-depth in the design, construction, and operation of an HTGR is adequate.

1.5 Relationship to Other NGNP Topics/Papers

The NGNP approach to PRA has significant interrelationships to other NGNP white papers as described in the following:

- NGNP LBE Selection[1]

  The PRA methods for identifying initiating events across a full set of plant operating states and postulated hazard groups and for identifying event sequences provide for a systematic and exhaustive search for candidate LBEs. In the PRA modeling of event sequences, those sequences with similar plant initial conditions, initiating events, plant response of SSCs that perform safety functions, and end states are grouped into accident families that help define the LBEs. The event sequence frequencies, as expressed in terms of events per plant year, where a plant may consist of one or more reactor modules, are used to classify LBEs as Anticipated Operational Occurrences (AOOs), Design Basis Events (DBEs), and Beyond Design Basis Events (BDBEs). The consequences of those event sequences involving a release of radioactive material, as expressed in exclusion area boundary doses, the frequencies, and the associated quantified uncertainties in the frequencies and consequences of the LBEs derived from the PRA are compared against the frequency-consequence limits derived from the Top Level Regulatory Criteria (TLRC). Information from the PRA is used to inform the selection of Design Basis Accidents (DBAs) once the safety classification of SSCs is determined.

- NGNP SSC Safety Classification[2]

  Information developed and used in the PRA to define event sequences and evaluate their frequencies and consequences is reviewed as an input to the SSC classification and to establish the necessary and sufficient conditions of SSC capability and reliability in order for LBE frequencies, consequences, and uncertainties to stay within the limits defined by the frequency-consequence limits derived from the TLRC. Reliability requirements for SSCs are determined on the basis of the need to maintain each LBE within its LBE category (AOO, DBE, or BDBE). Its capability requirements are defined by the selected design margins between the LBE consequences and the dose limits for that LBE category. Special treatment requirements for SSCs are derived in order to achieve the necessary and sufficient degree of reliability and capability of the SSCs.

- NGNP Defense-in-Depth Approach[3]

  The PRA models and supporting assumptions are based in part on the plant capabilities for defense-in-depth reflected in the design as well as assumptions about the limits placed on design and operation of the plant by assumed programmatic defense-in-depth measures. Information developed in the PRA is used to help evaluate the SSCs responsible for preventing and mitigating accidents. The PRA also provides an important role in the identification of key sources of uncertainty, and this supports a feedback loop to identify possible enhancements to plant capability and programmatic aspects of defense-in-depth. Hence, the PRA provides important input to the risk informed evaluation of defense-in-depth and complements the NRC's deterministic approach and traditional defense-in-depth philosophy.

- NGNP Mechanistic Source Terms[4]

  This white paper addresses the NGNP approach to developing mechanistic source terms for use in the safety analyses. In the PRA, the consequences of those event sequences involving a release of radioactive material will be based on event specific mechanistic source terms using realistic assumptions and quantitative estimates of the associated uncertainties. In the safety analysis of the DBAs, the mechanistic source terms and radiological consequences will be evaluated in a conservative manner.

2. REGULATORY FOUNDATION

2.1 U.S. Regulatory Foundation for PRA

2.1.1 NRC Regulations

The Commission originally issued 10 CFR Part 52 on April 18, 1989. This rule provided for issuing Early Site Permits (ESPs), standard design certifications, and COLs with conditions for nuclear power reactors. In 2007, the NRC published a revision to 10 CFR Part 52[5] and 10 CFR Part 50.[6] The revision to 10 CFR Part 52 includes the requirement for a COL applicant to conduct a plant-specific PRA, and to provide a description of the plant-specific PRA and its results within its Final Safety Analysis Report (FSAR). The revision to 10 CFR Part 50 includes the requirement for the COL holder to maintain and upgrade the PRA periodically throughout the life of plant.

Plants licensed under Part 52 must meet the requirements of 10 CFR 50.71(h), as follows:

> *(h)(1) No later than the scheduled date for initial loading of fuel, each holder of a combined license under subpart C of 10 CFR part 52 shall develop a level 1 and a level 2 probabilistic risk assessment (PRA). The PRA must cover those initiating events and modes for which NRC-endorsed consensus standards on PRA exist one year prior to the scheduled date for initial loading of fuel.*
>
> *(2) Each holder of a combined license shall maintain and upgrade the PRA required by paragraph (h)(1) of this section. The upgraded PRA must cover initiating events and modes of operation contained in NRC-endorsed consensus standards on PRA in effect one year prior to each required upgrade. The PRA must be upgraded every four years until the permanent cessation of operations under § 52.110(a) of this chapter.*
>
> *(3) Each holder of a combined license shall, no later than the date on which the licensee submits an application for a renewed license, upgrade the PRA required by paragraph (h)(1) of this section to cover all modes and all initiating events.*

Recognizing that this requirement was written for new LWR plants, the NGNP COLA intends to meet the intent of this requirement with the following clarifications. The Level 1-2-3 structure of a PRA developed for LWRs does not strictly apply to the HTGR under consideration for the NGNP for reasons given in Section 3 of this paper. However, the information to be developed in the HTGR PRA is comparable to that provided in a Level 1, Level 2, and certain aspects of a Level 3 LWR PRA in the sense that it will include a development of event sequences that involve releases to the point of defining mechanistic source terms, as well as offsite radiological doses. The HTGR PRA will use the available and applicable PRA standards as called for in this requirement. It is expected that a trial use version of the American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS) PRA Standard for Advanced non-LWRs will be approved in advance of the completion of the development of the COLA.

Another clarification on meeting this requirement is that the scope of the HTGR PRA will include a full range of event sequences, including those within and beyond the design basis, whereas the current PRA requirements for LWRs are limited to the treatment of severe accidents beyond the design basis.

2.1.2 NRC Policy Statements

2.1.2.1 PRA Policy Statement

On August 16, 1995, the Commission adopted the following Policy Statement regarding the expanded use of PRA[7]:

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.

PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices.

The approach to performing the HTGR PRA in support of the COLA and the expected uses of the information provided by the PRA to support the licensing basis are consistent with the expectations raised in this policy statement. The COLA will address both the stated NRC intent to rely more on PRA methods and the need to acknowledge and meet existing regulations.

The traditional licensing requirements referred to in this policy statement are embodied in a primary manner for LWRs in 10 CFR Part 50, Appendix A.[8] Risk insights from the PRA will be used to guide the application of the traditional deterministic licensing requirements to the NGNP and its safety design philosophy. The risk-informed safety design and licensing approach adopted for the NGNP COLA includes a systematic review of the regulations to assure that all are met to the extent they are applicable and that the associated licensing principles are applied in a manner appropriate for the NGNP. Risk insights from the PRA are also expected to be useful to identify any safety issues specific to the NGNP for appropriate regulatory treatment. Through the process of integrating the risk significant event sequences with the LBEs, an enhanced level of coherence between the deterministic and probabilistic perspectives is expected.

As explained more fully in the white paper on the NGNP approach to defense-in-depth, risk insights from the PRA will be used to complement the application of deterministic defense-in-depth principles. Hence, the uses of the PRA for the NGNP are considered to be consistent with the intent of this policy statement.

2.1.2.2 Policy Issues Related to Use of PRA for non-LWRs

The NGNP COLA is subject to policy issues involving non-LWR applications. It is the intent of the COLA to comply with the NRC's guidance on these issues.

SECY 2003-0047, "Policy Issues Related to Licensing Non-Light Water Reactor Designs,"[9] offers staff recommendations on seven relevant policy issues that had been originally defined in SECY 2002-0139. Of these seven issues there are two, Issue 4: 'Use of PRA to Support Licensing Basis' and Issue 5: "Use of Mechanistic Source Terms," which specifically relate to the NGNP HTGR PRA and are discussed herein. On these two issues the Staff Requirements Memorandum for SECY 2003-0047[10] stated the Commissioner's approval of the staff recommendations on both of these issues.

Also included, but left unresolved from the seven issues of SECY 2003-0047, were policy issues associated with the treatment of integrated risk on multi-reactor sites and for modular reactor designs, which is part of Issue 4. These are addressed below.

With respect to Issue 4, the staff recommended that the Commission take the following actions:

Modify the Commission's guidance, as described in the SRM of July 30, 1993, to put greater emphasis on the use of risk information by allowing the use of a probabilistic approach in the identification of events to be considered in the design, provided there is sufficient understanding of plant and fuel performance and deterministic engineering judgment is used to bound uncertainties.

- *Allow a probabilistic approach for the safety classification of structures, systems, and components.*
- *Replace the single failure criterion with a probabilistic (reliability) criterion.*

> *This recommendation is consistent with a risk-informed approach. It should be noted that this recommendation expands the use of probabilistic risk assessment (PRA) into forming part of the basis for licensing and thus puts greater emphasis on PRA quality, completeness, and documentation.*

The NGNP COLA will include an NGNP design-specific PRA and demonstrate compliance with the staff recommendation for Issue 4. Risk information is being used and will be presented in the COLA to support the "probabilistic approach in the identification of events to be considered in the design." The need for 'sufficient understanding of plant and fuel performance' is acknowledged and will be addressed by future topical reports covering the verification and validation of evaluation models and code suites; fuel design and qualification,[11] and in the development of the mechanistic source terms that will be used in the PRA[4] and in the safety analysis of design basis events. The integration of the PRA with deterministic analyses and engineering judgment will be demonstrated. The classification of SSCs will follow an approach based on the LBEs derived from the PRA results as described in another paper on the safety classification of SSCs.[2] The NGNP COLA will include a use of the PRA to evaluate the accident prevention and mitigation strategies as discussed in the paper on defense-in-depth.[3]

With respect to Issue 5 of SECY 03-0047, the staff recommended that the Commission take the following action:

> *Retain the Commission's guidance contained in the July 30, 1993, SRM that allows the use of scenario-specific source terms, provided there is sufficient understanding and assurance of plant and fuel performance and deterministic engineering judgment is used to bound uncertainties.*
>
> *This recommendation will allow credit to be given for the unique aspects of plant design (i.e., performance-based) and builds upon the recommendation under Issue 4. Furthermore, this approach is consistent with prior Commission and ACRS views. However, this approach is also dependent upon understanding fuel and fission product behavior under a wide range of scenarios and on ensuring fuel and plant performance is maintained over the life of the plant.*

SECY 2003-0047 states that in NUREG-1338, "Draft Preapplication Safety Evaluation Report for the Modular High Temperature Gas-Cooled Reactor,"[12] the staff had stated that final acceptance of the mechanistic source term was "contingent on the satisfactory resolution of technical and policy considerations" and noted that "extensive research and testing was needed to address the technical issues."

In their review of these NRC staff recommendations regarding Issue 5, the Advisory Committee on Reactor Safeguards (ACRS), in a letter dated February 19, 1993,[13] stated that:

> *The staff proposal to base the source term on mechanistic analyses appears reasonable, although it is clear that the present data base will need to be expanded.' and 'It will be appropriate for the staff to consider using newer approaches when it develops source terms, and to take specific account of the unique features of …the reactor type.*

The HTGR PRA that will be performed to support the NGNP COLA, which is discussed more fully in Section 3 of this paper, will be of sufficient scope and detail to calculate the frequencies and radiological consequences of design-specific event sequences, and it will address the uncertainties in both frequencies and consequences. The information to be provided by the HTGR PRA is similar to that provided in an LWR Level 3 PRA with the clarification that the calculation of offsite consequences is expected to be simpler as compared to a full scope Level 3 PRA, due to the reduced complexity of the HTGR design. Hence, the PRA will use mechanistic source terms as well as radiological dose calculations to assess the consequences of the modeled event sequences. Mechanistic source terms will also be required to perform the safety analysis for Design Basis Accidents (DBAs) that will be included in the COLA. Among the issues to be resolved is the issue of establishing the adequacy of the mechanistic source terms. This includes demonstrating sufficient understanding of fuel and plant performance and all significant radionuclide transport phenomena for a sufficiently wide range of scenarios. Resolution of these issues is expected to place requirements on the safety analyses that will be included in the COLA. More details on source term treatment are found in a separate paper.[4]

The HTGR PRA performed to risk-inform the licensing bases for the NGNP COLA will be updated as necessary to reflect changes in the plant design, construction, and operational stages to the extent needed to ensure that conclusions derived from previous upgrades of the PRA in support of the licensing basis remain valid. The methods for selecting LBEs and for making safety classification of SSCs as described in other papers include deterministic elements to address uncertainties in the PRA results so that LBE selection is not expected to be sensitive to expected small numerical changes in the PRA results during subsequent PRA updates. In summary, the NGNP COLA will use the PRA and mechanistic source terms consistent with the staff recommendations in SECY 03-0047 for Issues 4 and 5.

Another issue addressed in SECY 03-0047 is the consideration of the integrated risk of a multi-reactor module facility. The PRA will address the integrated risk of multi-module HTGR designs in an explicit manner. As explained more fully in Section 3 of this paper, this will be accomplished by using risk metrics based on event sequence frequencies calculated on a per plant year and by including event sequences that include releases from two or more modules. This approach is expected to accommodate a full range of outcomes of ongoing policy discussions among the staff, Commissioners, and ACRS regarding the issue of integrated risk.

The HTGR PRA performed to support the COLA will include a full-scope PRA treatment of internal and external hazard groups and different plant operating states. The treatment of relevant issues in the PRA is expected to be consistent with the staff expectations for future designs.

The Advanced Reactor Policy Statement[14] states that for advanced reactors the Commission expects, as a minimum, the same degree of protection of the public and the environment that is required for current generation LWRs. This policy was reaffirmed in the SRM to SECY 2003-0047. Thus, the Commission expects that advanced reactor designs will comply with the Commission’s Safety Goals Policy Statement.[15] Furthermore, the Commission expects that advanced reactors will provide enhanced margins to safety and/or utilize simplified, inherent, passive, or other innovative means to accomplish their safety function. According to the Advanced Reactor Policy Statement, advanced reactor designers are encouraged as part of their design submittals to propose specific review criteria or novel regulatory approaches that the NRC might apply to their designs. The licensing approach and the PRA proposed for the NGNP COLA are specifically designed to meet the objectives set forth in these cornerstones of the NRC policies guiding the licensing of advanced reactors. Risk insights from the PRA are expected to be useful in demonstrating conformance to the safety goals and in demonstrating that increased reliance on inherent and passive means to accomplish safety functions in the NGNP design is acceptable.

2.1.3 NRC Guidance

A number of NRC guidance documents apply to PRAs and the use of PRAs in risk-informed decision making. The HTGR PRA will conform to applicable sections of these documents and identify those sections that do not apply, with justifications and proposed alternatives. This section identifies the key references considered to be applicable or partially applicable. The following paragraphs separately discuss each of the more important guidance documents.

2.1.3.1 Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants" (LWR Edition)

Regulatory Guide 1.206[16] provides guidance for meeting the requirements discussed in the previous sections in 10 CFR Part 52 that calls for a PRA to be submitted in an application for a combined license. In this guide it is stated:

> *The COL applicant should provide in Chapter 19 of the FSAR an adequate level of documentation to enable the NRC staff to determine the acceptability of the risks to public health and safety associated with operation of a proposed new plant. The acceptability of the risks to public health and safety is determined from the interpretation of the results and insights of the applicant's (1)plant-specific PRA[a] and (2) severe accident evaluations.*
>
> *The applicant's PRA and severe accident evaluation are used as follows:*
>
> A. *During the design phase:*
>
>   i. *Identify and address potential design features and plant operational vulnerabilities, where a small number of failures could lead to core damage, containment failure, or large releases (e.g., assumed individual or common-cause failures could drive plant risk to unacceptable levels with respect to the Commission's goals, as presented below).*
>
>   ii. *Reduce or eliminate the significant risk contributors of existing operating plants[b] that are applicable to the new design by introducing appropriate features and requirements.*
>
>   iii. *Select among alternative features, operational strategies, and design options.*
>
> B. *Identify risk-informed safety insights based on systematic evaluations of the risk associated with the design, construction, and operation of the plant such that the applicant can identify and describe the following:*
>
>   i. *The design's robustness, levels of defense-in-depth, and tolerance of severe accidents initiated by either internal or external events.*
>
>   ii. *The risk significance of specific human errors associated with the design, including a characterization of the significant human errors that may be used as an input to operator training programs and procedure refinement.*
>
> C. *Demonstrate how the risk associated with the design compares against the Commission's goals of less than 1×10^{-4}/year for core damage frequency and less than 1×10^{-6}/year for large release frequency. In addition, compare the design against the Commission's approved use of a containment performance goal, which includes (1) a deterministic goal that containment integrity be maintained for approximately 24 hours following the onset of core damage for the more likely severe accident challenges and (2) a probabilistic goal that the conditional containment*

a. References in this guide to the plant-specific PRA includes both PRA techniques and alternative approaches for addressing contributors to risk, per the Commission direction provided in the SRM, dated July 21, 1993, for SECY-93-087.

b. The reference to existing operating plants applies to LWR plant technology contemporary with the issuance of the Commission's Severe Reactor Accident Policy Statement on August 8, 1985.

failure probability be less than approximately 0.1 for the composite of all core damage sequences assessed in the PRA.

D. Assess the balance of preventive and mitigative features of the design, including consistency with the Commission's guidance in SECY-93-087 and the associated SRM.

E. Demonstrate whether the plant design, including the impact of site-specific characteristics, represents a reduction in risk compared to existing operating plants.

F. Demonstrate that the design addresses known issues related to the reliability of core and containment heat removal systems at some operating plants (i.e., the additional TMI-related requirements in 10 CFR 50.34(f)).

The results and insights of the PRA are used to support other programs as follows:

A. Support the process used to demonstrate whether the RTNSS is sufficient and, if appropriate, identify the SSCs included in RTNSS.

B. Support, as a minimum, regulatory oversight processes, e.g., the Mitigating Systems Performance Index (MSPI) and the significance determination process (SDP), and programs that are associated with plant operations, e.g., TS, reliability assurance, human factors, and Maintenance Rule (10 CFR 50.65) implementation.

C. Identify and support the development of specifications and performance objectives for the plant design, construction, inspection, and operation, such as ITAAC; the RAP; TS; and COL action items and interface requirements.

These uses of the PRA and severe accident evaluation and the uses of the PRA results and insights are drawn from 10 CFR Part 52, the Commission's Severe Reactor Accident Policy Statement regarding future designs and existing plants, the Commission's Safety Goals Policy Statement, the Commission-approved positions concerning severe accidents contained in SECY-93-087, and NRC interest in the use of PRA to help improve future reactor designs.

All uses of the PRA and severe accident evaluation should reflect the potential limitations of the PRA, as indicated by the results of sensitivity and uncertainty analyses.

Chapter 19.1 of the Standard Review Plan for LWRs provides criteria for NRC staff reviews of the PRA aspects of the COLA.[17]

The HTGR PRA that will be included with the NGNP COLA will address the expectations set in Regulatory Guide 1.206 and Chapter 19.1 of the Standard Review Plan (SRP) with the following clarifications.

- The scope of the HTGR PRA is not limited to the treatment of severe accidents but includes a spectrum of event sequences within and beyond the design basis.
- The PRA applications listed in Regulatory Guide 1.206 are based on the risk-informed applications established for existing and advanced LWR designs. A broader set of applications is envisioned for the NGNP, including input to the selection of LBEs, safety classification of SSCs, and a risk-informed evaluation of defense-in-depth.

- The risk metrics referred to in Regulatory Guide 1.206, such as CDF and large early release frequency (LERF), are not applicable to HTGR designs being considered for the NGNP since those risk metrics are tied to LWR specific definitions of core damage. Hence, the listed PRA applications will have to be reformulated in terms of HTGR specific risk metrics, e.g., frequency of HTGR-specific LBEs and release categories. The risk metrics for the NGNP will be selected in a manner that the margins to the NRC Safety Goal QHOs can be clearly defined and demonstrated.
- The format and content of the PRA aspects of the COLA may have to be modified to reflect the differences in how the PRA interfaces with other chapters of the submittal. No specific changes are identified in this paper; however, such changes may be defined later during the preapplication period and included in a future writer's guide for development of the COLA.

2.1.3.2 Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-specific Changes to the Licensing Basis"

Regulatory Guide 1.174[18] establishes an integrated process for determining the acceptability of changes to design of existing LWR plants using criteria for CDF and LERF to establish that proposed changes have an acceptably small risk impact. RG 1.174 also provides guidance for using PRA in the licensing of the NGNP with the exception of using CDF and LERF, which are not appropriate as risk metrics for the HTGR. Reactor specific risk metrics that relate to NGNP design-specific event sequences and end states (described in Section 3 of this paper) will be used to provide risk management functions similar to those specified for these LWR-specific risk metrics in this guide.

RG 1.174 also addresses the need for considering defense-in-depth. It offers several criteria for ensuring that defense-in-depth is maintained in risk-informed decision making, including those to ensure:

- *A balance between accident prevention and mitigation,*
- *No over-reliance on programmatic activities to compensate for weaknesses in plant design,*
- *System redundancy, independence, and diversity are employed,*
- *Potential common cause failures are minimized through the use of passive, and diverse active systems to support key safety functions,*
- *Barriers to radionuclide release are independent, and*
- *The potential for human errors is minimized.*

As discussed more fully in the white paper on defense-in-depth,[3] these topics will be addressed by evaluating the roles of SSCs in the prevention and mitigation of accidents and by thoroughly evaluating the impacts of uncertainties on the HTGR PRA results and the design decisions derived from these results. Deterministic elements of the defense-in-depth approach, including the safety classification of SSCs and the performance of conservative safety analysis of DBAs, will be applied with a view toward addressing these defense-in-depth criteria.

Section 2.2.3 of this Regulatory Guide provides general information on the quality of PRAs. It states:

> *The quality of a PRA analysis used to support an application is measured in terms of its appropriateness with respect to scope, level of detail, and technical acceptability. The scope, level of detail, and technical acceptability of the PRA are to be commensurate with the application for which it is intended and the role the PRA results play in the integrated decision process. The more emphasis that is put on the risk insights and on PRA results in the decision making process, the more requirements that have to be placed on the PRA, in terms of both scope and how well the risk and the change in risk is assessed.*

In addition, Section 2 of Regulatory Guide 1.174 includes the following general principles related to PRAs:

> *The plant-specific PRA supporting the licensee's proposals has been subjected to quality assurance methods and quality control methods.*
>
> *Appropriate consideration of uncertainty is given in analyses and interpretation of findings, including using a program of monitoring, feedback, and corrective action to address significant uncertainties.*
>
> *The use of core damage frequency (CDF) and large early-release frequency (LERF) as bases for PRA acceptance guidelines is an acceptable approach. Use of the Commission's Safety Goal quantitative health objectives (QHOs) in lieu of LERF is acceptable in principle, and licensees may propose their use. However, in practice, implementing such an approach would require an extension to a Level 3 PRA, in which case the methods and assumptions used in the Level 3 analysis, and associated uncertainties, would require additional attention.*

Section 2.2.5 of Regulatory Guide 1.174 states that the impact of three classes of uncertainty on the results of PRAs should be addressed: parameter uncertainty, model uncertainty, and completeness uncertainty. Finally, Section 2.5 of the Regulatory Guide states that the following quality assurance requirements from Appendix B to 10 CFR Part 50 should be met to ensure that the PRA is sufficient to be used for regulatory decisions:

- *Use personnel qualified for the analysis.*
- *Use procedures that ensure control of documentation, including revisions, and provide for independent review, verification, or checking of calculations and information used in the analyses (an independent peer review or certification program can be used as an important element in this process).*
- *Provide documentation and maintain records.*
- *Use procedures that ensure appropriate attention and corrective actions are taken if assumptions, analyses, or information used in previous decision making are changed or determined to be in error.*

Consistent with Regulatory Guide 1.174, SRP-19.1[17] provides guidance to the NRC on how to review a licensee's PRA findings and risk insights to support changes in an individual plant's licensing basis. The guidance in SRP-19.1 parallels the guidance in RG-1.174. The NGNP COLA will use these criteria to establish the technical adequacy of the PRA.

2.1.3.3 Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-informed Activities"

Regulatory Guide 1.200[19] describes one acceptable approach for determining that the technical adequacy of a PRA is sufficient to provide confidence in the results such that the PRA results can be used in regulatory decision making. When used in support of a regulatory decision, this Regulatory Guide is intended to obviate the need for an in-depth review of the PRA by NRC reviewers.

Regulatory Guide 1.200 provides guidance in the following four areas:

1. *a definition of a technically acceptable PRA*
2. *the NRC's position on PRA consensus standards and industry PRA peer review program documents*

3. *demonstration that the baseline PRA (in total or specific pieces) used in regulatory applications is of sufficient technical adequacy*
4. *documentation to support a regulatory submittal.*

This Regulatory Guide provides useful guidance for establishing the adequacy of the HTGR PRA for risk-informed decision making. However, this guide and several of its key references, such as the ASME and ANS PRA standards and the Nuclear Energy Institute PRA Peer Review Process, were specifically developed for PRAs on currently licensed LWR plants. Currently, ASME and ANS are working on enhancements to the PRA standards to address PRA applications in the design and preoperational stages as well as a new standard for advanced non-LWR designs. HTGR reactor-specific risk metrics described in Section 3 of this paper will be used in lieu of the LWR-specific metrics CDF and LERF that are used in this Regulatory Guide and the referenced guides and standards. Although most of this guide and the associated standards and peer review approaches apply to the HTGR PRA, there are several areas where this guidance does not address certain quality issues that are important to the HTGR PRA. As discussed more fully in Section 3, there are significant differences in the way in which event sequences are modeled in PRAs for HTGRs and LWRs stemming from differences in the safety design approach. Secondly, this guide and its key references do not address the development of mechanistic source terms or the estimation of radiological consequences for HTGRs.

Finally, a significant number of requirements suggested in this guidance and the supporting standards were developed for PRAs on plants already built that do not apply to design stage or pre-operational plant PRAs that lack operational details that may not be available at the time of the COLA. These requirements include those that address PRA model to plant fidelity issues. As explained more fully in Section 3, the assumptions made in lieu of any unavailable plant knowledge will be clearly documented and taken into account in the treatment of uncertainties and the application of conservative assumptions. Some PRA requirements, such as those that require application of industry- and plant-specific service experience, may not be fully satisfied for certain parts of the PRA until a significant number of reactor years of HTGR operating experience has accumulated. As discussed more fully in Section 3, the HTGR PRA will take this into account in the development of the PRA database and in the treatment of uncertainties in quantification of event sequence frequencies. Through participation on relevant standards committees and working groups, the NGNP project plans to track progress being made by ASME and ANS to develop requirements for design stage and preoperational PRAs, as well as PRA requirements for advanced non-LWR designs that may apply to the HTGR PRA, at least to the extent that HTGR-specific risk metrics are supported.

2.2 NRC Precedents Involving Gas-Cooled Reactors

2.2.1 Exelon Pebble Bed Modular Reactor Preapplication Review

In 2001 to 2002, the NRC staff conducted a preapplication review of the Pebble Bed Modular Reactor (PBMR) at the request of Exelon who proposed to use a PBMR PRA to support licensing decisions.[20] In a letter to Exelon dated March 26, 2002,[21] NRC Staff provided feedback on various technical, safety, and policy issues raised by Exelon during preapplication reviews for the PBMR. With respect to the PRA, the staff stated:

> *The staff supports Exelon's plan to develop a full-scope, detailed PRA including internal events and external events (e.g., fires, earthquakes, floods, high winds) and to follow the fundamental applicable aspects of industry PRA standards (i.e., ASME, ANS). While such a PRA may not fit into the mold of the Level 1-2-3 framework, it can provide equivalent information regarding radiological consequences. However, the staff believes that further development of standards is necessary because the current ASME standard focuses on LERF analysis for Level 2 PRAs and does not address Level 3 PRAs. Although the*

ASME standard provides requirements for treating uncertainties, the lack of operating experience (e.g., initiating event frequencies, component reliability, phenomenology, fuel performance) to factor into the PBMR PRA will lead to relatively large uncertainties in the PRA results.

The staff further stated that:

…the PRA should include accidents involving spent fuel stored on site (analogous to spent fuel pool accidents in LWRs).

The HTGR PRA that will be used to support the NGNP COLA will address these staff comments from the Exelon PBMR preapplication review. The treatment of uncertainties will address the available relevant gas-cooled reactor service experience. The HTGR PRA will also account for sources of radioactive material that are included in the scope of the application, including the spent fuel stored on site and associated fuel handling and storage systems.

2.2.2 NUREG-1338, "NRC Pre-application Review of MHTGR"

The HTGR PRA approach proposed for the NGNP COLA builds upon the approach that was originally proposed for and applied to the Modular High Temperature Gas-cooled Reactor (MHTGR) as part of preapplication review that was initiated by the US Department of Energy (DOE).[22,23] The PRA approach takes into account insights from NRC's review of the MHTGR Preliminary Safety Information Document in NUREG-1338.[12] The scope of the MHTGR effort and associated NRC review included:

- A PRA[23] that included:
  - MHTGR-specific initiating events, event sequences, and end states sufficient for integrated plant risk assessment
  - Event sequences involving releases from single and multiple reactor modules
  - Fault tree models and data to estimate event sequence frequencies
  - Plant transient response analysis for each event sequence
  - Mechanistic source terms for each event sequence involving a release of radioactive material
  - Offsite dose consequences for each MHTGR-specific release category.
- A risk-informed licensing approach based on:
  - Then current LWR requirements and the NRC safety goals
  - LBEs derived from a PRA based on probabilistic and deterministic criteria, including AOOs, DBEs, Emergency Planning Basis Events[c] (EPBEs), and Safety Related Design Conditions (SRDCs)[d]
  - A method for selecting safety-related SSCs based on probabilistic input and deterministic criteria and application of the method to the MHTGR
  - Regulatory design criteria for safety-related SSCs during MHTGR-specific DBEs in the performance of MHTGR-specific safety functions.
- Deterministic safety analyses for all AOOs, DBEs, EPBEs, and SRDCs.

Insights from the NRC review of the MHTGR preapplication submittal provide an important input to the development of the HTGR PRA. Although the MHTGR has some design differences relative to that

---

c. In the LBE selection approach described in the NGNP White Paper,1 which uses a similar method of defining LBE categories, EPBEs are referred to as "Beyond Design Basis Events (BDBEs).

d. Safety Related Design Conditions are referred to in the NGNP LBE White paper as deterministic Design Basis Accidents.

being developed for the NGNP, this is another example of a modular HTGR that shares many of the inherent and passive features of the NGNP safety design approach. Insights from the MHTGR PRA will be used to develop the HTGR PRA, and issues raised in the NRC review will be specifically accounted for in developing the HTGR PRA models.

The MHTGR risk-informed design approach was exercised with a conceptual design and NRC design review, a design-specific PRA and its NRC review, a specific set of LBEs, and independent analyses by NRC and NRC contractors. This PRA and its review are expected to provide useful background to the NRC in the review of the NGNP COLA. Although the DOE submittal and the NRC review were terminated before firm regulatory decisions were finalized, these references provide concrete examples of how PRA was used to support the selection of LBEs for a specific modular HTGR design using an approach that is similar to that proposed for the NGNP COLA. The NRC review report provides useful guidance on potential issues that will likely need to be addressed in the preparation and review of the NGNP COLA.

2.3 Other Documents Relevant to HTGR PRA

A number of draft standards are being developed that are expected to influence the development of the HTGR PRA and the way it is applied to support the design and provide input to the formulation of the licensing basis. The NGNP Project will follow the development of these standards and consider their applicability to the HTGR PRA. These draft standards are summarized as follows:

- ANS 53.1, "Nuclear Safety Design Process for Modular Helium-Cooled Reactor Plants." This draft standard describes a risk-informed and performance-based process for the design of modular HTGRs of the type under consideration for the NGNP and calls for the use of a quality PRA to provide inputs to the design.
- ASME Section XI, Division 2 for Modular HTGRs**.** This draft code is being developed to support the development and application of Reliability and Integrity Management (RIM) programs to assure the reliability of passive metallic components for modular HTGR designs. This draft code is intended to be used rather than Section XI Division 1 which is based on the in-service inspection concept for LWRs. The RIM program concept starts with reliability targets derived from a design-specific PRA for passive components and then applies design, testing, surveillance, and inspection strategies that are necessary and sufficient to achieve the reliability targets. HTGR specific rules are also under development under ASME Section III, Division 5.
- ASME/ANS, "Standard for Probabilistic Risk Assessment for Advanced non-LWR Nuclear Power Plants." This standard is being drafted specifically for advanced non-LWRs and for the type of applications envisioned for the NGNP and follow-on HTGRs.

3. NGNP APPROACH TO PRA

The technical approach to performing the HTGR PRA is described in this section in a way that identifies potential policy and technical issues that need to be addressed and resolved prior to applying for a COLA. This section describes how standard state-of-the-art PRA methods will be applied to the NGNP HTGR, how the HTGR safety design approach will be reflected in the definition and modeling of event sequences, how certain technical issues for performing a PRA on a new reactor with this safety design approach will be addressed, and how the adequacy of the PRA quality for use in support of licensing decisions is established.

When comparing the HTGR PRA to PRAs on currently licensed and operating LWRs, there are many points in common and some significant points of departure. This section identifies both the aspects in common as well as the significant points of departure with a view towards a successful NGNP COLA development and review. It does not describe the PRA methodology and its modeling details but rather provides a high-level summary of the key issues for the PRA in preparation for future discussions with NRC staff.

3.1 Overview of HTGR PRA

The HTGR PRA provides a logical and structured method to guide the design and evaluate the overall safety characteristics of the NGNP design. This is accomplished by systematically enumerating a sufficiently complete set of accident scenarios and assessing the frequencies and consequences of those scenarios individually and in the aggregate to identify challenges to the safety case and quantify the overall risk profile. The PRA is selected as a tool to help identify the LBEs, in part because of its structured process of identifying event sequences and its ability to account for the dependencies and interactions among SSCs, human operators, and the internal and external plant hazards that may perturb the operation of the plant and lead to an accidental release of radioactive material.

Rather than limit the quantification to point estimates of selected risk metrics, the PRA will be structured to give emphasis to the treatment of uncertainties. The quantification of both frequencies and consequences of event sequences and sequence families address uncertainties through the performance of quantitative uncertainty analysis where information is available to perform this function and sensitivity analyses to address other sources of uncertainty that are more difficult to quantify. The treatment of uncertainties for the NGNP design will address the available applicable reactor service experience. The quantification of frequencies and consequences of event sequences and the associated quantification of uncertainties will provide an objective means of comparing the likelihood and consequence of different scenarios and of comparing the assessed level of safety against the applicable requirements. The sources of uncertainty identified in the uncertainty analysis will be given visibility for deterministic treatment in the selection of LBEs and in the development of regulatory design criteria.

The PRA will be structured to be able to examine the risk significance of design features and SSCs in the performance of safety functions as called for in the NRC Advanced Reactor Policy Statement.[14]

3.2 Rationale for Use of PRA

PRA is selected as an analysis tool in order to:

- Comply with NRC regulations, guidance, and standards associated with the performance of PRA for a NGNP COLA.
- Provide a systematic and exhaustive identification and enumeration of plant operating states, hazard groups, initiating events, and event sequences that will provide a basis for the quantification of risk to public health and safety, and serve as an appropriate and acceptable input to the selection of LBEs, SSC safety classification, and risk-informed evaluation of defense-in-depth.

- Provide a systematic examination of dependencies and interactions and the role that SSCs and operator actions play in the development of each event sequence and accident scenario; this examination will have the capability to display the cause and effect relationships between the plant characteristics and the resulting risk levels that are sufficient to support the identification of LBEs and the safety classification of SSCs.
- Provide quantitative estimates of accident frequencies and consequences under a realistic set of assumptions that can be supported by available data, expert opinion, and other scientific evidence.
- Define an appropriate set of HTGR-specific risk metrics from the information provided in the PRA that can be used to demonstrate that the principles of defense-in-depth have been applied and that there is a reasonable consideration of the prevention and mitigation of potential accidents for this type of reactor.
- Address uncertainties through quantification of the impact of identifiable sources of uncertainty on the results and by appropriately structured sensitivity studies to examine the risk significance of key issues. Provide input to the development of requirements that address uncertainties and defense-in-depth considerations.
- Support appropriate and, where required, conservative decision making through the examination of uncertainty distributions.
- Provide a reasonable and acceptable degree of completeness in the enumeration of event sequences and the treatment of appropriate combinations of failure modes, including consideration of the potential for multiple failures necessary to determine risk levels, identify LBEs, and perform safety classification of SSCs.
- Determine the cause and effect relationships between elements of the safety design approach and the risk profile. This includes the risk significance of SSCs and design features in order to support the selection of LBEs and perform safety classification of SSCs.
- Provide insights into the provision of special treatments of SSCs commensurate with their safety significance in any given event sequence.

Key assumptions that are used to develop success criteria, to develop and apply probability and consequence models, and to select elements for incorporation into the models will be clearly documented. Assumptions that are made in lieu of as-built and as-procured characteristics for the NGNP design will also be identified and documented.

3.3 Objectives of HTGR PRA

The objectives of the HTGR PRA are:

- Provide risk insights into the design of the NGNP, including the design of SSCs that perform safety functions.[e]
- Provide an acceptably complete set of event sequences from which to select the LBEs for the COLA.
- Confirm that the applicable requirements, including the safety goal Quantitative Health Objectives (QHOs) for individual and societal risks, are met at the site selected for the COLA.

---

e. The term "safety function" as used in this report is any function by any SSC that is responsible for preventing or mitigating a release of radioactive material from any radioactive material source within the plant. These include design-basis functions and functions included in the PRA model for preventing or mitigating severe accidents, and also would include support functions for other SSCs that perform a safety function. The scope of SSCs to be included in the PRA includes all SSCs that perform a safety function for the radionuclide sources in the scope of the PRA. Since the PRA is performed initially prior to the safety classification of SSCs, we do not yet know which modeled SSCs will be considered "Safety Related." Hence safety functions should not be confused with safety classification.

- Provide input for the development of HTGR-specific regulatory design criteria for the plant.
- Support the determination of safety classification and special treatment requirements of SSCs.
- Support the identification of emergency planning specifications, including the location of the site boundary as well as the goal of appropriately sizing the emergency planning zones.
- Support the development of technical specifications.
- Provide insight on the role of HTGR SSCs in the prevention and mitigation of event sequences as part of the risk-informed evaluation of defense-in-depth.
- Determine the risk significance of design features and SSCs to the extent needed to support LBE selection and safety classification of SSCs.
- Meet applicable codes, guides, and standards that ensure the technical adequacy of the PRA.
- Provide PRA maintenance and update process that supports risk informed decisions at appropriate stages in the design, licensing, commissioning, and operation of the NGNP facility.

NRC agreement on the PRA objectives is an important outcome of this paper.

3.4 Scope of HTGR PRA

The HTGR PRA will provide a primary source of candidate event sequences for the selection of LBEs, be a key input to the safety classification of SSCs, and provide an evaluation of the plant's defense-in-depth. In view of this application, completeness and accuracy in the enumeration of event sequences are viewed as especially important outcomes of the PRA. The emphasis placed on the roles of inherent and passive capabilities in the safety design approach of the HTGR requires a comprehensive set of challenges to the HTGR passive SSCs be included. Such a comprehensive set includes a full spectrum of internal events and external hazards that pose challenges to the inherent and passive capabilities of the plant. When the PRA is initially introduced at an early stage in the design, the PRA scope will be limited to sources within the primary system pressure boundary and reactor core, full power initial conditions, and internal events. As the design matures and design details become available, the scope of the PRA will be broadened to achieve a full scope status prior to plant operation. As such, the scope of the PRA will include treatment of internal and external events and hazards consistent with state-of-the-art of PRA technology to support selection of LBEs for the NGNP design.

The PRA at the time of the NGNP COLA will include the following aspects of a full-scope PRA:

- The potential sources of release of radioactive material, including the sources in the reactor core, primary coolant system pressure boundary, process systems, and fuel handling and storage systems.
- All planned operating and shutdown modes, including plant configurations expected for planned maintenance, tests, and inspections.
- A full range of potential causes of initiating events, including internal plant hardware failures, human operator and staff errors, internal plant hazards such as internal fires and floods, and external plant hazards such as seismic events, transportation accidents, and any nearby industrial facility accidents.
- Event sequences that cover a comprehensive set of combinations of failures and successes of SSCs and operator actions in the performance of HTGR-specific safety functions. These event sequences will be defined in sufficient detail to characterize mechanistic source terms and offsite radiological consequences comparable to an LWR Level 3 PRA as defined by NUREG/CR-2300.[24]
- Quantification of the frequencies and radiological consequences of each of the significant event sequences modeled in the PRA. This quantification includes mean point estimates and an appropriate quantification of uncertainty in the form of uncertainty probability distributions that account for quantifiable sources of parameter and model uncertainty in the accident frequencies, mechanistic

source terms, and offsite radiological consequences. An appropriate set of sensitivity analyses will also be performed to envelope sources of uncertainty that are not quantifiable.

- For HTGR plants covered under COLAs that are comprised of multiple reactor modules, definitions of event sequences that impact reactor modules independently as well as those that impact two or more reactor modules concurrently. The frequencies will be calculated on a per-plant-year basis, and the consequences will consider the number of reactor modules and sources involved in the definition of the mechanistic source terms.
- To support the development of regulatory design criteria, capability of evaluating the cause and effect relationships between design characteristics and risk and supporting a structured evaluation of sensitivities to examine the risk impact of adding and removing selected design capabilities, and setting and adjusting SSC reliability requirements.

The HTGR PRA model will be structured differently than the traditional Level 1-2-3 model for an LWR PRA (as defined in NUREG/CR-2300). While HTGR particle fuel fission product retention performance may start to degrade if subjected to extreme temperatures (e.g., greater than 1,800°C to 2,000°C) for some period of time, the modular HTGR core is specifically designed with physical dimensions, fuel enrichment and loading, and ceramic core materials that prevent temperatures of this magnitude from occurring under beyond design-basis event conditions. Hence, there is nothing comparable to a Level 1 PRA for the NGNP HTGR because credible accident scenarios that involve LWR-defined core damage have not been identified for the HTGR, even for BDBE scenarios with a frequency of occurrence as low as 5×10-7 per reactor year.

Because of the different fuel characteristics and core material properties mentioned above, "core damage" as defined for LWRs and the resulting large early release of radionuclides are not meaningful terms for the modular HTGR. Thus, the HTGR does not have a singular metric such as CDF that is a precursor to the bulk of the high risk event sequences. It is not expected, based on previous HTGR safety analyses, that any NGNP release types would be classified as a "large early release" as the term is used in an LWR PRA context. While the HTGR PRA will not calculate CDF or LERF metrics, it will calculate HTGR-specific plant state frequencies that correspond with the LBEs, as explained more fully elsewhere in this paper.

In supporting the identification of risk insights, it is expected that certain intermediate plant states may be defined that provide the opportunity to define certain intermediate risk metrics. Events involving pressurized or depressurized conduction cooldown are examples of intermediate plant states typically developed in HTGR PRAs. Conduction cooldown events are events wherein the capability for forced circulation core cooling by active systems is lost. In such cases, core heat removal is accomplished via thermal conduction, convection, and radiation heat transfer from the core to the reactor pressure vessel walls, and thermal radiation and convection heat transfer from the reactor pressure vessel walls to the reactor cavity. There are variations of conduction cooldown with the reactor pressurized or depressurized and with successful or unsuccessful operation of the reactor cavity cooling system. Not all conduction cooldown events involve a release of radioactive material to the environment, although some small releases from the fuel into the primary circuit may occur. Some depressurized conduction cooldowns have a radionuclide transport mechanism from the high pressure primary helium; others involve a mixture of the primary helium and water/steam from the steam generator.

Another simplification in the HTGR PRA model structure stems from the relative simplicity of the NGNP design in terms of the number of SSCs and events that need to be modeled. This factor lends itself to defining a continuous event sequence spanning the initiation of events to the release categories for which mechanistic source terms and radiological consequences can be calculated. For organizing the computer model, this continuous event sequence model may be broken up into different stages of event trees to represent the different responses of the plant systems and structures. In this respect, the HTGR PRA model may exhibit some similarities with the classic Level 1-2-3 LWR PRA structure. However, in the end, the elements of the PRA are combined into a single, event sequence model framework that starts with initiating events occurring in different plant operating states and ends in HTGR-specific event families and release categories, including appropriate categories for successful prevention of release. A given release category will contain one or more event families for which frequencies, mechanistic source terms, and offsite consequences are calculated. The integral HTGR PRA encompasses the functions of a full-scope Level 1-2-3 LWR PRA. However, there are some modifications that are expected to justify modification of some of the elements of a full Level-3 PRA. For example, it is expected that radiological consequence analysis will be limited to the performance of exclusion area boundary dose calculations with very simple conservative models to treat the risks of offsite health effects and property damage.

A comparison of the HTGR PRA structure for the NGNP COLA with that of the Level 1-2-3 framework for an LWR is provided in Table 3-1. As seen in this table, there are both similarities and differences in the PRA modeling structures.

Table 3-1. Comparison of HTGR PRA with LWR PRA model structure.

PRA Model Attributes	PRA Outputs	LWR			HTGR
		Level 1	Level 2	Level 3	
Assessment of accident frequencies	Core damage frequency (CDF)	Yes	Yes	Yes	No, however a range of selected risk metrics consider releases from the fuel
	Plant damage state (PDS) frequencies	Not necessary but sometimes included	Yes, all PDSs are variations of LWR core damage state	Yes, all PDSs are variations of LWR core damage state	Yes, NGNP plant states defined as event sequence families for LBEs; some intermediate states may be defined
	Release category frequencies	No	Yes, all involve core damage and are LWR specific	Yes, all involve core damage and are LWR specific	Yes, however, NGNP HTGR-specific release categories are not tied to a core damage state
	Frequencies of site meteorological conditions and emergency planning responses	No	No	Yes	Yes, conservative bounding treatment is expected to meet COLA requirements
Assessment of accident consequences	Source Terms	No	Yes, mechanistic source terms for each LWR release category quantified	Yes, mechanistic source terms for each LWR release category quantified	Yes, mechanistic source terms for each NGNP HTGR release category quantified
	Consequences to the Public		No	Yes, early and latent health effects (QHOs).	Yes, but doses would be assessed at the exclusion area boundary.

The treatment of all operating and shutdown modes for an HTGR will also be simpler than that of current LWRs because of fewer plant configurations that give rise to unique success criteria and event sequence modeling end-states. This is partly because the use of a single phase gas for the reactor coolant and the capability of SSCs for active and passive heat removal and reactivity control to perform their functions during both pressurized and depressurized conditions. For the HTGR, the more limited set of SSCs that need to function for the events involving the potential release of radionuclides in the reactor core and the reactor cooling system helps to reduce the size of the PRA event tree/fault tree models.

The HTGR PRA will also address sources of radioactive material outside the reactor module, such as those within in the fuel handling and storage systems and plant configurations in which the reactor is defueled to perform certain unscheduled maintenance actions. Treatment of low power and shutdown modes are taken into account in the baseline PRA models rather than after the fact.

Future HTGRs are expected to have multiple reactor modules to be located at the same site, with some systems and loads shared between the modules. The PRA will account for the risk of multiple modules. The existence of multiple modules increases the site-wide likelihood of scenarios that impact a single module independently, and creates the potential for scenarios that involve multiple modules as well as the potential for a mechanistic source term involving two or more reactors. These modular reactor considerations will impact the scope and level of detail of the PRA.

Another key difference in the process of building the HTGR PRA models relative to the approach used for existing LWRs is the sequencing of the various stages of PRA model development. In existing LWR PRAs, which were first developed after the plants were already built and in operation, it has been common practice to first construct a detailed PRA model for internal events from full power operation and then to add other plant operating states and hazard groups onto an already completed and detailed PRA model of internal events. In the case of the HTGR PRA, the expansion of scope to consider different plant operating states and different hazard groups needs to be introduced at an earlier stage so that the level of detail in developing the internal events at full power part of the PRA is developed in parallel with the other states and hazard groups. At each stage of PRA development, the level of detail will match the level of detail of design and site information available at the time.

NRC agreement on the necessary scope and structure of PRA development is an important outcome of this paper.

3.5 NGNP HTGR PRA Elements

The HTGR PRA will be organized into elements that are consistent with the way in which PRA elements have been defined in the ASME/ANS PRA Standards,[25,26] and Regulatory Guide 1.200.[19] The NGNP PRA elements, which may be considered building blocks of the PRA models, include:

- Definition of Plant Operating States
- Initiating Events Analysis
- Event Sequence Development
- Success Criteria Development
- Thermal and Fluid Flow Analysis
- Systems Analysis
- Data Analysis
- Human Reliability Analysis
- Internal Flooding Analysis
- Internal Fire Analysis
- Seismic Risk Analysis
- Other External Events Analysis
- Event Sequence Frequency Quantification
- Mechanistic Source Term Analysis
- Radiological Consequence Analysis

- Risk Integration and Interpretation of Results
- Peer Review.

The role these elements play in the development and quantification of the NGNP HTGR event sequence model is illustrated in Figure 3-1. These elements are similar to those associated with a full-scope Level 3 PRA for an existing LWR. Some of the key differences identified are as follows:

- The following design-specific PRA elements are developed specifically for the NGNP HTGR:
    - Safety functions
    - SSC to support each function
    - Success criteria
    - Functional initiating event categories
    - Plant response to initiating events
    - Human actions prior to, in the initiation of, and in response to events modeled in the PRA, including the time frames available for these actions
    - Event sequence end states
    - Mechanistic source terms
    - Radiological consequences.
- The event sequences cover relatively frequent events classified as AOOs, infrequent events classified as DBEs, and rare events classified as BDBEs.
- There are no calculations of CDFs or LERFs, but there are calculations of the frequencies and consequences of accident families referred to as LBEs. Each LBE is a group of event sequences with similar plant operating state, initiating event, plant response to performance and failure to perform safety functions, and end-state. The results for some PRA calculations, such as those to demonstrate the plant performance against the NRC safety goal QHOs, are organized into HTGR-specific release category frequencies. Each release category is a grouping of LBEs with similar end-states.
- Event sequence frequencies are calculated on a per-plant-year basis, where a plant may consist of a number of reactor modules. This facilitates an integrated treatment of risk for the entire plant. The consequences of event sequences may involve source terms from one, multiple, or all reactor modules that comprise the plant. This will facilitate the definition of LBEs for the multi-module design and provide the capability to address the integrated risk of the multi-module plant.

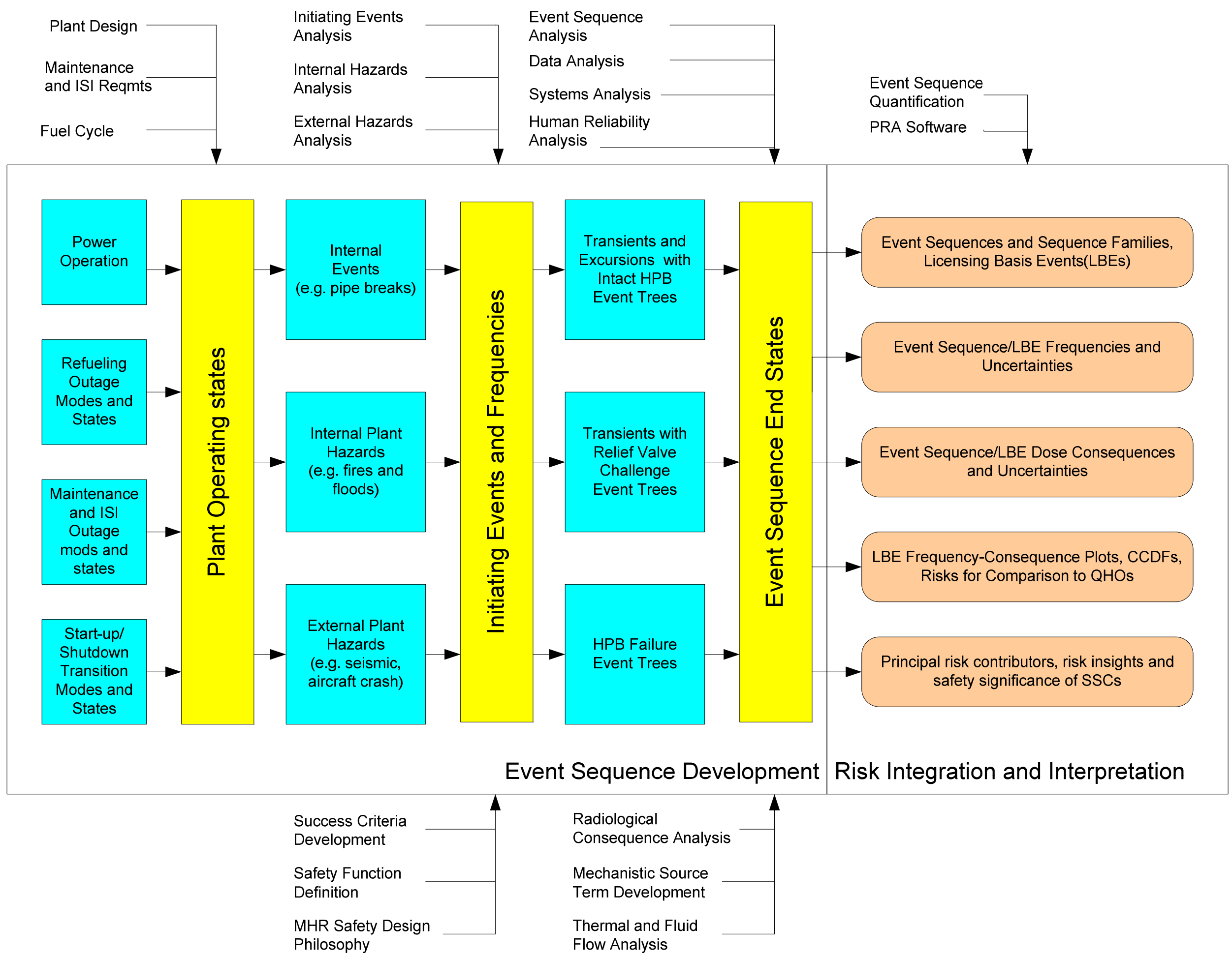


Figure 3-1. Overview of HTGR PRA Model Elements.

- The frequency-dose acceptance criteria, referred to in the LBE Selection white paper1 as TLRC are expressed in terms of exclusion area boundary radiological doses. Because the mechanistic source terms are expected to be very small, the treatment of offsite radiological consequences may be simpler in comparison to that of a typical LWR Level 3 PRA. As demonstrated in prior PRAs,[23,27] mechanistic source terms for HTGRs are far below the dose thresholds necessary to produce early health effects. Information will be presented in the NGNP COLA to show that this is indeed the case with the NGNP design. In addition, the capability to use bounding estimates to demonstrate that the NRC safety goal QHOs have been met without the need for complex health effects and evacuation models will be demonstrated. Hence, complex evacuation and population dose models are generally not required for the PRA, and simplified radiological analyses, e.g., site boundary doses, that do not credit evacuation are expected to be sufficient for this PRA application. Some of the key features of the HTGR PRA modeling process are described in Paragraph 3.6.

3.6 Technical Approach to Modeling HTGR Event Sequences

3.6.1 Systematic Search for Initiating Events

An important element of the HTGR PRA is the systematic approach to the search for initiating events, which begins the process of event sequence modeling. The approach to performing this task is derived from previous HTGR PRAs such as the MHTGR PRA,[23] and it is consistent with the approaches used in contemporary LWR PRAs. The initial conditions for the selection of initiating events for the HTGR PRA cover all operating and shutdown modes expected during the NGNP facility's operating life, including the expected shutdown configurations for conducting maintenance and refueling. A structured process known as the Master Logic Diagram method is used to ensure that an exhaustive enumeration of initiating events appropriate for the NGNP design is accomplished.

As shown in Figure 3-2, the process starts with the identification of the sources of radioactive material, barriers to fission product release, safety functions, and initial plant operating states. There is no a priori assumption to limit the coverage of radionuclide sources to that inside the reactor core as in LWR PRAs.

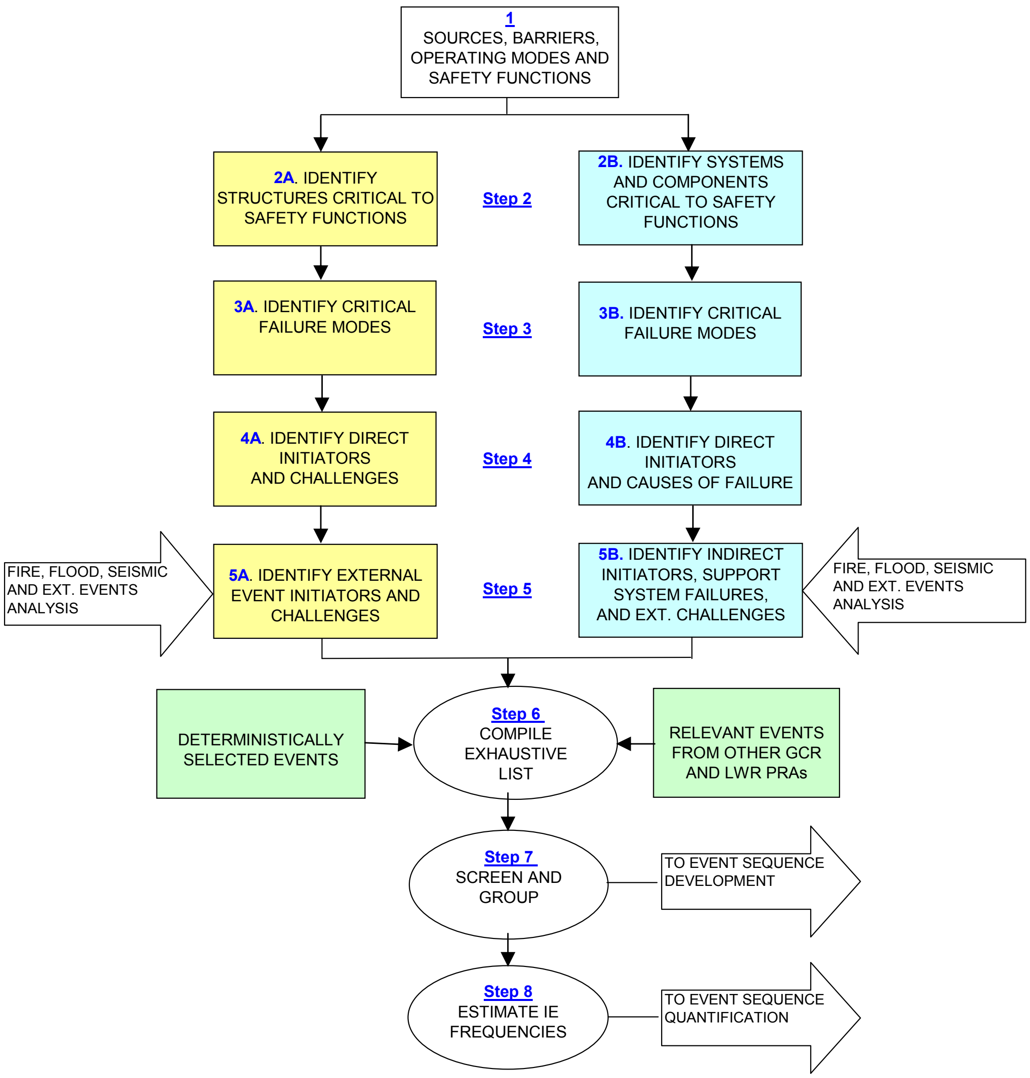


Figure 3-2. Master logic diagram guiding the steps to selection of initiating events.

The following sources of radioactive material are considered for the HTGR:

- Sources within the primary system helium pressure boundary (HPB):
  - Fuel elements in core
  - Intact coated particles
  - Failed or defective coated particles

- Uranium contamination outside coated particles
- Sources imbedded/attached to graphite components
- Dust and plateout on HPB surfaces
- Circulating primary coolant activity.

- Sources outside the HPB:
  - Fuel elements in storage systems
  - Helium purification system (HPS) gas-borne activity
  - Solid and liquid radwaste systems.

The principal barriers to each of these sources are summarized in Table 3-2.

Table 3-2. HTGR radionuclide sources and barriers.

Radioactive Material Source	Barriers to Radionuclide Transport
Fuel elements in the core	Fuel particle kernel, silicon carbide and pyrocarbon coatings of the fuel particle, fuel matrix and fuel element graphite, HPB (primary circuit), reactor building
Fuel elements outside the core	Fuel particle kernel, silicon carbide and pyrocarbon coatings of the fuel particle, fuel matrix and fuel element graphite, fuel handling and storage systems, reactor building
Non-core sources within the HPB	HPB , reactor building
Other sources	Various tanks, piping systems and containers, reactor building or ancillary buildings housing waste management equipment

Once the sources, barriers, and safety functions are defined, the Master Logic Diagram follows a step-by-step process of defining the failure modes of each SSC, the impacts of these modes in challenging the barriers and safety functions, and of identifying direct initiating events, as well as challenges posed by internal and external hazards. Two separate paths are followed through these steps on the diagram shown in Figure 3-2: one from the point of view of each barrier and its set of challenges and the other from the point of view of the SSCs providing safety functions in support of these barriers. The former may be viewed as direct challenges to the integrity of the barriers and the latter as indirect challenges to the barriers.

An initial screening is performed for all SSCs in the plant, including the radionuclide transport barriers. SSCs that play no direct or indirect role in supporting a safety function and whose failure does not impact the safety functions of other SSCs or cause an initiating event are screened out. Failure modes and effects analyses are performed for all unscreened SSCs and transport barriers to identify potential internal initiating events. An analysis of internal and external plant hazards (including those from co-located facilities) is performed to encompass the remaining challenges to the plant safety functions. These processes ensure that events specific to the NGNP design are considered. Insights from reviews of nuclear plant operating experience and previous safety and risk analyses are used to ensure completeness of the exhaustive list of events. In the design and licensing of the NGNP facility, the systematic selection of initiating events is viewed as common to both the probabilistic and deterministic elements of the safety analysis approach. This fact is important to understand the way in which deterministic and probabilistic elements have been integrated into the HTGR design, which is the key advantage of applying PRA technology in the beginning.

3.6.2 HTGR Safety Functions

The HTGR PRA will include a set of reactor-specific safety functions and will define the SSCs available or potentially available to perform these safety functions. This section describes the basis for defining the safety functions to be modeled in the HTGR PRA and selecting the SSCs to be modeled in the performance of these safety functions.

The term "safety function," as used in this report, is any function by any SSC that is responsible for preventing or mitigating a release of radioactive material from any radioactive material source within the plant. These include support functions for SSCs that perform a safety function. The scope of SSCs to be included in the PRA includes all SSCs that perform a safety function for the radionuclide sources in the scope of the PRA. Since the PRA is performed initially, prior to the safety classification of SSCs, it is not yet known which modeled SSCs will perform a required safety function and of those which will be relied on in the Chapter 15 safety analyses.

The exhaustive set of initiating events determined in Step 6 (Figure 3-2) is grouped according to the nature of the challenges to HTGR safety functions. HTGR safety functions have been defined in the context of a top-down logical structure starting with the high-level function of controlling the transport of radionuclides. Such transport is fundamentally controlled in the safety design approach by preserving the integrity of the radionuclide transport barriers identified in Table 3-2.

3.6.3 HTGR SSCs Providing Safety Functions

Both inherent and engineered (other than inherent) safety features and SSCs are included in the design to perform the safety functions. Engineered safety features include both passive and active SSCs. Consistent with good PRA practice, the safety functions modeled in the PRA include those required to meet the required safety functions, as well as SSCs included to meet availability and investment protection needs and serve defense-in-depth roles by preventing and mitigating challenges to barriers and SSC performing the required safety functions. The HTGR safety design philosophy uses inherent safety features and passive SSCs to perform the required safety functions. Active SSCs are also provided for supportive safety functions as well as to meet plant investment protection and availability performance criteria. SSCs that serve both required and supportive safety functions are included in the PRA in order to capture a sufficiently complete set of safety function challenges and associated event sequences and to apply the principle of realistic PRA success criteria. The process of using safety functions to develop the event sequences is fundamentally the same process as used in LWR PRAs. The need to model both safety and nonsafety classified SSCs is also no different; only the functions and SSCs differ. Once the differences in safety functions and the SSCs that provide these functions are understood, the capability to review the PRA event sequence model is available.

The safety functions for the HTGR include:

- Maintain control of radionuclides
- Control heat generation (reactivity)
- Control heat removal
- Control chemical attack
- Maintain core and reactor vessel geometry.

A summary of the inherent features and passive SSCs along with the active SSCs that support or provide defense-in-depth for the safety functions for the HTGR is provided in Table 3-3. The table shows design features representative of those under consideration for the NGNP. This indicates the types and scope of SSCs that would be modeled in the PRA and that will be included in the NGNP COLA.

Table 3-3. Major SSCs modeled in the example HTGR PRA.

Safety Function	Inherent Features and Passive SSCs	Active SSCs[a]
Control of Radionuclides	Fuel barrier: • Fuel particle kernel • Silicon carbide and pyrocarbon coatings of fuel particle • Fuel matrix and fuel element graphite HPB barrier Reactor building barrier: • Retention capabilities of reactor building • Reactor building pressure relief vents	Primary system safety relief valves Reactor building dampers (reclosure) Reactor building heating, ventilation, and air-conditioning (HVAC) filtration system Steam generator isolation and dump system isolation valves
Control of Heat Generation	Strong negative temperature coefficient of reactivity Gravity fall of control rods and reserve shutdown system absorber material	Control and protection systems: • Operational control systems • Investment protection system • Reactor Protection System (RPS) Reactivity control systems: • Trip release of control rod drives • Reserve shutdown system release of absorber material
Control of Heat Removal	Large thermal heat capacity Passive core heat removal Core size, power density, geometry Core, uninsulated reactor vessel, and reactor cavity configuration Passive reactor cavity cooling system (RCCS) Reactor building pressure relief vents	Main loop cooling systems via: • Electric power conversion system • Process steam system Shutdown cooling system (SCS)
Control Chemical Attack	HPB high reliability piping and pressure vessels HPB design minimize penetrations in top of reactor vessel High purity specifications for inert helium coolant Primary system safety valves Reactor building pressure relief vents	Reactor building vent dampers limit air ingress Isolation valves in primary interfacing systems HPS maintains high purity levels of helium coolant Steam generator isolation and dump system
Maintain Core and Reactor Vessel Geometry	Reactor core and structures Reactor pressure vessel and structures Passive RCCS maintains integrity of structures Reactor building structure	None

a. Not shown in this table are support systems such as electric power systems, instrument and service air systems, and some of the man-machine interface systems.

Functional initiating event categories are defined by the nature of the challenge to safety functions. These categories are used to decide which different event sequence models need to be developed. The following list presents representative examples (not considered exhaustive) of functional initiating event categories being considered for the HTGR PRA for the sources of radioactive material inside the reactor vessel and the primary system pressure boundary:

- Plant transients with intact primary system HPB:
  - Main loop and shutdown cooling system (SCS), still capable of forced cooling operation
  - Main loop system failed, SCS still capable of operation
  - SCS failed, main loop system still capable of operation
  - Main loop and SCS not capable of operation.
- Energy conversion system transients with intact HPB and reactivity addition:
  - Control rod or group withdrawal
  - Overcooling transients.
- Primary system HPB leaks and breaks:
  - HPB failures resulting in slow depressurization
  - HPB failures resulting in rapid depressurization.
- HPB heat exchanger failures:
  - Steam generator tube leak
  - Steam generator tube rupture
  - SCS heat exchanger failure.

Each of the above categories represents a unique challenge to the HTGR required and supportive safety functions. These categories are used as a starting point for the development of event sequence models as described in Subsection 3.6.4.

Specific initiating events or causes of initiating events for each of the above categories can be defined having the same functional challenge to the safety functions. For example, one cause of a transient with the Main loop system failed and the SCS still capable of operation (if the onsite diesel generator successfully starts) is a loss of offsite power. An example of a transient with the Main loop and SCS still capable of operation is a Power Turbine Generator trip. Seismic events that do not cause a breach of the HPB are classified as power conversion system transients, while those that do are included in the HPB leaks and breaks category. As part of the PRA submitted to support the NGNP COLA, the comprehensive treatment of initiating events and how they are dispositioned by screening and grouping will be documented according to applicable PRA guides and standards.

3.6.4 Development of Event Sequence Models

Once functional categories of the initiating events are established, event sequence diagrams and event trees are developed to define event sequences resulting from each initiating event and initial condition to be modeled. The event trees will be quantified for each specific initiating event in each functional initiating event category in order to account for significant dependencies between the causes of the initiating event and the modeled SSC failure probabilities. The event tree top events will be derived in consideration of the SSCs provided to support each of the safety functions. The event sequences define the possible successes and failures of each SSC to implement each safety function to a sufficient extent to determine the event sequence end-states.

The treatment of operator actions in the modeling and quantification of event sequences follows the same process as for LWR PRAs. The following are the major differences in human reliability analysis (HRA) treatment in the NGNP COLA PRA:

- Because of the safety design approach of the NGNP, there are few operator actions that must be fulfilled to achieve a safe, stable end-state to an event sequence.
- In general, the time windows available to implement the operator actions in the PRA model are very long. The application of existing HRA techniques that recognize the dependence of the human error rate on the time window may result in human error rates that are too small to be verifiable or appear credible. This is expected to result in a conservative treatment of human error rates in relation to that which would be considered realistic. It should not be viewed as a problem for the HTGR PRA because the PRA results are not that sensitive to the assumed human error rates and most of the important safety functions are fulfilled without need for time critical operator actions. Hence, the use of conservative human error rates is not expected to skew risk insights.
- Since there is less PRA experience in performing HRA in PRAs for reactors such as the HTGR, it is expected that the uncertainties in the human error rates will be larger than found in typical LWR PRAs. For the same reasons cited above regarding the use of conservative human error rates, the assignment of large uncertainties should not be viewed to adversely impact the PRA results or their use in selecting LBEs.
- Because the PRA provides input in the selection of LBEs and the greater reliance on inherent and passive means to fulfill safety functions in the HTGR, there will be increased emphasis on the treatment of human errors of commission in the HTGR PRA.
- At the early design stage versions of the PRA, many of the details of the emergency operating procedures, man-machine interface, and human factors engineering model will be unknown. This will be taken into account in the human error rate uncertainty analysis and will tend to increase the uncertainties. As noted above, this is not expected to cause a problem in terms of masking risk insights or adversely impacting the capability of the PRA to support LBE selection.

Figure 3-3 depicts the event sequence modeling framework for the HTGR. This framework includes the following elements:

- Initiating event in the context of a plant operating state.
- Plant response to initiating event.
- Response of the reactor building and associated SSCs.
- Factors influencing the end-state, including achievement of success criteria and mechanistic source terms.

The causes of the initiating events depicted in Figure 3-3 include internal plant hardware failures, human errors, internal plant hazards such as fires and floods, and external hazards such as seismic events and transportation accidents. The responses of the plant and reactor building functions include the responses of SSCs and the human operators that are involved in the performance of or failure to perform each function. Human responses include favorable or unfavorable acts and errors of omission and commission.

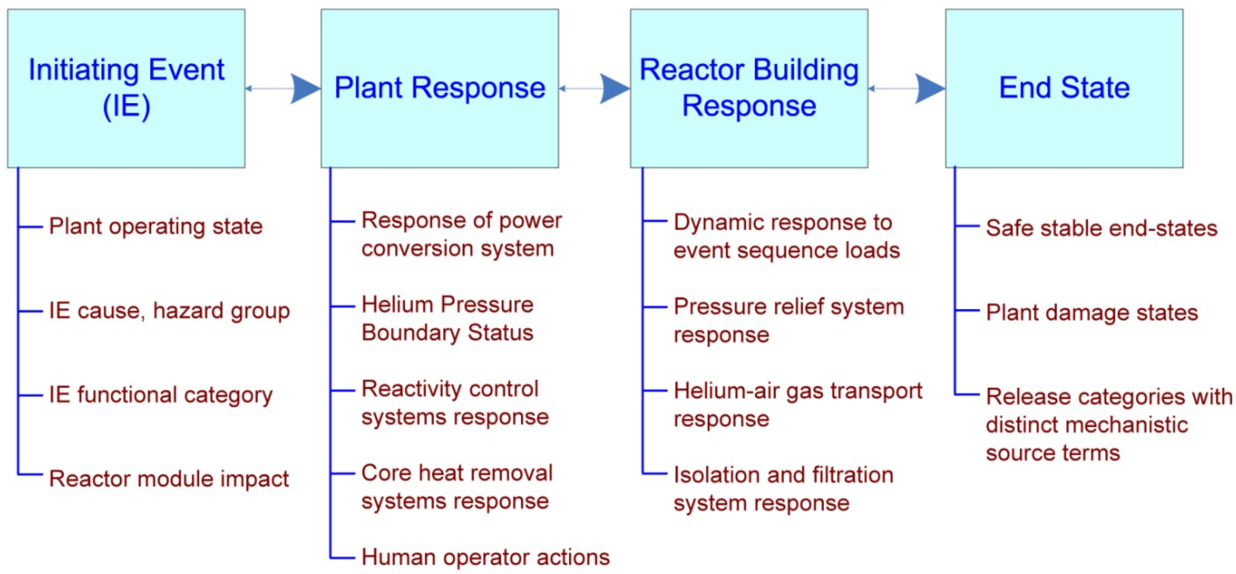


Figure 3-3. Event sequence modeling framework for HTGR PRA.

A further grouping of event sequences will be made in terms of the characteristics of any radionuclide release. Representative NGNP HTGR release categories are listed in Table 3-4. The NGNP HTGR PRA will include variations of these to account for design changes that may be made prior to the COLA, to account for the integrated risk of the multi-module design and other factors that may influence the mechanistic source term. The principle that will be used to make the final definition of release categories will be to define the necessary and sufficient set to capture the risk profile.

Table 3-4. Representative Release Categories for HTGR PRA.

Code	Definition
RC-I	No release with an intact HPB
RC-II	Delayed fuel release with intact HPB
RC-II	Release of circulating activity only
RC-III	Delayed fuel release with primary HTS pump-down
RC-IV	Delayed fuel release without primary HTS pump-down
RC-V	Delayed fuel release with oxidation from air or water ingress and lift-off of plated out radionuclides
RC-VI	Loss of core, reactor vessel, or HPB structural integrity with conditions of RC-V

3.6.5 Event Sequence Families

In selecting LBEs, event sequence families are used to group together two or more event sequences when the sequences have a common initiating event, safety function response and end-state. The process of defining event sequence families applies the following considerations:

- The guiding principle is to aggregate event sequences to the maximum extent possible while preserving the functional impacts of the initiating event, safety function responses, and end-state. The end-state for a multi-module plant includes the number of reactor modules involved in any releases for the event sequence.

- The safety function responses are delineated to a necessary and sufficient degree to identify unique challenges to each SSC that performs a given safety function along the event sequence. Event sequences with similar but not identical safety function responses are not combined when such combination would mask the definition of unique challenges to the SSCs that perform safety functions.
- In many cases for a single module plant, there may be only one event sequence in the family.
- For a multi-module plant, event sequence families are used to combine event sequences that involve individual reactor modules independently into a single family of single reactor module event sequences. In this case, the individual event sequences are associated with a specific reactor module and the family groups them together for the entire multi-module plant.
- Each event tree initiating event and safety function response has a corresponding fault tree that delineates the event causes and SSC failure modes that contribute to the frequencies and probabilities of these events. Hence each event sequence is already a family of event sequences when the information in the fault trees is taken into account.
- The frequency of the LBE defined by the accident family is the linear sum of the individual event sequence frequencies. The frequency units are events per plant-year. This provides a common frequency basis to compare and combine different types of sequences involving different numbers of reactor modules, and different plant operating states.

A common situation that yields event sequence families is when two or more initiating events that belong to the same functional category are quantified through the event trees separately, but follow the same event tree model and end-states. For example, for primary system heat exchanger tube breaks, separate initiating events could be defined for precooler and intercooler tube breaks, but since the event sequences follow the same event tree logic and result in the same end-states, they are aggregated into a family. Alternatively, a heat exchanger tube break initiating event could be defined, in which case the event sequence families already contain the individual event sequences for both precooler and intercooler tube breaks. Another common situation includes the case when event sequence families are used to combine event sequences in a multi-module PRA.

Without the use of event sequence families, the level of detail in the definition of the initiating event categories and decisions to balance the level of detail between the event trees and fault trees may inadvertently impact the classification of an individual event sequence as an AOO, DBE, or BDBE. By aggregating the sequences into the event sequence families, the decisions made in structuring the event sequence model do not impact the LBE classification. A discussion of how event sequence families are used to define LBEs is provided in the LBE Selection paper.

3.7 Example PBMR Event Sequence Model

In order to illustrate the approach to developing event sequences for the HTGR PRA, an example previously presented to the NRC during pre-licensing interactions for the PBMR is used.[28] This example is used because the NRC has access to significant details of this PBMR design whereas the NGNP design is still under development. This example design was developed for the PBMR Demonstration Power Plant in South Africa. The example event sequence model is developed for an assumed main power system (MPS) heat exchanger tube leak event.

This paragraph describes the:

- Approach that is used to develop the event sequence models for the HTGR PRA through the use of an example for one selected functional initiating event category
- PBMR design features relevant to a selected event
- Safety functions and SSCs available to mitigate the consequence of the event

- Elements of the modeling of event sequences specific to this PBMR design.

The PBMR design assumptions and PRA models used to develop these examples are based on an early design of the PBMR and a corresponding PRA model, which is the same as that used to support the Exelon PBMR Pre-licensing activities documented in the Exelon Generation Company Letter.[20] This is done to provide examples with public domain references and to provide consistency with the LBE Selection paper, which uses examples from the same design and PRA. Significant differences will exist in both the design and PRA models associated with the NGNP COLA. The use of these examples does not indicate that the NGNP project will adopt the PBMR design. However, these examples serve the intended purpose of describing how the HTGR safety design philosophy is reflected in the PRA and help to bring out potential issues that can be addressed during the pre-licensing phase. The COLA PRA model is not currently available to provide such examples.

3.7.1 PBMR MPS Heat Exchanger Tube Break Event Sequence Diagram

To illustrate the approach used to model and document the event sequence development for the HTGR PRA, consider the example of the PBMR MPS heat exchanger tube break. The PBMR MPS has two physically identical gas-to-water heat exchangers, referred to as the precooler and intercooler. During normal plant operation at full power, helium flows from the outlet of the recuperator to the inlet of the precooler at 142°C at 2.9 MPa and exits the precooler at 24°C at about the same pressure. The precooler outlet flow enters the low-pressure compressor and then the intercooler at 111°C at 5.1 MPa, and leaves the Intercooler at 23°C at about the same pressure. The water sides of these heat exchangers are cooled by two independent closed water circuits within the active cooling system (ACS). These water circuits are low temperature and low pressure systems and provide cooling water to each heat exchanger at 18°C at <1 MPa. The water leaves the precooler and intercooler at 71°C and 56°C, respectively. There is a minimum of 2.0 MPa pressure drop across the gas-to-water heat exchanger surfaces during all modes of power operation. Hence, if there is a heat exchanger tube break, helium gas will flow into the water system. The capability of the power conversion unit (PCU) as a core heat removal system is lost when this occurs, as the ACS is the only heat removal pathway for the PCU.

As illustrated in Figure 3-4, the ACS is equipped with control valves and rupture discs to prevent water-side overpressure and minimize subsequent water ingress in the event of a heat exchanger break. The rupture discs are set to open at about slightly above 1 MPa. The safety design philosophy to protect the plant investment, maintain plant availability goals, and assure safe plant response is to shut down the plant, provide forced circulation cooling using the core conditioning system (CCS), isolate the MPS from the reactor vessel using the MPS maintenance valves, and continue in this mode until the MPS heat exchanger can be repaired, ACS rupture discs replaced, and the ACS refilled so the plant can be returned to full power operation. The fuel handling system would be shut down and the fuel would remain inside the reactor vessel while these repairs are made. The event sequence diagram for this initiating event is shown in Figure 3-5 and Figure 3-6. This diagram shows the major event sequences for this initiating event and describes some key plant conditions that are important to determine the ultimate end-state.

The first key event in the event sequence diagram (ESD) involves the expected plant shutdown via the operational plant control system (OCS), which would shut down the reactor by a controlled insertion of the control rods. This is backed up by a reactor protection system (RPS) reactor trip of the control rods and operator actions to insert the control rods or the SAS of the reserve shutdown system. There is physically very little difference in plant response, whether the reactor is shut down via the OCS, it automatically trips via the RPS, or if none of the reactivity control systems or operators respond, because the loss of the ACS as a consequence of the initiating event will lead to prompt negative reactivity feedback and the reactor will shut down via inherent and passive means. The ESD tracks the response of the ACS rupture discs. The disks are unlikely to fail but, should they fail, there is somewhat greater potential for water ingress to the MPS and a challenge to the chemical attack safety function.

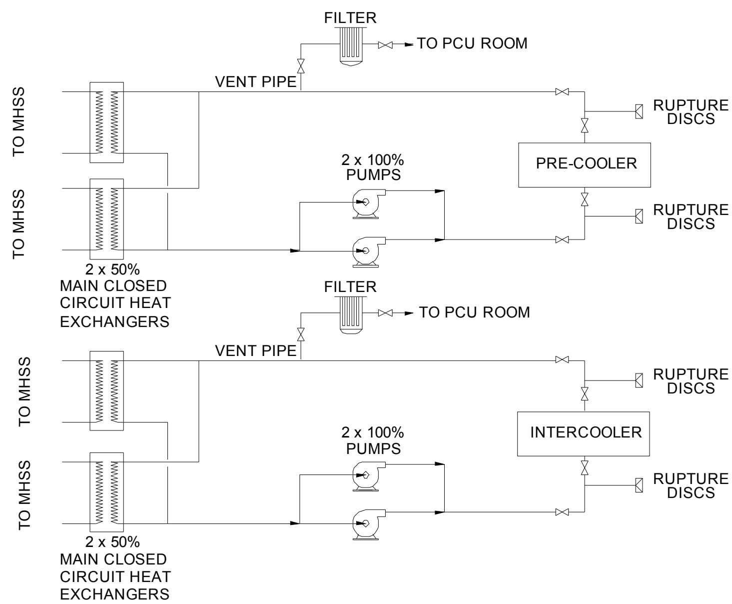


Figure 3-4. Schematic diagram of PBMR active cooling system.

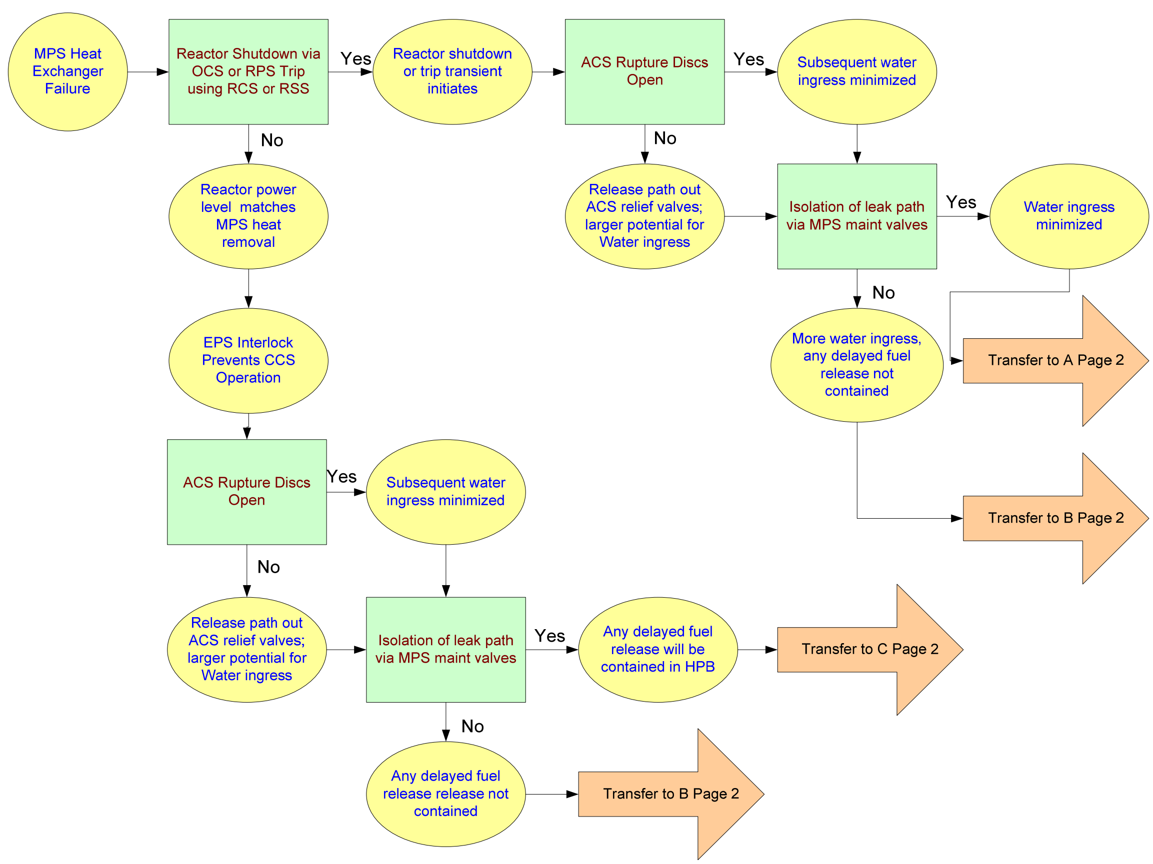


Figure 3-5. Event sequence diagram for MPS heat exchanger leak (Page 1 of 2).

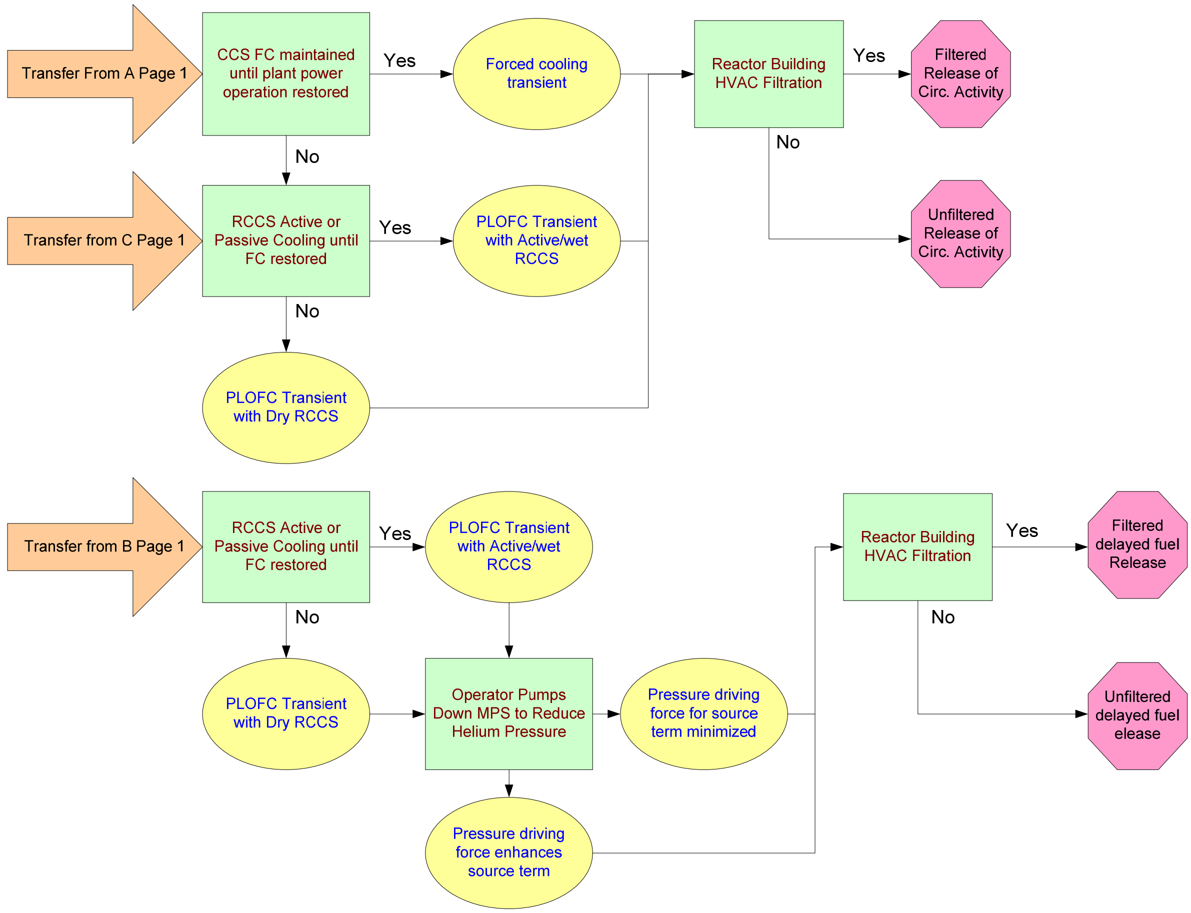


Figure 3-6. Event sequence diagram for MPS heat exchanger tube leak (Page 2 of 2).

The next key event is the action to isolate the MPS leak path. This is normally done using a nonreturn valve that closes from the action of the CCS circulator to prevent bypass flows around the MPS circuit and eventually the closure of the maintenance valves via operator action which could occur when the MPS is sufficiently depressurized. If the isolation is successful, the CCS system can continue to be used to provide forced cooling. Even if it fails to perform this function, any delayed fuel release will be contained within the reactor vessel with the environmental release path limited to leakage past these valves.

The development of mechanistic source terms for each sequence considers the following components of radioactive material inventory that could contribute to a potential source term:

- Circulating helium coolant radioactivity, including elemental and dust-borne activity
- Elemental and dust-borne radioactivity plated out on HPB surfaces
- Radioactivity from uranium contamination outside fuel particles
- Radioactivity in failed and defective fuel particles
- Radioactivity in intact fuel particles.

The delayed fuel release is associated with the slow release of part of the inventory in any failed or uranium contaminated fuel particles in regions of the core that experience an increasing temperature transient several days after the initiating event. This condition is satisfied only for small regions of the core, and only when there is a sustained loss of forced core cooling. As shown in Figure 3-7, peak core temperatures decrease with time for any pressurized or depressurized condition with continued forced circulation cooling via the CCS.

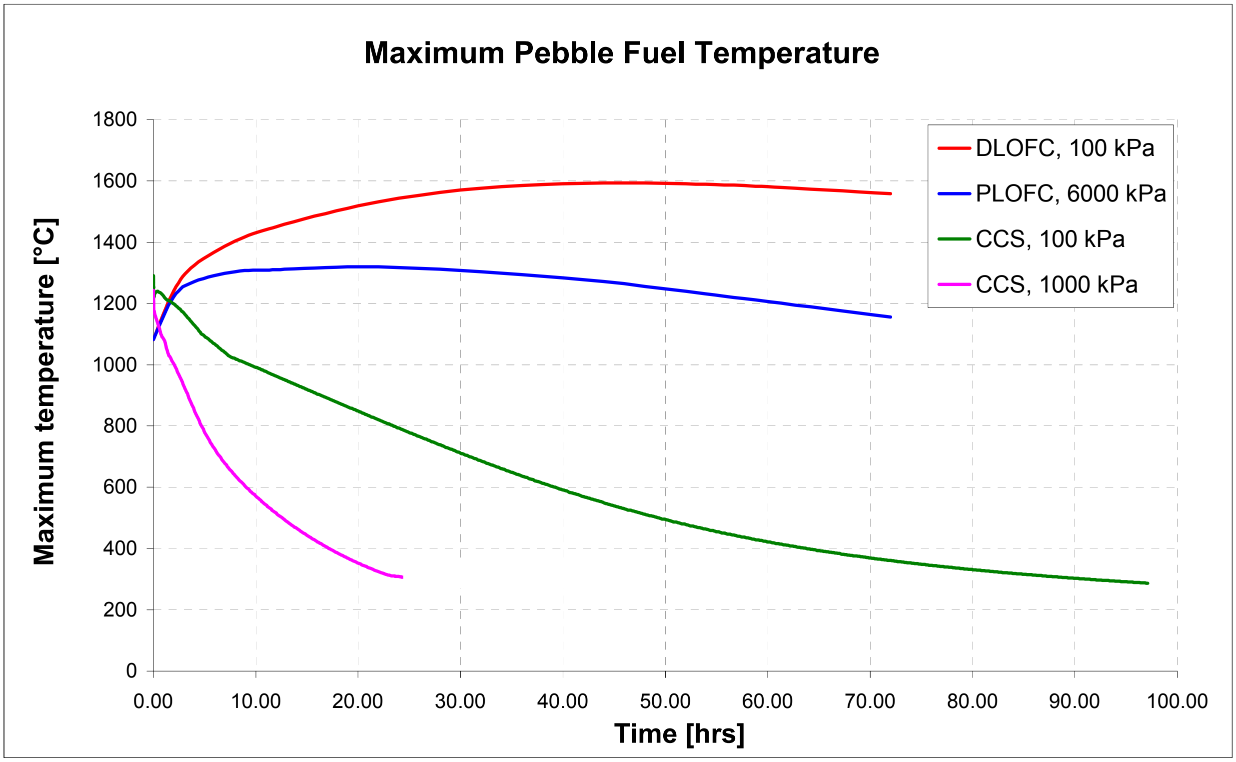


Figure 3-7. Example: Peak core temperatures for selected pressurized and depressurized forced and loss of forced cooling transients.

On sequences where there is no isolation of the MPS leak path, the mitigation strategy is to pump down the MPS helium inventory to reduce the MPS pressure and the pressure drop across the release pathway at the location of the HPB breach. If the pressure drop is reduced, the driving force for a source term involving a delayed fuel release is minimized.

The final issue addressed in the scenario development is the response of the reactor building HVAC system. The system is designed to maintain a negative pressure in the PCU citadel where the MPS release path is located and pass any source term through an HVAC filtration system which would significantly reduce the mechanistic source term for filterable radionuclides such as I-131. The scenarios in the event sequence diagram are organized in an abbreviated format with the note that any source term is dependent on the path followed through the entire diagram so that the condition of the core, the release path, and source term mitigation factors can be properly combined.

The HTGR PRA to be submitted with the NGNP COLA will include these types of ESDs, a deterministic plant transient analysis that describes the physical plant response for all key sequences, and mechanistic source terms for all risk significant sequences. The ESDs will be developed in somewhat greater detail than those presented here merely for illustration purposes.

3.7.2 MPS Heat Exchanger Failure Event Tree Diagram

A simplified event tree diagram for this initiating event is illustrated in Figure 3-8. This diagram shows example initiating event frequencies and event probabilities that illustrate several aspects of how the PRA will be used to provide input to the selection of LBEs. Event sequences with frequencies less than 1×10^{-8} per plant-year are not developed in terms of a quantitative consequence analysis consistent with standard PRA practice. In this diagram, a sequence-specific assessment of end-state conditions and radiological consequence is performed. In this case, this is done qualitatively by indicating key factors that will determine the magnitude of the source term. This event tree is developed for the case of a single reactor module. The event sequence frequencies per plant-year are the same as the frequencies per reactor-year. Those event sequences with frequencies above 1×10^{-2} per plant-year are classified as AOOs, those with frequencies between 1×10^{-4} per plant-year and 1×10^{-2} per plant-year as DBEs, and those with frequencies less than 1×10^{-4} per plant-year as BDBEs. The significance of these event sequence classifications, the basis for the frequency ranges, and how they are used to define LBEs is explained in the LBE Selection paper.[1] This information is provided here to provide traceability between the PRA and the LBE selection process.

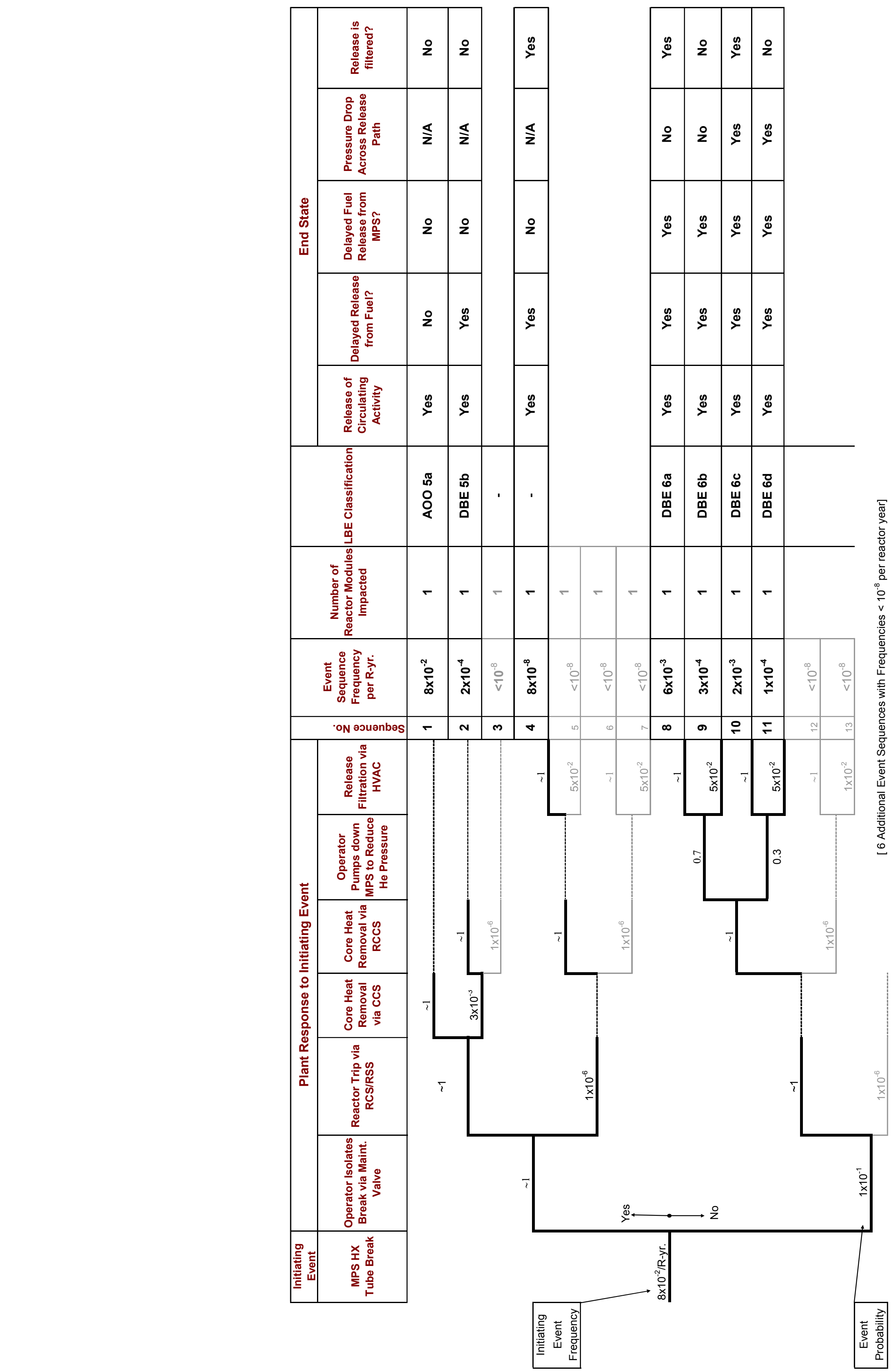


Figure 3-8. Event tree for MPS heat exchanger leak for single reactor module design.

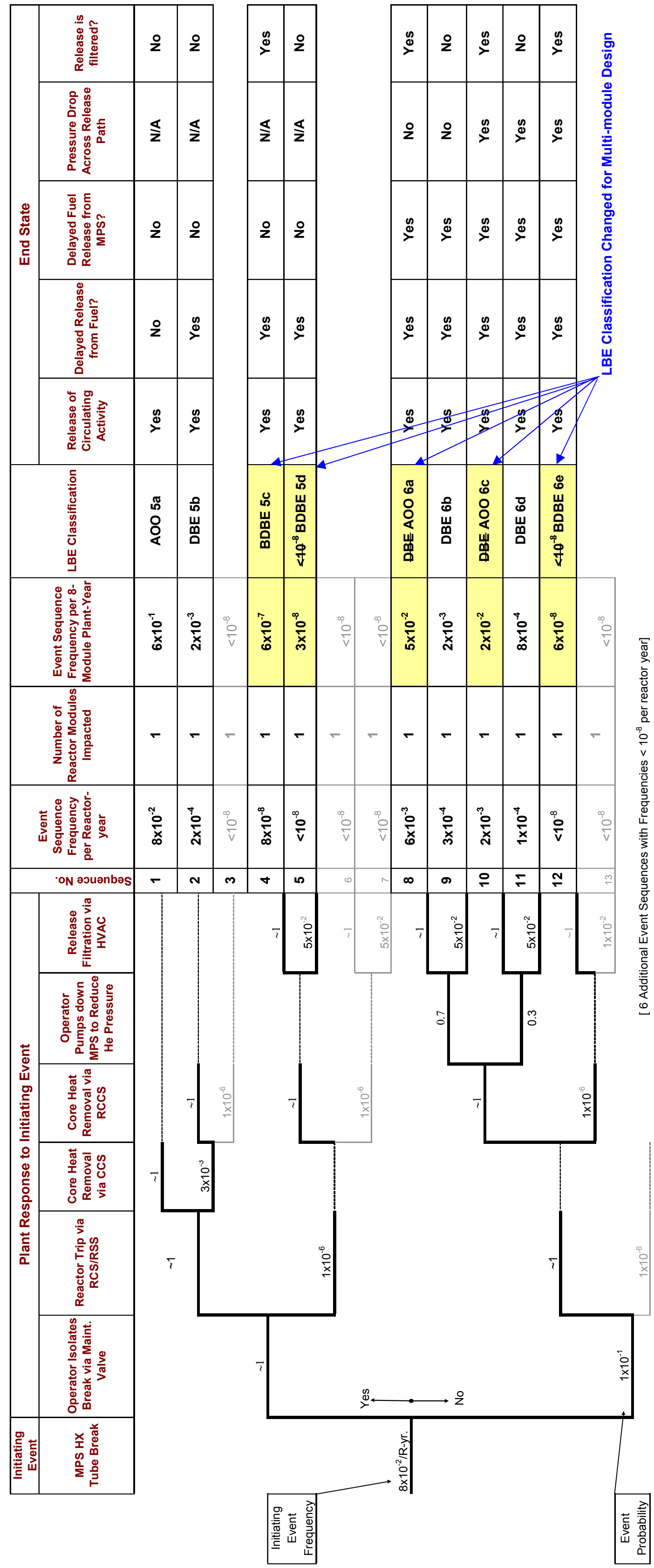


Figure 3-9. Event tree for MPS heat exchanger tube leak for 8-reactor module design.

In the case of an eight-reactor module plant, the event tree development would be performed differently, as shown in Figure 3-9. Initiating events would occur on a single reactor module, because each module has its own MPS heat exchangers and own closed cooling water circuits in the ACS. The total frequencies of each sequence for eight modules would be a factor of eight higher than the former case, as these are reactor module independent events. Hence, some event sequences that are classified as DBEs or BDBEs for a single reactor plant might be classified as AOOs or DBEs, respectively when this factor of eight is taken into account. As this initiating event is reactor module independent, the magnitude of any mechanistic source term would be based on the inventories of a single reactor module. There are also external initiating events, such as seismic events, in which the mechanistic source term could involve events impacting two or more reactor modules. Hence both the frequencies and consequences of the event sequences could be influenced by the number of modules present. By expressing the event sequence frequencies on a per-plant-year basis, an integrated assessment of risk for the multi-module plant will be developed. This example ESD and event tree will of course be repeated for all the events within the scope of the PRA. The rest of the PRA addresses the models and data developed to quantify the event sequence frequencies, mechanistic source terms, and radiological consequences and uncertainties.

3.8 PRA Treatment of Inherent and Passive Safety Features

The PRA will be structured and performed in a manner that reflects the safety design philosophy of the NGNP. This is accomplished in the definition of the HTGR-specific safety functions and SSCs to support those functions as described in the previous sections and the development of success criteria that are derived from the properties of inherent features as well as those of the SSCs involved in the prevention and mitigation of accidents. The HTGR safety design approach places considerable emphasis on the use of inherent characteristics and passive design features to perform safety functions. An outline of these inherent and passive design features and the associated SSC correlated to the safety functions modeled in the PRA as provided in Table 3-3. This approach is reflected in the definition of the scope of the PRA, as well as the way in which the PRA models are defined and analyzed. Some of the key elements of the inherent and passive safety features of HTGRs and how they are treated in the PRA are described in Table 3-5.

Table 3-5. PRA treatment of HTGR inherent and passive features.

HTGR Inherent and Passive Features	PRA Treatment
Fuel particle capabilities during normal and accident conditions	Failed fuel fraction treated probabilistically based on manufacturing, operating, and heat-up test data; failed fuel during burn-up and accident modelled probabilistically as part of fuel failure model in source term analysis; source term uncertainties quantified, including those associated with fuel performance and other transport mechanisms.
Negative temperature coefficient of reactivity	Deterministic accident simulation models will treat this realistically; uncertainties in core reactivity and thermal response addressed as part of mechanistic source term and associated uncertainty analysis.
High thermal heat capacity (low-power density) of core and reflector	Deterministic accident simulation models will treat this realistically; uncertainties in core thermal response addressed as part of mechanistic source term and associated uncertainty analysis.
Passive core cooling capability	Event trees will define success and failure combinations of the core heat removal systems, including the RCCS; seismic events and other external events will be defined that challenge and exceed the RCCS capability; fragilities assessed; potential for blockage of the RCCS cooling flow path because of common cause failure mechanisms to be addressed; uncertainties in passive heat transfer during conduction cool-down events to be assessed as part of the mechanistic source term uncertainty analysis.

HTGR Inherent and Passive Features	PRA Treatment
Core, vessel, and associated support structures	Full seismic and external event analysis will be performed that consider events that challenge or exceed design basis capabilities of all active and passive SSCs modelled in the PRA. Fragilities will be assessed for these hazards.
Coolant pressure boundary integrity and capability to limit air ingress	LWR piping experience and pipe reliability models are applied for expected HTGR applicable pipe damage mechanisms to quantify HPB failure initiating event frequencies; leak before break approaches being factored into the design will be accounted for in these estimates. Event trees will cover a range of HPB failure sizes and failure modes; consequence analysis will include a quantification of the impacts of any air ingress and oxidation reactions as part of the core thermal transient analysis, and will be addressed as part of the mechanistic source term and associated uncertainty analysis.
Reactor building structure including pressure relief features	Event trees will develop a spectrum of sequences that define a range of challenges and responses of blow-out panels. The uncertainty analysis will treat the response of the reactor building pressure relief features probabilistically, if needed.

Addressing inherent characteristics and passive design features is not unique to the HTGR PRA. PRAs on currently licensed LWRs also address both inherent characteristics and passive design features. Examples of passive safety features in LWRs include: the reactor coolant pressure boundary and containment building; natural circulation capability in the reactor coolant system, which eliminates dependence on certain pumps under certain conditions capability of removing heat by boiling off inventories of primary and secondary coolant without pumping fluid; and negative temperature coefficients of reactivity, reactivity feedback from voiding in the coolant, gravity feed capabilities to make up lost coolant inventories under certain conditions, and many other examples of safety functions that rely at least in part on the performance of passive engineered safety systems.

The approach employed for passive SSCs in PRAs for HTGRs is fundamentally the same as for LWRs. The increased reliance on inherent characteristics and passive design features for the HTGR has the following types of impacts on the PRA:

- As is the case with LWR PRA, the HTGR PRA models and supporting assumptions are built on a technically sound foundation of mechanistic models to predict the plant response to initiating events and event sequences and to develop the mechanistic source terms.
- The HTGR uses a full-scope PRA treatment of internal and external hazards, such as internal fires and seismic events, to capture a comprehensive set of challenges to the inherent and passive safety features. Given the reduced reliance on active SSCs to perform safety functions, it is reasonable to expect that safety function failures will be dominated by events and conditions that exceed the design basis envelope for passive SSCs. Extreme external hazards represent one way this can occur.
- It is generally recognized that passive SSCs tend to exhibit lower failure probabilities than active SSCs. Lower failure probabilities also exhibit generally greater uncertainty. This means that while passive SSCs are expected to have significantly lower failure probabilities, there are greater uncertainties in predicting the frequencies of passive SSC failures. Uncertainties in the estimation of both the event sequence frequencies and consequences will be addressed as defined in currently available PRA standards using standard PRA methods. Structured sensitivity analyses will also be applied where appropriate. The results of the uncertainty and sensitivity analysis will be taken into account in the selection of LBEs. The approach to selection of LBEs includes conservative elements to make the selection robust in light of the uncertainties as discussed more fully in the LBE Selection paper.

3.9 Development of a PRA Database for the NGNP

This subsection discusses how the PRA database for the NGNP design will be developed, and how limitations in the available HTGR service experience will be taken into account. The PRA database referred to is for establishing the initiating event frequencies, component failure rates, unavailability terms, common cause parameters, and other parameters within the domain of PRA data. The adequacy of the technical basis for the data is addressed first by analyzing the PRA data requirements in terms of the different types of data parameters and the evidence that is available to quantify the data parameters. It will be used to develop the HTGR PRA database. The second approach to address the adequacy of the data is to review the role that service experience has played in the development of LWR PRA technology over the past three decades to gain insights into how service experience impacts the estimation of rare event frequencies. This review will develop insights into some limitations in the use of service experience in the quantification of PRA data parameters. The review will show that with the exception of relatively high frequency events, even large amounts of service experience, do not eliminate the large uncertainties in the prediction of rare events.

3.9.1 Types of PRA Data Required for the HTGR PRA

The PRA data parameters provided in the HTGR PRA database will include the following data categories (see additional discussion that follows):

1. Failure rates and unavailabilities for active components unique to gas-cooled reactors (GCRs) (e.g. gas blowers, gas-to-gas and gas-to-water heat exchangers, GCR control rod drives, and gas system valves)
2. Failure rates and maintenance terms for active components common to LWRs (e.g., pumps and valves in water systems, water-to-water heat exchangers, diesel generators, breakers, and instrumentation and control components)
3. Common cause failure parameters for a limited set of redundant components, mostly in common cause groups of components common to LWRs
4. Initiating event frequencies for HPB passive component failure modes (e.g., pipes, pressure vessels, weldments, and pressure relief valves)
5. Initiating event frequencies for power conversion system failure modes (turbo compressors, gas-turbine generators)
6. Initiating event frequencies for the same internal and external plant hazards found in full-scope LWR PRAs (fires, floods, seismic events, transportation accidents).

The associated component failure modes for the parameters in the first category above are not normally risk significant because of the reliance on inherent characteristics and passive SSCs to perform safety functions. These data parameters appear in the PRA primarily with respect to initiating event frequencies. The number of unique components in this category is also rather small because of the increased reliance on passive safety systems. Data from GCR experience in the United Kingdom (e.g. control rods, gas blowers, and gas valves) is available to support some of these component failure rates. These parameters will be addressed via engineering judgment and be assigned larger uncertainty bands.

The existing LWR PRA databases and supporting service experience apply directly to applicable Category 2 parameters. Uncertainties may be increased via engineering judgment in cases where the applicability of the LWR data to HTGR conditions is open to question.

Only a few systems employ redundancy for Category 3 parameters. For the most part they are Category 2 components supported by the LWR failure rate and common cause parameter database.

The NGNP design is expected to use piping and pressure vessel components, materials, and design codes common to LWRs for Category 4 parameters. Although there are internal components that are exposed to helium temperatures higher than seen in LWR piping system service data, the external pressure boundary is kept at temperatures within the range of LWR reactor coolant system pressure boundary temperatures during normal plant operating conditions. The impact of HTGR design specific transient conditions on the integrity of the pressure boundary will be addressed as part of the HTGR PRA.

Some pipe damage mechanisms such as welding defects, thermal fatigue, and vibration fatigue apply to modular HTGRs, while others, such as internal corrosion mechanisms, are minimized because of the high purity requirements for the circulating helium, which are necessary to protect the fuel and graphite components from oxidation phenomena. Estimates of failure rates and rupture frequencies for PBMR HPB components have been derived from LWR service experience, taking into account the applicable failure mechanisms.[29] In order to meet the Reliability and Integrity Management program requirements for the metallic pressure boundary components being developed for Division 2 of ASME Section XI for Modular HTGR plants, it will be necessary to perform an engineering evaluation of the NGNP design-specific damage mechanisms and ensure that these are accounted for in setting and meeting reliability targets for metallic pressure boundary components.

As an example, a set of failure rates as a function of rupture severity for welds in carbon steel pipe on the HTGR pressure boundary is presented in Figure 3-10. The service data for this HPB component from BWR main steam system piping was found to be applicable to the design codes and service conditions for the HTGR. In assessing the conditional probabilities of different rupture sizes used in these estimates, use was made of the results of a recent expert elicitation that was performed to update estimates of loss of coolant accident (LOCA) initiating event frequencies for LWRs.[30]

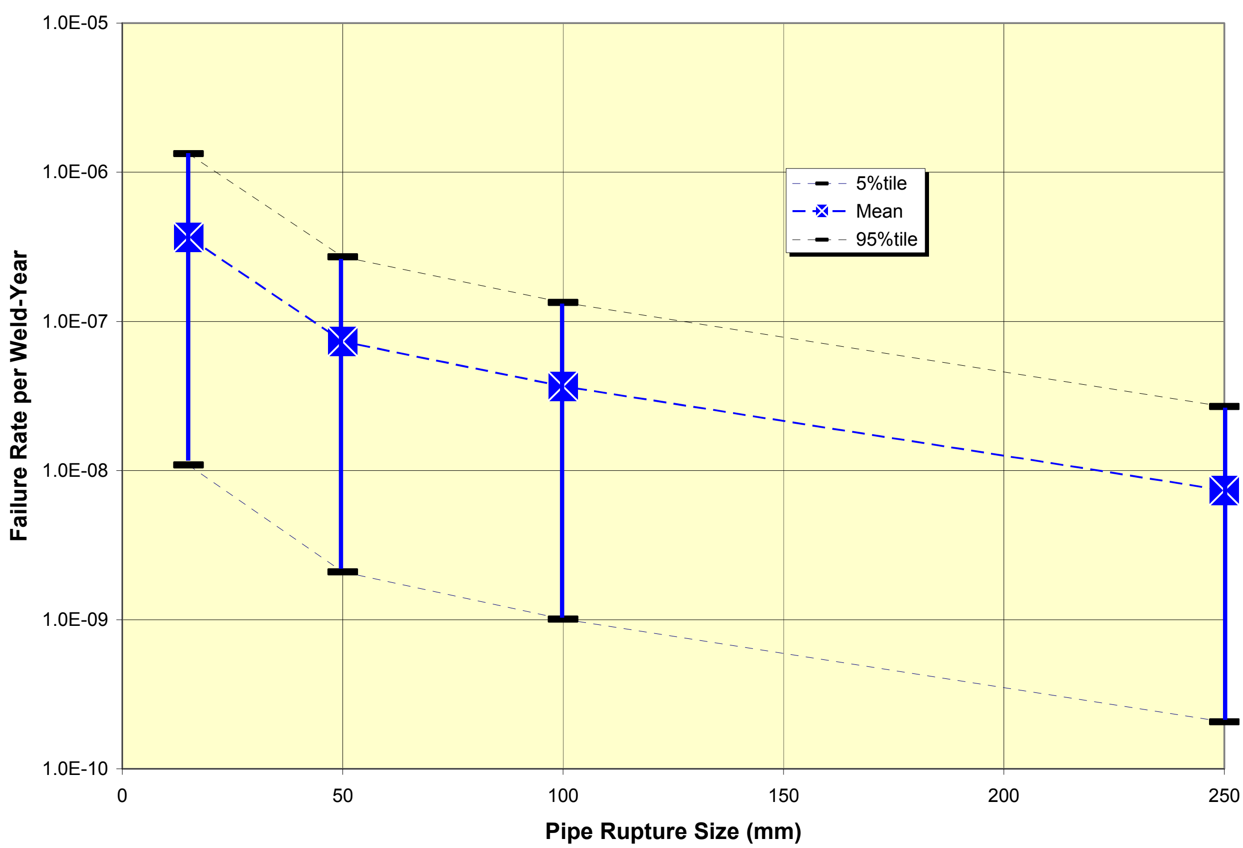


Figure 3-10. Failure rate vs. rupture size for 250 mm carbon steel pipe weld on PBMR HPB.

Although the benefits of using a highly pure and chemically inert coolant in the HTGR are expected to be positive, the initial HTGR PRAs will use piping failure rates and rupture frequencies for the HPB that are not much different than for comparable LWR piping.

There are significant differences in the design of the power conversion systems for Category 5 events among the various modular HTGR designs, as well as differences with standard LWR steam cycle designs. This will be taken into account in the treatment of uncertainty for this category of data parameters. There are some relevant data from fossil-fuelled plants that can be used to support this category. Meanwhile, the combination of expert opinion and conservative assumptions will be relied upon in the quantification of data parameters for this category.

There is no difference between LWRs and HTGRs with respect to initiating event frequencies for Category 6. However, there are significant differences that need to be taken into account when assessing the impacts of fires, floods, and seismic events on the operability of unique HTGR SSCs. These unique impacts are reflected in the treatment of safety functions, success criteria, and deterministic analyses to simulate the plant response as discussed previously.

Service experience with GCRs has proven to be useful in estimating component failure rates for some selected components and events. For many of the component-level data that are needed for the HTGR PRA, existing generic data from LWRs are available and will be used. Engineering judgment will be relied upon for unique HTGR components for which there are little or no service data available to derive failure rates from. In such areas, the PRA will emphasize the quantification of uncertainties in both the accident frequencies and consequences; the limited service data will be reflected in larger uncertainties than cases where there is more data available to support the estimates. In some cases, where the PRA results are insensitive to data assumptions, conservative assumptions may be used in lieu of full uncertainty treatment

3.9.2 Relationship between Uncertainty and Amount of Service Experience

Current PRAs on LWRs are supported by several thousand plant years of operating experience with LWRs to support the estimation of the data parameters that are modeled in an operating LWR PRA. As discussed in Subsection 3.9.1, this service experience applies to many of the HTGR data parameters that need to be quantified. Only one category of data parameters—Category 1—must be quantified without the benefit of this LWR or other substantial service experience. The amount of relevant HTGR and GCR experience that will be available to support the HTGR PRA is comparatively small. Still, it is comparable to the amount of experience that existed with LWRs when the WASH-1400 study[31] was performed in the mid-1970s. It is useful to review the development of the database used in that landmark study since those results and insights are still used today. This review aims to establish the relationship between the amount of service experience and PRA data uncertainties.

The quantification of the event sequence frequencies in WASH-1400 was supported mostly by generic industry data from non-nuclear power plants. The initiating event frequencies for LOCA frequencies, a critical data parameter for an LWR PRA, were based on data collected from gas-pipelines and from non-nuclear fossil fueled steam cycle power plants. Engineering judgment was applied to estimate the improvement in performance in the piping systems to be expected by applying the ASME nuclear codes and special treatments. Despite the lack of a firm statistical basis, these estimates of the LOCA frequencies were used to support LWR PRAs for more than 20 years, during which time most of the current risk informed applications on LWRs were completed. Only recently have improved estimates of LOCA frequencies been developed that have materially benefited from the accumulation of many years of LWR service experience, such as those documented in NUREG-1829.[30] These improved estimates serve to validate WASH-1400 conclusions such as the revelation that large LOCAs are less risk significant than small LOCAs.

Despite the lack of service data in the LOCA frequency estimates, the data was adequate to support the applications of those PRAs and the development of technically sound conclusions. That is, the profound insight from WASH-1400 that small LOCAs are more risk significant than large LOCAs has not been revised through the accumulation of extensive service experience.

The limitations of service experience in supporting estimates of rare event frequencies can be seen with the following example. Most LWR PRAs since WASH-1400 have used an estimate of large break LOCA frequencies on the order of 10^{-4} per reactor-year. Uncertainty in this estimate is typically characterized using a lognormal distribution with a range factor of 10, and the above estimate taken as the mean value of this distribution. By 2005, there were nearly 10,000 reactor operating years of service experience with current generation LWRs worldwide with no observed medium or large break LOCAs, and no small break LOCAs that challenged a full set of LOCA mitigation functions such as emergency core cooling system recirculation switch over.

The results of a Bayesian update of the above generic estimate of large break LOCA frequency is shown in Figure 3-11 as a function of the number of years of accumulated service experience observed without an event. As seen in this figure, the updated estimates do not change appreciably either in terms of the mean value or the uncertainty percentiles until the experience exceeds approximately 1,000 reactor years. This helps to explain why the LOCA frequency estimates originally developed in WASH-1400 have not changed much, in spite of the fact that nearly 10,000 reactor years of LWR service experience has been incorporated into the most recent estimates, which are still highly dependent on expert opinion.

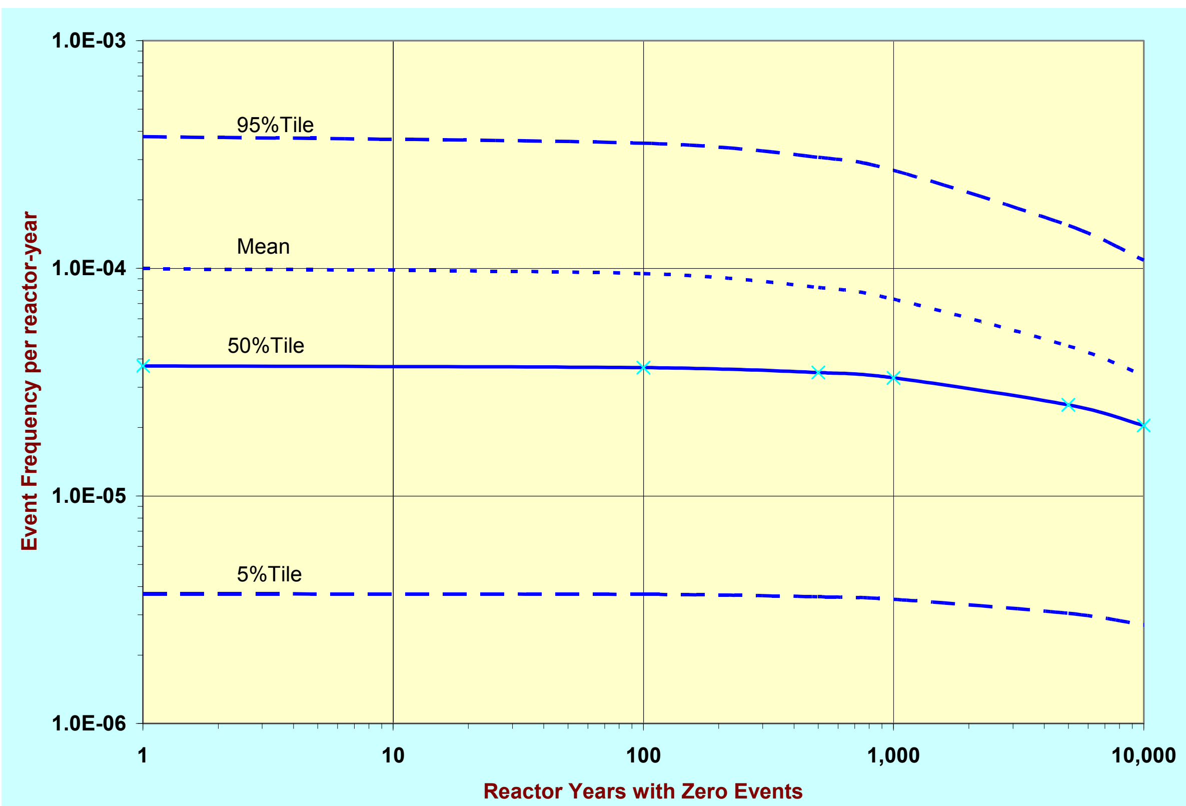


Figure 3-11. Bayesian update of lognormal distribution for large LOCA frequency as a function of amount of operating experience.

When such large amounts of service experience are accumulated, it is often not possible to use it all to try and justify a low failure probability because all the service experience may not be homogenous.

Design changes and changes in operational conditions and inspection practices may lead to a need to exclude much of the service experience for statistical analysis purposes. This tends to limit the capability to aggregate large plant population exposure data sets, even when a large number of reactor years of experience are available. For the HTGR as well as the LWR, the event sequences expected to be risk significant from rare events will exhibit large uncertainties, despite the amount of service experience available. This example makes the point that the accumulation of large amounts of service experience has limited usefulness in reducing the uncertainty in estimating the frequency of the type of rare events that often appear as risk-significant events in PRAs for any type of reactor.

3.10 Key Interfaces with Deterministic Safety Analysis

The HTGR PRA will be developed in conjunction with a technically sound and conservative engineering basis that supports the safety case. The uses of the HTGR PRA results as part of the licensing basis are regarded as examples of a risk-informed as opposed to a risk-based process. As the PRA cannot be separated from the underlying deterministic bases, the interfaces with the deterministic analysis are discussed here. It is important to highlight the role of the PRA in a risk-informed design process that is integrated with a traditional regulatory approach. The role of deterministic-based safety analyses has not been diminished by this use of a PRA, but rather, it has been strengthened as outlined in the following paragraphs.

In the development of the NGNP design, safety analyses will be developed considering both deterministic and probabilitistic processes in an integrated fashion. The safety design philosophy itself is rooted in a deterministic process that aids development of key design parameters (such as the core size and shape, power density, reactor cavity configuration, fuel particle design, and manufacturing specification) that are based on the principle of preventing core damage and large releases from the fuel. Important aspects of the HTGR safety design philosophy, such as the importance placed on inherent and passive means to implement safety functions, will be based on sound conservative design principles. The related design calculations will be based on a combination of analytically and empirically based engineering analysis for a set of enveloping events and boundary conditions, and in accordance with the defense-in-depth philosophy that are anticipated to result in a conservative outcome including appropriate levels of margin for uncertainty.

A systematic selection of initiating events and event sequences will be performed for the PRA. The applicable knowledge available to support the selection of possible initiating events and sequences is derived using both probabilistic and deterministic processes. This knowledge base is systematically developed by applying failure modes and effects analysis, hazard and operability investigations, and by reviews of lists of events considered for other reactor designs. The need for a systematic, comprehensive, and reproducible set of initiating events is viewed to be fundamental to both the probabilistic as well as the traditional approach to the selection of LBEs.

The development of a sequence of events that could occur in the NGNP design in response to an initiating event is fundamentally a deterministic process that is as essential to the task of developing ESDs and event trees for the PRA as it is for listing the sequence of events for Chapter 15 of the FSAR portion of the COLA. Conservative engineering analyses are applied to establish the plant response to initiating events and the event sequences resulting from success/failure combinations of SSCs defined in the event sequence models. Verified and validated models of the physical phenomena must also be applied to determine the success criteria for SSCs along each event sequence and for determining the end-states and mechanistic source terms. The sequences and conditions derived by the traditional approaches for selecting DBAs are imbedded in the PRA as are the sequences and conditions excluded from the traditional DBAs. So the net effect of the PRA approach is that of bringing a more complete enumeration of event sequences into consideration as LBEs. Regardless, plant responses to the event sequences are determined by the application of verified and validated models to predict the plant response to initiating events. The PRA approach to selecting LBEs is regarded as robust because it yields a more complete set of scenarios to consider compared with the traditional prescriptive rules such as the limitation imposed by the single failure criterion.

The PRA also requires the use of verified and validated models of the physical phenomena to determine the criteria for successfully terminating the event sequences and for determining the end-states. Development of mechanistic source terms is also an area where such models play an important role.

One area where the roles of probabilistic and deterministic analyses may be contrasted is in the treatment of uncertainty. Traditional approaches to safety analysis have approached uncertainty with such concepts as safety margins, defense-in-depth, and conservative assumptions in the safety analyses. In PRA, sources of uncertainty are exposed in the context of quantifying the risks of events, including those within and outside the design basis envelope. Uncertainties are not introduced by the PRA or by the safety analysis, but rather are properties of our state of knowledge as to how the plant responds during infrequent events. Judgments concerning uncertainty will be made independent of the safety analysis approach being used. Sources of uncertainty identified in the course of quantifying the risks of the event sequences in the PRA will be identified for proper treatment in the selection of LBEs and the formulation of design criteria for the SSCs that perform required safety functions.

It is expected that sources of uncertainty will be identified in the course of performing the safety analysis for the NGNP design, and that these uncertainties will be addressed by making appropriate judgments to apply safety margins, conservative assumptions, and identifying the need for additional empirical investigation while using interim conservative approaches to support licensing preapplication and application review activities. The use of PRAs provides a uniform framework for assessing uncertainties, applying conservatisms, and evaluating margins, defense-in-depth, and the value of additional mitigating features. The most effective way to identify these sources of uncertainty is to subject the plant to a state-of-the-art PRA supported by technically sound safety analyses. The roles of the deterministic and probabilistic approaches as elements of this risk-informed licensing process for the NGNP facility are more fully explained in the LBE Selection paper.[1]

As is explained in the LBE Selection[1] and SSC Safety Classification[2] papers, once the LBEs are selected based on input from the PRA, the safety classification of SSCs is established. This safety classification is then subjected to a rigorous and conservative safety analysis to demonstrate that the safety classified SSCs are sufficient to ensure that the dose criteria for the DBA are met with sufficient safety margin. This provides a balanced use of deterministic and probabilistic approaches. PRA is not performed in place of deterministic analysis, but rather it provides a risk-informed logic structure for deciding which analyses to perform. The safety analysis is thus integrated with the PRA process. This integration affords the opportunity to incorporate the most risk significant event sequences into the design basis. Additional information on the roles of deterministic and probabilistic elements of the risk-informed design approach for the NGNP HTGR is found in the white paper on defense-in-depth.[3]

3.11 PRA Guidance, Standards and Approach to Technical Adequacy

This section describes the approach to using available guides and standards to assure the technical adequacy of the HTGR PRA. Comparisons to LWR PRAs are made to establish the similarities and differences between the PRAs for these reactor types in order to assist the NRC in planning for the NGNP COLA PRA review.

The applications envisioned for the HTGR PRA require the ultimate resolution of reactor accident consequences in a manner similar to that supported by an LWR Level 3 PRA. However, the means of dividing the LWR PRA into a Level 1-2-3 structure is not applied to the NGNP design for the reasons explained earlier in this paper.

By design, an HTGR has no damage states analogous to the LWR core damage state in which a large fraction of the fission product inventory is released from the fuel as is postulated to occur in more severe core damage events that are modeled in typical LWR PRAs. The HTGR may define intermediate plant states to support risk insights; however these states will be defined in light of the HTGR safety design approach. For example, the frequency of pressurized and depressurized conduction cool-downs are often developed in HTGR PRAs as intermediate metrics.

The HTGR PRA is structured to identify the appropriate damage states for the reactor in a manner that determines the level of risk of events, supports the development of risk insights, and helps define the limiting LBEs appropriate for the NGNP design.

LERF is not a useful risk metric for HTGR PRAs. HTGR PRAs completed to date have yet to define a credible scenario that would release large enough quantities of fission products, nor early enough, to approach the definition of a large early release.

The following aspects of current NRC guidance on PRAs should be modified to support their application to the HTGR PRA:

- The current quality initiatives focus on PRAs that are used to calculate CDF and LERF. However, the core damage end-state has a definition that is specific to LWRs and is not directly applicable to the HTGR, which is subject to fundamentally different types of end-states. By replacing CDF and LERF with the frequencies of HTGR-specific event families, the HTGR can use the vast majority of the technical requirements in the PRA standards in a straightforward manner. HTGR-specific event families will be defined in a manner analogous to accidents for LWRs by specifying appropriate combinations of initiating events and successful and unsuccessful operation of SSCs and operator actions to fulfill plant-specific safety functions.
- As noted previously, it is neither appropriate nor necessary to fit the HTGR PRA into the mold of the Level 1-2-3 framework. Instead, an integrated PRA that develops sequences from initiating events all the way to source terms and offsite radiological consequences will be developed.
- Also, as noted previously, it is not necessary to develop a completely different set of PRA models for full-power versus low-power and shutdown. The HTGR lends itself to an integrated treatment of accident sequences that covers all operating and shutdown modes.
- The initial HTGR application to select LBEs will require quantification of exclusion area boundary dose consequences to be able to apply the LBE selection criteria for frequency and dose. To the extent supported by the anticipated relatively small magnitude source terms, basic models to estimate offsite health effects will be used that allow application of the LBE selection frequency-dose criteria and demonstration that the NRC safety goal QHOs are met.
- The calculation of exclusion area boundary doses is supported by a mechanistic accident progression and source term analysis that includes a quantification of uncertainties. The technical basis for the HTGR mechanistic source terms will be included as part of the NGNP COLA, as explained more fully in the white paper on source terms.[4] There are no available PRA standards for mechanistic source terms, and most of the available guidance for establishing their adequacy is based on LWR-specific source terms and associated phenomena. ANS is developing a Level 2 PRA standard; however its scope is limited to LWRs. Hence the criteria for acceptance of the HTGR mechanistic source terms need to be established, and this is identified as an issue to address during the preapplication phase of NGNP COLA.
- In view of the applications envisioned for the HTGR PRA, a full-scope treatment of internal events and internal and external hazards is anticipated including events both within and beyond the design basis for these hazards. Some generic treatments of internal and external hazards will be necessary for the PRA that is included with the COLA as explained more fully below. The treatment of internal and external hazards will be simplified during early stages of the PRA and the level of detail of the PRA across all hazard groups will be developed in parallel.

- Assumptions made to support the PRA development for the NGNP COLA will be identified and documented. These assumptions will be evaluated and taken into account in the uncertainty and sensitivity analysis. As explained more fully in the LBE Selection paper[1], deterministic approaches will be applied in the selection of LBEs to make the selection of LBEs rather insensitive to the expected differences in PRA results because of differences between the COLA design and site-specific designs.

With these modifications, the applicable and available PRA standards and peer review process will be used as an approach to ensure adequate PRA quality for the NGNP COLA. The NGNP project is supporting the ASME/ANS efforts to develop a technology neutral PRA standard that can be applied to advanced non-LWR designs[34]. Until that standard is approved, available LWR PRA standards will be used. An evaluation of the applicability of the LWR standards to each HTGR PRA element is provided in Table 3-6. Note that the ASME standard proposes three Capability Categories to address PRA requirements for different applications. The process described in Section 3 of the ASME PRA Standard will be followed to determine the appropriate capability level to apply for each requirement. It is expected that Capability Level II will be appropriate for many requirements, but where appropriate, Capability Level I and III requirements will be applied. As part of the PRA documentation, the interpretations of the PRA standards assumed in the PRA development and the assumed PRA capability category and its basis will be documented.

Table 3-6. Comparison of HTGR PRA technical elements and applicable PRA standards.

Technical Elements	Applicable PRA Standards	Comments
1. Definition of Plant Operating States	ANS draft low power and shutdown (LPSD) PRA standard for low-power and shutdown states.[26]	One set of plant operating states will be defined to cover all envisioned plant operating and shutdown states for the primary coolant system radionuclides. Appropriate states will be defined for other sources of radioactivity.
2. Initiating Events Analysis	ASME/ANS PRA Standard[25] and ANS LPSD PRA standard - Initiating Events Analysis	NGNP HTGR and LWR PRAs are essentially equivalent for this element; Initiating events include those caused by both internal and external hazard groups for all modelled plant operating states.
3. Accident Sequence Definition	ASME/ANS PRA Standard and ANS LPSD PRA standard - Accident Sequence Analysis	Event trees will be developed for the response of SSCs in the performance of plant-specific safety functions for each source; core damage and large early release end states would be replaced by HTGR-specific end states that include a full set of release categories.
4. Success Criteria Development	ASME/ANS PRA Standard - Success Criteria and Supporting Engineering Analysis	Success criteria will be specific to HTGR characteristics and end states.
5. Thermal and Fluid Flow Analysis	ASME/ANS PRA Standard - Success Criteria and Supporting Engineering Analysis	The physical and chemical processes that govern core reactivity, fuel temperatures, and all factors influencing radionuclide transport are fundamentally specific to HTGRs and will be addressed using deterministic computer models.
6. Systems Analysis	ASME/ANS PRA Standard - Systems Analysis	HTGR and LWR PRAs are essentially equivalent for this element except that the HTGR has fewer systems to analyse, the safety functions are different, and there is greater reliance on passive design principles.
7. Human Reliability Analysis (HRA)	ASME/ANS PRA Standard - HRA	HTGR and LWR PRAs are essentially equivalent for this element except that there are fewer actions to consider and the scenarios tend to progress slowly.

Technical Elements	Applicable PRA Standards	Comments
8. Data Analysis	ASME/ANS PRA Standard - Data Analysis	HTGR and LWR PRAs are essentially equivalent for this element. As there is less relevant operating experience for some SSCs, the treatment of uncertainty will be an important issue.
9. Internal Flooding Analysis	ASME/ANS PRA Standard - Internal Flooding Analysis	HTGR and LWR PRAs are essentially equivalent for this element except that there are fewer flooding sources and consequences of flooding will be in the context of an HTGR-specific event sequence model.
10. Internal Fires Analysis	ASME/ANS PRA Standard - Internal Fire PRA	HTGR and LWR PRAs are essentially equivalent for this element except that there are fewer cables and the consequences of fires will be assessed in the context of a NGNP design-specific event sequence model.
11. Seismic Analysis	ASME/ANS PRA Standard - Seismic PRA	HTGR and LWR PRAs are essentially equivalent for this element; the consequences of seismic failures will be assessed in the context of an HTGR-specific event sequence model.
12. Other External Events Analysis	ASME/ANS PRA Standard -Other External Events	HTGR and LWR PRAs are essentially equivalent for this element; the consequences of external events will be assessed in the context of an HTGR-specific event sequence model.
13. Event Sequence Quantification	ASME/ANS PRA Standard Quantification	LWR separation of accident sequences into Level 1-2-3 structure is not appropriate for HTGR; scope of accident sequences include doses and risk importance measures to be developed and analysed for each major plant-specific accident category.
14. Mechanistic Source Term Analysis	No corresponding PRA standard	This task is functionally similar to the mechanistic source terms analysis in an LWR Level 2 PRA; mechanistic source term phenomena and barrier design are specific to HTGR safety design approach.
15. Accident Consequence Analysis	ANS Draft Level 3 PRA Standard[32]	This task is similar to the consequence analysis in an LWR PRA (which is not currently covered in LWR PRA standards) except that exclusion area boundary doses are needed.
16. Risk Integration and Interpretation	No corresponding PRA standard	This task is needed to integrate the frequency and consequence information into a frequency-consequence format. Risk importance metrics will be normalized to HTGR-specific accident families and end states.
17. Peer Review	ASME/ANS PRA Standard and ANS LPSD PRA standard Requirements for peer review; Nuclear Energy Institute PRA Peer Review Process[33]	A peer review will performed for each major PRA phase that supports the various stages of the design process; periodic updates during plant operation will be performed as needed to support the design and the COLA.

4. OUTCOME OBJECTIVES

The objective of this paper and follow-up workshops and paper revisions is to obtain NRC agreement on the list of issues for the use of PRA to support NGNP HTGR licensing as well as agreement on the approach to solving these issues. Specifically, NGNP would like the NRC to agree with the following statements, or provide an alternative set of statements that they agree with:

1. The scope of the HTGR PRA outlined in this paper is appropriate for the intended uses of the PRA in the NGNP COLA for the HTGR facility. These uses include input to:

   - Evaluation of design alternatives and incorporation of risk insights into the design
   - Input to the selection of LBEs
   - Input to the safety classification of SSCs
   - Risk-informed evaluation of defense-in-depth.

   NGNP Approach: A full-scope, all modes, and all hazards PRA as described in Section 3.4 will be performed for the NGNP COLA. This is consistent with the requirements of 10 CFR 52. Risk insights derived from such an approach will produce a balanced perspective for selecting LBEs, safety classification of SSCs, and risk-informed evaluation of defense-in-depth. As discussed more fully in Section 2.1.2, these intended uses are generally consistent with those described in Issue 4 of SECY 2003-0047 and are generally consistent with NRC's technology neutral licensing framework initiative.

2. The approaches to initiating event selection, event sequence development, end-state definition, and definition of risk metrics are appropriate.

   NGNP Approach: As explained more fully in Section 3.1, core damage frequency is not an appropriate risk metric because the core damage state as defined for LWRs is precluded by the NGNP HTGR safety design approach. The available definitions of core damage, such as those referred to in the ASME/ANS PRA standards, refer to LWR properties such as liquid levels in the reactor vessel, LWR fuel temperatures in relation to oxidation properties of Zircaloy, and potential for large releases from the fuel, none of which apply to the NGNP HTGR. NGNP HTGR-specific accident families and release categories will be used as a basis to define NGNP HTGR-specific risk metrics that relate directly to the safety design approach of the NGNP HTGR and are expressed in terms of frequency of offsite radiological consequences.

3. The approach to the treatment of inherent characteristics and passive SSCs outlined in this paper is reasonable and consistent with current state-of-the-art PRAs.

   NGNP Approach: As outlined in the event sequence framework in Section 3, the NGNP HTGR PRA is characterized by the systematic identification of NGNP HTGR-specific initiating events, definition and analysis of NGNP HTGR safety functions, delineation of all SSCs that provide either required or supportive safety functions, technically sound engineering analyses, and mechanistic source terms. The approach to the treatment of inherent and passive safety characteristics is summarized in Table 3-6.

4. The approach to the use of deterministic engineering analyses to provide the technical basis for predicting the plant response to initiating events and event sequences, success criteria, and mechanistic source terms yields an appropriate blend of deterministic and probabilistic inputs to support NGNP licensing.

   NGNP Approach: The NGNP HTGR safety design approach is deeply rooted in conservative engineering principles. The NGNP HTGR PRA will be developed on a foundation of technically sound, analytically and empirically-based engineering processes. The areas in which deterministic processes will play a role include the definition of NGNP HTGR safety functions and success criteria, the prediction of the plant response to initiating events, and the development of mechanistic source terms. The deterministic and probabilistic analyses will be done in a coordinated and integrated manner. Once LBEs and safety classifications of SSCs have been established, the licensing approach will include conservative safety analysis of DBAs to demonstrate that the selection of safety-related SSCs is sufficient, and in this respect similar to that found in Chapter 15 of the SAR for current LWRs. This is discussed more fully in Section 3.10.

5. The approach to the development a PRA database outlined in this paper, including the use of applicable data from LWRs, use of expert opinion, and treatment of uncertainty is a reasonable approach for the PRA.

   NGNP Approach: A technically sound database for the PRA will be developed by:

   - Identifying SSCs that are the same or similar to SSCs and events in LWRs
   - Utilizing PRA data developed for these items
   - Identifying other SSCs and events such as the pressure boundary components that are made of the same materials and use the same design codes as LWRs and applying the corresponding service data after considering the applicable failure mechanisms
   - Identifying SSCs and events that are similar to those with applicable HTGR or GCR service experience, and using that information
   - Identifying SSCs and events that are unique to the NGNP HTGR design and carefully applying expert judgement in accordance with PRA standards
   - Assessing uncertainties and including them in the PRA data

   Please refer to Section 3.8 for a more in-depth discussion of this issue.

6. The process for representing uncertainties and the quantification of mechanistic source terms in the PRA (as outlined in a companion paper on Mechanistic Source Terms[4]) is a reasonable approach for the purpose of developing and analyzing the results of the PRA.

   NGNP Approach: The NGNP COLA will include mechanistic source terms and a treatment of uncertainty in the development of these mechanistic source terms as part of the COL. These source terms will account for the reliability of the fuel manufacturing process and for fuel performance during normal plant operation and burn-up, and during transient and accident conditions. Also reflected in the mechanistic source terms are the core reactivity behaviour, diffusion and oxidation phenomena, heat transport phenomena, fluid flow phenomena, and all relevant radionuclide transport phenomena. Uncertainties in the estimation of these source terms will be addressed. Please refer to the Mechanistic Source Terms paper for more details on the approach to source terms.[4]

7. The approach for the PRA treatment of single and multiple reactor accidents is sufficient to support licensing of a basic single HTGR module and for multi-module configurations.

   NGNP Approach: The PRA will be developed in a way that supports both single and multi-module designs; however the PRA to be provided with the COLA will be based on a single reactor design. Event sequences involving single reactor and multiple reactor source terms will be explicitly developed for the multi-module design. Event sequence frequencies will be calculated on a per multi-module plant year basis. The capabilities to support a fully integrated risk assessment will be available pending the outcome of ongoing policy discussions among the NRC commissioners, staff, and ACRS on the integrated risk issue. The example event tree presented in Section 3.7 illustrates certain aspects of this approach.

8. The approach to using available guides and standards for PRA quality and independent peer review is an acceptable approach for determining the adequacy of the PRA for its intended uses outlined above.

   NGNP Approach: An approach to using existing LWR PRA standards and guidance as described in Section 3 and an independent peer review will be used to help ensure the adequacy of the PRA for the use in NGNP COLA. The NGNP project will advise the NRC on how the existing standards were interpreted for application to the NGNP HTGR PRA. Certain requirements in the PRA standards and guidance that require knowledge of the as-operated design details and accumulation of service experience will not be met until after a licensed NGNP HTGR is built and operated. This will be taken into account in the PRA treatment of uncertainties. Specific details on which standards and guides are useful for each PRA element are found in Table 3-6.

9. The PRA approach to treatment of uncertainties is adequate for the intended PRA applications.

   NGNP Approach: The approach used in developing the PRA that will be submitted for the COLA is adequate to support the selection of LBEs for future operating NGNP HTGRs. The PRA itself is based on a deterministic foundation that is expected to be fundamental to future operating plants. The PRA uncertainties may be larger than for an existing operating plant to account for the fact that the plant is not yet operating.

   These uncertainties will be reflected in relatively large error bands in the PRA results. Even given these large error bands, it is expected (based on HTGR experience) that there will be sufficient margins between the PRA results and the frequency-dose criteria that will be used to select the LBEs. The LBE selection process also has deterministic elements to make the final decisions on LBEs rather insensitive to numerical changes in PRA results.

   As a result of the conservative treatment of uncertainties, the use of deterministic elements in the PRA and the LBE selection process, and the expected large margins between the PRA results and the frequency dose criteria for selecting the LBEs, there is confidence that the design and site assumptions will not impact the selection of LBEs. A design review is expected to be required to verify the appropriateness of the LBEs and SSC safety classification during significant updates and upgrades of the PRA. More information on this topic is found in Section 3.

10. The PRA approach used to support the risk-informed evaluation of defense-in-depth in the design, construction, and operation of an HTGR is adequate.

   NGNP Approach: Information from the PRA will be used to identify the roles of each NGNP HTGR SSC responsible for preventing or mitigating each LBE that makes a significant contribution to the risk of a release of radioactive material.[3] Prevention will be analysed in terms of how the reliability characteristics of SSCs contribute to the frequency of initiating events and the probability of failure of SSCs that fail to perform their functions in response to an initiating event. Mitigation will be analysed in terms of the retention fractions of the radionuclide source inventories within each of the barriers to release including the fuel particle, graphite matrix, plate-out surfaces, HPB, and reactor building SSCs. The roles that redundancy, diversity, independence, and safety margins play in managing the risks of event sequences will be examined in this investigation. Deterministic approaches that are taken to address uncertainties will also be identified. This approach to using the information from the PRA to address defense-in-depth is explained more fully in the Defense-in-Depth white paper.[3]

5. REFERENCES

1. Idaho National Laboratory, *Next Generation Nuclear Plant Licensing Basis Event Selection White Paper*, INL/EXT-10-19521, September 2010, [ADAMS Accession No. ML102630246].
2. Idaho National Laboratory, *Next Generation Nuclear Plant Structures, Systems, and Components Safety Classification White Paper*, INL/EXT-10-19505, September 2010, [ADAMS Accession No. ML102660144].
3. Idaho National Laboratory, *Next Generation Nuclear Plant Defense-in-Depth Approach*, INL/EXT-09-17139, December 2009, [ADAMS Accession No. ML093480191].
4. Idaho National Laboratory, *Next Generation Nuclear Plant Mechanistic Source Terms White Paper*, INL/EXT-10-17997, July 2010, [ADAMS Accession No. ML103050268].
5. 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," *Code of Federal Regulations*, Office of the Federal Register, 2007.
6. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," *Code of Federal Regulations*, Office of the Federal Register, 2007.
7. 60 FR 158, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," *Federal Register*, U.S. Nuclear Regulatory Commission, August 16, 1995, pp. 42622–42629.
8. 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," *Code of Federal Regulations*, Office of the Federal Register, 2007.
9. SECY 2003-0047, "Policy Issues Related to Licensing Non-Light Water Reactor Designs," U.S. Nuclear Regulatory Commission, March 28, 2003.
10. SRM 2003-0047, "Staff Requirements Memorandum for SECY 03-0047—Policy Issues Related to Licensing Non-Light Water Reactor Designs," U.S. Nuclear Regulatory Commission, June 26, 2003.
11. Idaho National Laboratory, *Next Generation Nuclear Plant Fuel Performance and Qualification White Paper*, INL/EXT-10-17686, July 2010.
12. NUREG-1338, "Draft Preapplication Safety Evaluation Report for the Modular High Temperature Gas-Cooled Reactor," U.S. Nuclear Regulatory Commission, March 1989.
13. ACRS Letter, Subject: Issues Pertaining to the Advanced Reactor (PRISM, MHTGR, and PIUS) and CANDU 3 Designs and Their Relationship to Current Regulatory Requirements, ACRSR-1509, February 19, 1993.
14. 59 FR 35461, "Regulation of Advanced Nuclear Power Plants; Statement of Policy," *Federal Register*, U.S. Nuclear Regulatory Commission, July 12, 1994
15. 51 FR 149, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," *Federal Register*, U.S. Nuclear Regulatory Commission, August 4, 1986, pp.28044-28049, (51 FR 160, republished with corrections, August 21, 1986, pg. 30028–30023).
16. Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants," *Federal Register*, U.S. Nuclear Regulatory Commission, July 2007.
17. NUREG-0800, Standard Review Plan 19.1, "Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," *Federal Register*, U.S. Nuclear Regulatory Commission, February 2004.
18. Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant Specific Changes to the Current Licensing Basis," *Federal Register*, U.S. Nuclear

Regulatory Commission, Revision 1, November 2002 [Rev.2 was issued May 13, 2011 (76FR28102)].

19. Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-informed Activities," *Federal Register*, U.S. Nuclear Regulatory Commission , Revision 2, March 2009.
20. Exelon Generation Company Letter, Subject: Proposed Licensing Approach for the Pebble Bed Modular Reactor in the United States, January 31, 2002.
21. U.S. Nuclear Regulatory Commission Letter, Subject: "NRC Staff's Preliminary Findings Regarding Exelon Generation's (Exelon's) Proposed Licensing Approach For The Pebble Bed Modular Reactor (PBMR)," March 26, 2002.
22. U.S. Department of Energy, *Preliminary Safety Information Document for the Standard MHTGR*, DOE-HTGR-86-024, September 1988.
23. U.S. Department of Energy, *Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor*, DOE-HTGR-86-011, Revision 5, April 1988.
24. NUREG/CR-2300, "PRA Procedures Guide," *Federal Register*, U.S. Nuclear Regulatory Commission, January 1983.
25. American Society of Mechanical Engineers and American Nuclear Society, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME-RA-Sa-2009.
26. American Nuclear Society, "Low-Power and Shutdown PRA Methodology Standard" Draft 8c, 2010.
27. Fleming, K. N., et al, *HTGR Accident Initiation and Progression Analysis Status Report – Phase II Risk Assessment*, General Atomic Report No. GA-A15000, April 1978.
28. PBMR Letter, Subject: PBMR White Paper: PRA Approach, USDC20060613-1, Pebble Bed Modular Reactor (Proprietary) Ltd., June 13, 2006.
29. Bengt Lydell and Karl Fleming, "PBMR Passive Component Reliability – Helium Pressure Boundary Components," Prepared by Technology Insights for PBMR (Pty) Ltd., PBMR Proprietary Data, Final Report, 2006.
30. NUREG-1829 "Estimating Loss-of-Coolant-Accident (LOCA) Frequencies Through the Elicitation Process," *Federal Register*, U.S. Nuclear Regulatory Commission (Draft for Comment), June 2005.
31. WASH-1400 (NUREG 75/014), "Reactor Safety Study," U.S. Nuclear Regulatory Commission, October 1975.
32. American Nuclear Society, American National Standard—Radiological Accident Offsite Consequence Analysis (Level 3 PRA) to Support Nuclear Installation Applications (Draft 18), October 2010
33. NEI-00-02, "Probabilistic Risk Assessment (PRA) Peer Review Process Guidance," Revision 1, May 2006.
34. American Society of Mechanical Engineers and American Nuclear Society, "Technology Neutral Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants," Draft for Ballot Review, July 2011.