December 9, 2009

CCN 219274

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 2055-0001

NRC Project #0748

SUBJECT: Contract No. DE-AC07-05ID14517 – Next Generation Nuclear Plant Project Licensing White Paper Submittal – Next Generation Nuclear Plant Project Defense-in-Depth Approach - NRC Project #0748

Consistent with the actions identified in "NGNP Licensing Strategy – Report to Congress," dated August 2008, the purpose of this letter is to submit the subject Next Generation Nuclear Plant (NGNP) Project white paper for U.S. Nuclear Regulatory Commission (NRC) review as part of the early licensing phase of the project. The NGNP will be a licensed commercial high temperature gas-cooled reactor (HTGR) plant capable of producing electricity and high temperature process heat for a variety of energy intensive industries.

The NRC licensing process encourages early interactions to identify and resolve policy, regulatory, and key technical issues related to the proposed facility. Conducting effective interactions with the NRC is a critical part of the NGNP licensing strategy because the early resolution of issues can significantly impact the preparation of an acceptable license application, the subsequent application review schedule, and the ultimate deployment of the NGNP. This white paper represents the first in a series of submittals that will address priority licensing topics related to establishing HTGR regulatory requirements using the process outlined in the Report to Congress.

The enclosed document, INL/EXT-09-17139, "*Next Generation Nuclear Plant – Defense-in-Depth Approach,*" provides the definition of defense-in-depth and the approach that will be used to assure that its principles are satisfied for the NGNP Project. Defense-in-depth is a safety philosophy in which multiple lines of defense and conservative design and evaluation methods are applied to assure the safety of the public. The philosophy is also intended to deliver a design that is tolerant to uncertainties in the knowledge of plant behavior, component reliability, or operator performance.

This white paper includes a review of the regulatory foundation for defense-in-depth, a definition of defense-in-depth that is appropriate for advanced reactor designs based on HTGR technology, and an explanation of how this safety philosophy will be achieved during the design and licensing of this technology within the NGNP Project. This foundation forms a portion of the risk-informed and performance-based approach, and is one in a series of white papers planned in this topical area. Additional papers in this series are planned for development and submittal in the near term.

D080
NRO

Following NRC Staff review of this paper, and pending resolution of associated follow-on questions or requests for additional information, the NGNP Project requests that NRC provide feedback and documentation of its review in a format that will facilitate resolution of key design, safety, and licensing issues, and that can be used as a firm basis for the preparation of future HTGR license application(s).

If you have any questions, please contact me at (208) 526-6063 or Jim Kinsey, Director, NGNP Regulatory Affairs at (208) 569-6751.

Sincerely,

Greg Gibbs, Project Director
Next Generation Nuclear Plant Project

MH:CN

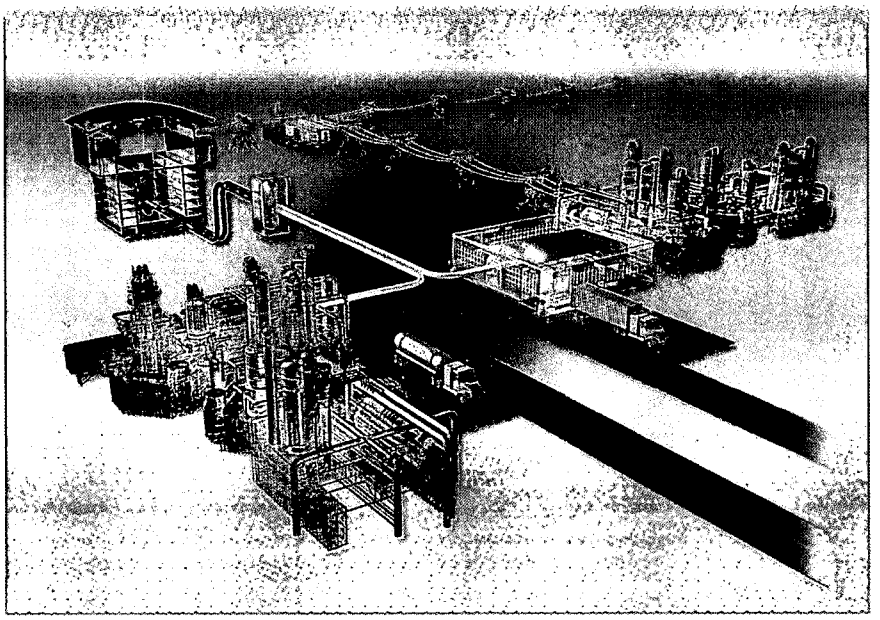
Enclosure as stated

cc:	DOE-HQ	DOE-ID	INL	NRC
	T. L. Cook	C. P. Fineman	J. Alvarez, (w/o Enc.)	J. R. Jolicoeur
	T. J. O'Connor	R. V. Furstenau	A. Clark, (w/o Enc.)	M. E. Mayfield
	R. M Versluis	G. R. McClellan	J. J. Grossenbacher, (w/o Enc.)	W. D. Reckley
	J. L. Zamore		L. A. Sehlke, (w/o Enc.)	J. F. William

INL/EXT-09-17139

Next Generation Nuclear Plant Defense-in-Depth Approach

December 2009



Idaho National Laboratory

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

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.

Next Generation Nuclear Plant Project

Next Generation Nuclear Plant Defense-in-Depth Approach

INL/EXT-09-17139

December 2009

Approved by:

Mark Holbrook
NGNP Licensing

12/9/09
Date

Jim Kinsey
Regulatory Affairs Director

12-9-09
Date

Greg Gibbs
NGNP Project Director

12/9/09
Date

ABSTRACT

This paper (1) documents the definition of defense-in-depth and the approach that will be used to assure that its principles are satisfied for the Next Generation Nuclear Plant Project and (2) identifies the specific questions proposed for discussions with the Nuclear Regulatory Commission. Defense-in-depth is a safety philosophy in which multiple lines of defense and conservative design and evaluation methods are applied to ensure the safety of the public. The philosophy is also intended to deliver a design that is tolerant to uncertainties in knowledge of plant behavior, component reliability, or operator performance that might compromise safety. This paper reviews the regulatory foundation for defense-in-depth, defines defense-in-depth as appropriate for advanced reactor designs based on high temperature gas-cooled reactor technology, and explains how this safety philosophy is achieved in the Next Generation Nuclear Plant design.

PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This paper (1) documents the definition of *defense-in-depth* and the approach that will be used to assure that its principles are satisfied for the Next Generation Nuclear Plant (NGNP) Project and (2) identifies the specific questions proposed for discussions with the Nuclear Regulatory Commission (NRC).

The defense-in-depth paper is the first in a series of white papers that will address risk-informed topics related to licensing the NGNP, such as selection of licensing basis events (LBEs) and classification of structures, systems and components (SSCs). It is necessary to incorporate sufficient defense-in-depth capabilities in the plant design and safety evaluation methodologies to demonstrate that the HTGR design will exhibit a sufficient level of defense-in-depth in the license application. The next generation of advanced designs will have the opportunity to advance defense-in-depth principles by incorporating risk-informed, performance-based design and regulation philosophy early in the design and licensing process.

Defense-in-depth is a safety philosophy in which multiple lines of defense and conservative design and evaluation methods are applied to ensure the safety of the public. The philosophy is also intended to deliver a design that is tolerant to uncertainties in knowledge of plant behavior, component reliability, or operator performance that might compromise safety. This paper includes a review of the regulatory foundation for defense-in-depth, a definition of defense-in-depth that is appropriate for advanced reactor designs based on high temperature gas-cooled reactor (HTGR) technology, and an explanation of how this safety philosophy will be achieved in the NGNP Project.

The specific objectives of this paper are to:

- Summarize the regulatory requirements, guidance, and precedents that apply to defense-in-depth in general, and specifically, to advanced HTGR reactor designs, including the NGNP design
- Develop a definition that addresses the various aspects of defense-in-depth appropriate to non-light water reactors
- Describe a methodology for achieving the various aspects of defense-in-depth, including plant design and operation
- Describe how the defense-in-depth approach identifies the role of special compensatory measures for the unique first-of-a-kind features in the NGNP design
- Describe a method for regulatory acceptance that demonstrates the adequacy and sufficiency of the NGNP defense-in-depth approach
- Describe how the NGNP defense-in-depth approach aligns with the NRC's expectations for greater use of risk-informed licensing practices
- Identify policy, technical issues, and outcome objectives for discussion with NRC.

The term "defense-in-depth" is used sparingly in NRC requirements, but is generally stated as a "philosophy" or a "concept," and those requirements are stated simply as, "Defense-in-depth shall be maintained." Guidance in the NRC Standard Review Plan provides further definition:

> *"Defense in depth is defined as a philosophy that ensures that successive measures are incorporated into the design and operating practices for nuclear plants to compensate for potential failures in protection and safety measures. In risk-informed regulation, the intent is to ensure that the defense-in-depth philosophy is maintained, not to prevent changes in the way defense in depth is achieved. The defense-in-depth philosophy has been and continues to be an effective way to account for uncertainties in equipment and human performance."*

Based on the analysis of NRC historical literature, requirements, guidance, and policy papers, and by considering the principles described by the International Atomic Energy Agency (IAEA), it is proposed that the NGNP framework for defense-in-depth address the three major elements summarized below and illustrated in Figure E-1:

- **Plant Capability Defense-in-Depth** reflects the decisions made by the designer in the selection of functions, structures, systems, and components for the design that ensure defense-in-depth in the physical plant.
- **Programmatic Defense-in-Depth** reflects the decisions made regarding the processes of manufacturing, constructing, operating, maintaining, testing, and inspecting the plant and the processes undertaken that ensure plant safety throughout the lifetime of the plant.
- **Risk-Informed Evaluation** of defense-in-depth reflects the development and evaluation of strategies that manage the risks of accidents, including the strategies of accident prevention and mitigation. This aspect of defense-in-depth also provides the framework for performing deterministic and probabilistic safety evaluations, which help determine how well various **Plant Capability Defense-in-Depth** and **Programmatic Defense-in-Depth** strategies have been implemented.

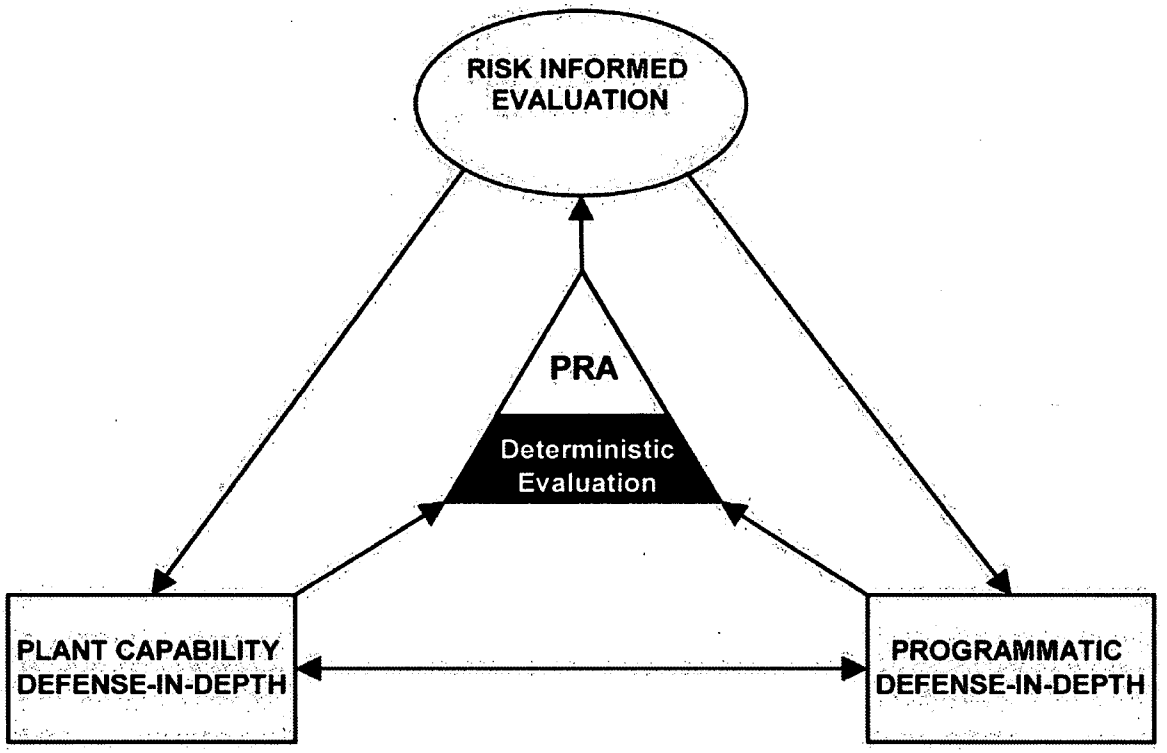


Figure E-1. Illustration showing the three major elements of the NGNP framework.

Figure E-2 presents an overview of the design and analysis process proposed for the NGNP project. The "historic" deterministic approach is integrated with a risk-informed evaluation methodology to ensure that selected design features provide the required level of safety and defense-in-depth.

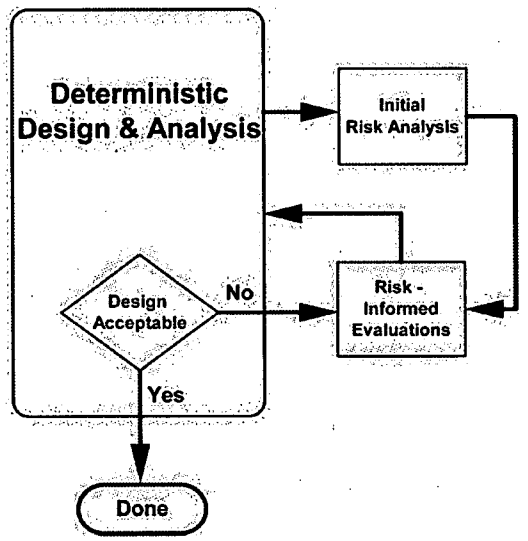


Figure E-2. Overview of the design and analysis process proposed for the NGNP project.

The NGNP defense-in-depth approach embraces the engineering and regulatory practices that have evolved over the last 50 years of reactor design and licensing and more completely integrates risk-informed, performance-based methods into the NGNP project design process. This process combines deterministic and probabilistic methods into a robust fabric designed to expose relationships in design and operation.

The proposed methodology also provides for compensatory special treatment requirements in design, manufacturing, construction, testing, operations and maintenance to compensate for uncertainties in the design and analysis process, thus providing a high confidence that equipment will perform as expected. The result will be a set of conservative design features combined with inherent reactor characteristics, passive design features, and active systems to (1) prevent transients and accidents, (2) ensure the performance of safety functions, (3) prevent the release of radioactive material, and (4) mitigate the consequences of accidents.

The principles of multiple, independent, and concentric barriers to radionuclide transport are assessed for each significant source of radioactive material to ensure that defense-in-depth has been maintained. In addition, the principles of design margin, redundancy, and diversity would be applied in the design of the structures, systems, and components that support the required safety functions and maintain the integrity and effectiveness of these barriers.

These defense-in-depth strategies ensure that the top level regulatory criteria are met, adequate safety margins are demonstrated, deterministic principles of defense-in-depth are included, and that residual uncertainties in the reliabilities and capabilities of the SSCs providing the required safety functions are adequately addressed for the life of the plant.

In summary, the questions proposed for discussions with NRC are:

- What is an appropriate definition of defense-in-depth for the NGNP project?
- Is the definition of defense-in-depth suitable to allow objective evaluation of plant safety?
- How does the defense-in-depth approach for the NGNP Project provide assurance that defense-in-depth is applied throughout the life of the plant?

- How is the defense-in-depth philosophy reflected in the risk-informed licensing evaluation methodology?
- Does the defense-in-depth approach described in this paper adequately address the technical elements as outlined in the NGNP Licensing Strategy Report to Congress?
- How are the defense-in-depth strategies of accident prevention and mitigation defined and evaluated for the NGNP Project?
- Is the defense-in-depth approach described in this paper sufficient to enable the NRC to evaluate the adequacy of the defense-in-depth treatment in the NGNP license application?

NRC documentation of its responses to the above questions and corresponding revisions to this paper will provide an agreed basis for related issues to be properly addressed in the NGNP license application.

CONTENTS

ABSTRACT iii

EXECUTIVE SUMMARY v

ACRONYMS xii

1. INTRODUCTION 1
   - 1.1 Purpose 1
   - 1.2 Objectives of this Paper 3
   - 1.3 Scope 3
   - 1.4 Statement of the Issues 3
   - 1.5 Summary of Outcome Objectives 4
   - 1.6 Relationship to Other NGNP Topics/Papers 5

2. REGULATORY FOUNDATION 7
   - 2.1 U.S. Regulatory Foundation for Defense-in-Depth 7
     - 2.1.1 NRC Requirements 7
     - 2.1.2 NRC Policy Statements 9
     - 2.1.3 NRC Guidance 9
   - 2.2 Other References 10
     - 2.2.1 NGNP Licensing Strategy—Report to Congress 10
     - 2.2.2 NRC Strategic Plan 10
     - 2.2.3 Development of a Risk-Informed and Performance-Based Update to 10 CFR Part 50 Requirements 11
     - 2.2.4 Advisory Committee on Reactor Safeguards Recommendations 12
     - 2.2.5 NRC Precedents Involving Gas-Cooled Reactors 13
     - 2.2.6 NRC Precedents Involving LWRs 15
   - 2.3 Regulatory Basis Summary 16

3. NGNP APPROACH TO DEFENSE-IN-DEPTH 18
   - 3.1 Risk-Informed and Performance-Based Design Process 18
     - 3.1.1 Design Process Overview 18
     - 3.1.2 Summary of Risk-Informed and Performance-Based Design Process 21
   - 3.2 NGNP Defense-in-Depth Framework 21
     - 3.2.1 Overview 22
     - 3.2.2 Plant Capability Defense-in-Depth 25
     - 3.2.3 Programmatic Defense-in-Depth 29
     - 3.2.4 Risk-Informed Evaluation of Defense-in-Depth 31
   - 3.3 Demonstrating Defense-in-Depth Adequacy 39
     - 3.3.1 Implementation of Plant Capability Defense-in-Depth 39
     - 3.3.2 Implementation of Programmatic Defense-in-Depth 45
     - 3.3.3 Implementation of Risk-Informed Evaluation of Defense-in-Depth 47
   - 3.4 Summary of Defense-in-Depth Insights for the NGNP Project 47

4. ISSUES FOR RESOLUTION 52

4.1 NRC Discussion Topics 52
4.2 Outcome Objectives 52

5. REFERENCES 54

Appendix A Regulatory Requirements Overview 56

Appendix B Bibliography of Related Documents 74

Appendix C Table of Cross References to PBMR Requests for Additional Information on Defense-In-Depth 78

Appendix D Expanded Description of Process for Risk Informing the Design 83

FIGURES

Figure E-1. Illustration showing the three major elements of the NGNP framework. vi
Figure E-2. Overview of the design and analysis process proposed for the NGNP project. vii
Figure 1-1. Elements of the NGNP defense-in-depth framework. 2
Figure 3-1. Major elements of the NGNP design approach. 18
Figure 3-2. Design—safety analysis—technology development overview. 20
Figure 3-3. Elements of the defense-in-depth framework. 23
Figure 3-4. Detailed elements of defense-in-depth framework. 25
Figure 3-5. Barriers to radionuclide transport included in plant capability defense-in-depth. 27
Figure 3-6. Elements of safety design approach incorporated into ***Plant Capability Defense-in-Depth***. 28
Figure 3-7. Logic for implementing ***Risk-Informed Evaluation*** of defense-in-depth. 37
Figure 3-8. Fuel primary barrier to radionuclide transport. 40
Figure 3-9. Example of major components and structures in HTGR designs 41
Figure D-1. Risk-informed performance-based design process 85
Figure D-2. NGNP frequency-consequence curve 87
Figure D-3. Example safety functions for an HTGR. 88
Figure D-4. Master logic diagram for selection of initiating events. 91
Figure D-5. Overview of PRA elements. 92

TABLES

Table 2-1. Requirements on defense-in-depth included in 10 CFR. 7
Table 3-1. Elements of ***Plant Capability Defense-in-Depth***. 30
Table 3-2. Elements of ***Programmatic Defense-in-Depth***. 32
Table 3-3. Derivation of defense-in-depth principles from Standard Review Plan, Chapter 19. 34

Table 3-4. Principles for establishing the adequacy of defense-in-depth. 36
Table 3-5. Elements of ***Risk-Informed Evaluation*** of defense-in-depth..... 38
Table 3-6. Radioactive sources and barriers. 40
Table 3-7. Examples of design features and SSCs providing plant capability defense-in-depth..... 43
Table 3-8. Approach to addressing defense-in-depth principles of Table 3-5. 48
Table A-1. Levels of defense-in-depth. 65
Table D-1. Evaluation of the deterministic bases for the PRA. 93
Table D-2. Risk-informed performance-based licensing approach. 94

ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
ALARA	as low as reasonably achievable
ALWR	advanced light water reactor
ANPR	advanced notice of proposed rulemaking
AOO	anticipated operational occurrence
ASME	American Society of Mechanical Engineers
BDBE	beyond design basis event
CFR	Code of Federal Regulations
DBE	design basis event
DBA	design basis accident
DCD	design control document
DID	defense-in-depth
DOE	Department of Energy
DVS	depressurization vent shaft
EAB	exclusion area boundary
EP	emergency planning
EPCC	equipment protection cooling circuit
EPRI	Electric Power Research Institute
EPZ	emergency planning zone
F-C	frequency-consequence (curve)
FHSS	fuel handling and storage system
HPB	helium pressure boundary
HTGR	high temperature gas-cooled reactor
HTS	heat transport system
HVAC	heating ventilation and air-conditioning
IAEA	International Atomic Energy Agency
INSAG	International Nuclear Safety Advisory Group
LBE	licensing basis event
LWR	light water reactor
MHTGR	modular high temperature gas-cooled reactor
MHSS	main heat sink system
NFPA	National Fire Protection Association
NGNP	Next Generation Nuclear Plant

NRC	Nuclear Regulatory Commission
NSRST	Non-Safety Related with Special Treatment
NUREG	Nuclear Regulatory Commission Report (United States)
NUREG/CR	Nuclear Regulatory Commission Consultant Report
PBMR	pebble bed modular reactor
PHTS	primary heat transport system
PRA	probabilistic risk assessment
PRS	pressure relief system
QHO	quantitative health objective
RAI	request for additional information
RB	reactor building
RCCS	reactor cavity cooling system
RG	Regulatory Guide
RIPB	risk-informed, performance-based
RIM	reliability and integrity management
RTNSS	regulatory treatment of non-safety systems
SCS	shutdown cooling system
SECY	NRC Commissioner's Document (acronym)
SER	Safety Evaluation Report
SFC	single failure criterion
SR	Safety Related
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan (U. S. Nuclear Regulatory Commission)
SSC	structures, systems, and components
TLDC	top level design criteria
TLRC	top level regulatory criteria
URD	Utility Requirements Documents

Next Generation Nuclear Plant Defense-in-Depth Approach

1. INTRODUCTION

1.1 Purpose

This paper (1) documents the definition of defense-in-depth and the approach that will be used to assure that its principles are satisfied for the Next Generation Nuclear Plant (NGNP) Project and (2) identifies the specific questions proposed for discussions with the Nuclear Regulatory Commission (NRC). Defense-in-depth is a safety philosophy in which multiple lines of defense and conservative design and evaluation methods are applied to ensure the safety of the public. The philosophy is also intended to deliver a design that is tolerant to uncertainties in knowledge of plant behavior, component reliability, or operator performance that might compromise safety. This paper includes a review of the regulatory foundation for defense-in-depth, a definition of defense-in-depth that is appropriate for advanced reactor designs based on high temperature gas-cooled reactor (HTGR) technology, and an explanation of how this safety philosophy is achieved in the NGNP design.

The principles of defense-in-depth are applied in the design, licensing, construction, operation and regulation of existing and advanced nuclear power plants; the NGNP design is no exception. In the design and analysis process proposed for the NGNP, the "historic" deterministic approach is integrated with a risk-informed evaluation methodology to ensure that selected design features provide the required level of safety and defense-in-depth. The result is a set of conservative design features combined with inherent reactor characteristics, passive design features, and active systems to (1) prevent transients and accidents, (2) ensure the performance of safety functions, (3) prevent the release of radioactive material, and (4) mitigate the consequences of accidents. The principles of multiple, independent, and concentric barriers to radionuclide transport are assessed for each significant source of radioactive material to assure that defense-in-depth has been maintained. In addition, the principles of design margin, redundancy, and diversity are applied in the design of the structures, systems, and components (SSCs) that support the required safety functions and serve to support and maintain the integrity and effectiveness of these barriers. The defense-in-depth strategies ensure that top level regulatory criteria (TLRC) are met,[a] adequate safety margins are achieved, deterministic principles of defense-in-depth are applied, and uncertainties in the reliabilities and capabilities of the SSCs providing the required safety functions are adequately addressed over the life of the plant.

Defense-in-depth is also demonstrated through the use of conservative assumptions and methods in a risk-informed safety evaluation process. This is achieved through the use of conservative assumptions and treatment of uncertainties in the selection of frequency and dose limits for use in defining and selecting licensing basis events (LBEs), performing deterministic analyses of design basis accidents (DBAs),

---

a. In the NGNP approach, the term TLRC refers to a set of criteria from the NRC regulations and guidance which together provide the basis for determinations of "adequate protection" as required by the Atomic Energy Act of 1954. Dose criteria from the TLRC are used to construct a Frequency-Consequence Curve that is used to evaluate the acceptability of the LBE frequency-consequence results in the risk-informed, performance-based methodology. In addition, NRC Safety Goal Quantitative Health Objectives (QHOs) and their surrogates are used in conjunction with Probabilistic Risk Assessments to provide a quantitative measure of integrated plant risk. Compliance with the Safety Goal QHOs and their surrogates is considered a measure of safety over and above that required for adequate protection (e.g., see SECY-89-102). Plant designers meet the TLRC and generally include enough conservatism in the design and analysis process such that the designs also meet the QHO surrogates, frequently by "orders of magnitude."

performing safety classifications[b] of SSCs, and developing special treatment requirements. The NGNP Project approach to defense-in-depth is structured to permit an objective quantitative evaluation of the roles that specific SSCs and design features play in the prevention and mitigation of accidents. This approach uses information developed in the probabilistic risk assessment (PRA) and includes an evaluation of uncertainties to identify the need for deterministic requirements and compensatory measures to ensure that the appropriate level of reliability and safety is achieved over the life of the plant. In this risk-informed evaluation process it is important to use a set of deterministic defense-in-depth principles, derived from the regulatory foundation, in demonstrating the adequacy and sufficiency of defense-in-depth.

The proposed framework for defense-in-depth recognizes the following three major elements (illustrated in Figure 1-1).

- ***Plant Capability Defense-in-Depth*** reflects the decisions made by the designer in the selection of functions, structures, systems, and components for the design that assure defense-in-depth in the physical plant.
- ***Programmatic Defense-in-Depth*** reflects the decisions made regarding the processes of manufacturing, constructing, operating, maintaining, testing, and inspecting the plant and the processes undertaken that ensure plant safety throughout the lifetime of the plant.
- ***Risk-Informed Evaluation*** of defense-in-depth reflects the development and evaluation of strategies that manage the risks of accidents, including the strategies of accident prevention and mitigation. This aspect of defense-in-depth also provides the framework for performing deterministic and probabilistic safety evaluations that help determine how well various ***Plant Capability Defense-in-Depth*** and ***Programmatic Defense-in-Depth*** strategies have been implemented. The goal of this evaluation is to demonstrate the adequacy and sufficiency of all physical and programmatic measures to assure that defense-in-depth is maintained in the design.

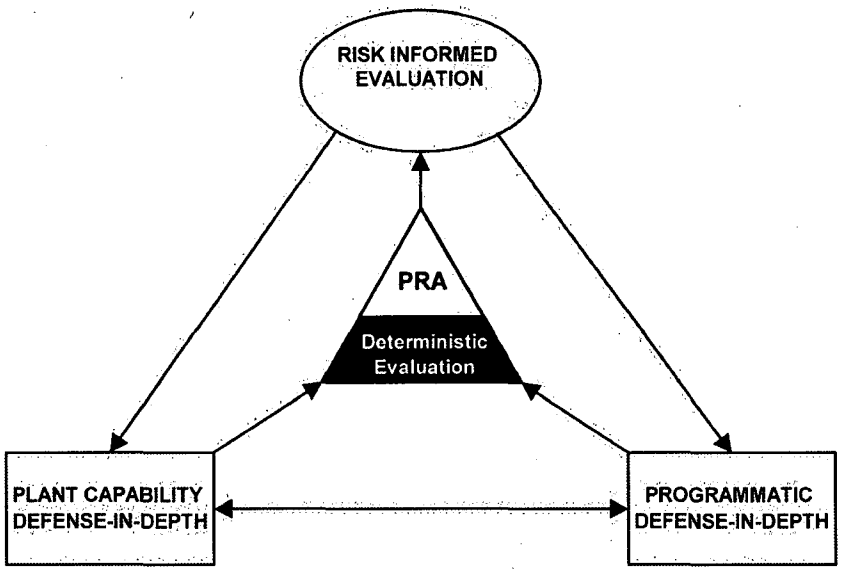


Figure 1-1. Elements of the NGNP defense-in-depth framework.

b. "Safety classification" means the process by which SSCs are classified as safety-related, non-safety-related, or non-safety-related with special treatment because they have some safety value in the PRA. "Safety classified" is used to refer to SSCs that have been through the safety classification process.

In summary, this paper addresses the integrated consideration of defense-in-depth for the NGNP Project. Key elements of the defense-in-depth approach are defined, and how they will be addressed in the design and license application is described.

1.2 Objectives of this Paper

The objectives of this paper are to:

- Summarize the regulatory requirements, guidance, and precedents that apply to defense-in-depth in general, and specifically, to advanced HTGR designs, including the NGNP design (Refer to Section 2)
- Develop a definition that addresses the various aspects of defense-in-depth appropriate to non-light water reactors (LWRs). Evaluate how this definition compares with definitions typically used by NRC (Refer to Section 3.2)
- Describe a methodology for achieving the various aspects of defense-in-depth, including plant design and operation (Refer to Sections 3.1 and)
- Describe how the defense-in-depth approach identifies the role of special compensatory measures for the unique first-of–a-kind issues in the NGNP design (Refer to Sections 3.1 and)
- Describe a method for regulatory acceptance that demonstrates the adequacy and sufficiency of the defense-in-depth approach (Refer to Section 3.3)
- Describe how the NGNP Project defense-in-depth approach aligns with NRC expectations for greater use of risk-informed licensing practices (Refer to Sections 3.3 and 3.4)
- Identify policy, technical issues, and outcome objectives for discussion with the NRC (Refer to Section 4).

1.3 Scope

The defense-in-depth 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 methodology described in this white paper addresses the entire plant design-operation life cycle.

1.4 Statement of the Issues

The issues addressed in this paper are framed in terms of the following questions about the NGNP Project approach to defense-in-depth that will be implemented as part of the design and license application:

- What is an appropriate definition of defense-in-depth for the NGNP Project?
- Is the definition of defense-in-depth suitable to allow objective evaluation of plant safety?
- What are the elements of defense-in-depth for the safety design philosophy, design approach and analyses, and the assurance programs to ensure that defense-in-depth is achieved throughout the life of the plant?
- How is the defense-in-depth philosophy reflected in the risk-informed licensing approach proposed for the NGNP Project?
- How are the defense-in-depth strategies of accident prevention and mitigation defined and evaluated?

- Does the defense-in-depth approach described in this paper adequately address the technical elements as outlined in the NGNP Licensing Strategy Report to Congress?
- Is the defense-in-depth approach described in this paper sufficient to enable the NRC to evaluate the adequacy of the defense-in-depth treatment in the NGNP Project license application?

1.5 Summary of Outcome Objectives

The objective of this paper is to solicit NRC feedback and agreement on an appropriate definition of defense-in-depth sufficient to support NGNP Project licensing, including relevant elements of a nuclear plant life cycle. Specifically, feedback is requested regarding NRC agreement with the following statements, or that the NRC provide an alternative set of statements that would be acceptable.

1. The definition of defense-in-depth presented in Section 3.2 of this paper, which recognizes three elements of a defense-in-depth approach: ***Plant Capability Defense-in-Depth***, ***Programmatic Defense-in-Depth***, and ***Risk-Informed Evaluation*** of defense-in-depth, is consistent with available definitions summarized in the regulatory foundation and is appropriate for the license application.
2. The ***Plant Capability Defense-in-Depth*** element, which includes multiple independent and diverse barriers to radionuclide transport, the use of inherent features and passive and active SSCs to perform the required safety functions, and conservative design strategies, is appropriate for the license application.
3. The ***Programmatic Defense-in-Depth*** element represents an acceptable approach to the incorporation of defense-in-depth principles into the definition of programs that will provide assurance that the plant capabilities to assure safety and defense-in-depth will have sufficient reliability and be maintained throughout the lifetime of the plant and that uncertainties not addressed by Plant Capability Defense-in-Depth are adequately addressed by compensatory actions.
4. The ***Risk-Informed Evaluation*** of defense-in-depth elements provides an acceptable balance of deterministic and probabilistic assessments and evaluation criteria. Further, this element approach includes an acceptable event sequence framework for the definition of accident prevention and mitigation and for the evaluation of the roles of design features and SSCs responsible for prevention and mitigation for demonstrating the safety case. Finally, the balanced use of deterministic and probabilistic evaluations provides a logical process to establish the adequacy and sufficiency of defense-in-depth.
5. When the approach described in this paper is applied to the design and described in the NGNP license application, the NRC will have sufficient information on which to judge the adequacy of the defense-in-depth provisions in the NGNP design. This information will include:
    a. A definition of defense-in-depth that is appropriate for the NGNP Project.
    b. The roles of each barrier to radioactive material retention for each significant inventory of radionuclides in providing the plant capabilities for defense-in-depth.
    c. How the reliability, capability, and independence of each barrier are defined and evaluated in terms of their plant capabilities for defense-in-depth.
    d. How the safety functions are defined and how they support the integrity of each barrier in providing the plant capabilities for defense-in-depth.
    e. The roles of diverse combinations of inherent and passive design features and SSCs that are used as well as active engineered systems to perform the safety functions as part of the plant capabilities for defense-in-depth.
    f. How the reliability, capability, and independence of each SSC providing a safety function is defined and evaluated as it relates to the plant capabilities for defense-in-depth.

g. How the principles of design margins, redundancy, diversity, and independence have been applied in providing the plant capabilities for defense-in-depth.

h. An appropriate definition of accident prevention and mitigation and a means to evaluate the impact of the defense-in-depth strategies on maintaining acceptable risk levels.

i. The roles and effectiveness of specific barriers and SSCs in the prevention and mitigation of accidents.

j. The role of design safety margins as reflected in the applied codes and standards in providing a robust design with defense-in-depth.

k. How compensating measures and other aspects of Programmatic Defense-in-Depth are applied to address uncertainties.

l. How a set of deterministic principles derived from the regulatory foundation is applied in the risk-informed evaluation of the adequacy and sufficiency of defense-in-depth.

m. How the elements of the NGNP Project safety design approach are used to evaluate plant design features in an integrated manner as part of an overall risk management approach in which risk analysis is used to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities to reduce risk.

1.6 Relationship to Other NGNP Topics/Papers

Broadly defined, defense-in-depth is a safety philosophy in which multiple lines of defense, conservative design and evaluation methods, and compensatory measures are applied to prevent and mitigate accidents and to assure the safety of the public. This philosophy covers broad areas of design, selection of LBEs, safety classification of SSCs, probabilistic and deterministic safety analysis, special treatment, and other regulatory requirements. Thus, the treatment of defense-in-depth is best evaluated in an integrated fashion.

This paper on defense-in-depth draws substantially from the Pebble Bed Modular Reactor (Proprietary) Limited (PBMR) preapplication white paper of the same name.[1] The PBMR paper was submitted to the NRC in December 2006 following earlier submittals of three white papers on PRA approach, LBE selection, and safety classification of SSCs.[2, 3, 4] The NRC reviewed these papers and provided an integrated set of requests for additional information (RAIs) in September 2007.[5] Following a workshop to discuss the RAIs, PBMR's responses to the RAIs on the four white papers were submitted to the NRC in March 2008.[6] Specific issues raised in the PBMR RAIs relevant to the NGNP Project defense-in-depth approach are incorporated in appropriate locations in Section 3 of this paper. Additionally, Appendix C includes a listing of the PBMR defense-in-depth RAIs along with a cross-reference to where within this paper each RAI issue has been addressed.

Companion papers to this paper on defense-in-depth will be submitted as part of the NGNP Project effort. Two papers that specifically strengthen the understanding of the defense-in-depth approach described in this paper include:

- ***Selection of LBEs.*** Defense-in-depth considerations are applied to the NGNP Project in the derivation of the frequency-consequence (F-C) curve (described in Appendix D, Section D.1.6) and the selection of LBEs based on deterministic inputs and information from the PRA. This white paper will:
  - Summarize the regulatory policy and guidance that is available for classifying and selecting LBEs for advanced reactor designs
  - Discuss the history of using a risk-informed, performance-based approach for LBE selection for advanced reactor designs

- Describe an approach for LBE selection that would result in a comprehensive risk-informed licensing approach that is consistent with NRC guidance for application of deterministic analysis and the use of PRA
- Include the basis for event frequency and consequence limits associated with anticipated operational events, design-basis events, and beyond design-basis events that would be used to develop a frequency/consequence curve for the NGNP design evaluation
- Highlight the portions of the recommended LBE selection methodology where deterministic principles are applied
- Describe the NGNP Licensing Strategy's (Report to Congress) recommended method for adapting existing light water reactor rules (Option 2) and discuss how the recommended LBE selection methodology compares to Option 2
- Identify policy and technical issues that should be discussed with the NRC.

- ***Safety Classification SSCs.*** The principles of defense-in-depth are applied in the identification of safety-related SSCs and in the development of special treatment requirements for safety classified SSCs for the NGNP design. This white paper will:
  - Summarize the regulatory policy and guidance that would apply to selecting and classifying SSCs for an HTGR
  - Describe the recommended approach for identifying and classifying SSCs that are relied upon to function during licensing basis events
  - Describe how special treatment methods would be identified for safety-related SSCs or any non-safety-related SSCs that are considered to be important to safety
  - Describe how the SSC selection/classification process relates to other parts of a risk-informed licensing approach
  - Identify policy and technical issues that should be discussed with the NRC.

Other NGNP Project white papers that help reinforce elements of the defense-in-depth approach include papers on fuel qualification, mechanistic source term, high temperature materials (metals and graphite), and safety analysis codes validation and verification.

2. REGULATORY FOUNDATION

Defense-in-depth is generally stated in regulation as a "philosophy" or a "concept," and the term is used in only a few regulatory requirements statements. This section briefly reviews regulatory requirements and guidance where defense-in-depth statements have appeared, and summarizes by proposing a generic "regulatory definition" from which an NGNP project approach can reasonably be stated.

The regulatory history on defense-in-depth has come together over a long period of time during which LWRs were the dominant technology undergoing regulatory review. A large body of defense-in-depth experience and insight was not developed for advanced, non-LWR designs because not as many non-LWR applications were reviewed by the NRC. As such, much of the terminology and attributes used in the regulatory discussion on defense-in-depth is directed at LWR technology. Differences in terminology and attributes, needed for a proper definition of a defense-in-depth approach, are described throughout this paper.

The body of documents available from which to derive a proper understanding of defense-in-depth principles is large. With the exception of the regulatory requirements statements described in Section 2.1.1, the other documents referenced in Section 2 represent a mere subset of the library that is available. A more detailed discussion of defense-in-depth statements in the regulatory history is provided in Appendix A. Appendix B includes a bibliography of additional references that add to the understanding of the topic.

2.1 U.S. Regulatory Foundation for Defense-in-Depth

2.1.1 NRC Requirements

NRC regulatory requirements, codified in 10 CFR (Code of Federal Regulations), contain only a handful of instances that specifically mention defense-in-depth. Table 2-1 lists these CFR references and the requirements statements. Generally, the statements specify that defense-in-depth concepts or practices are to be implemented, or simply, that defense-in-depth is to be maintained.

Table 2-1. Requirements on defense-in-depth included in 10 CFR.

10 CFR	Statement
§50.48, Fire protection Subsection (c) National Fire Protection Association (NFPA) Standard NFPA 805.	(2) Exceptions, modifications, and supplementation of NFPA 805. As used in this section, references to NFPA 805 are to the 2001 Edition, with the following exceptions, modifications, and supplementation: (vii) Performance-based methods. (C) Maintains fire protection defense-in-depth (fire prevention, fire detection, fire suppression, mitigation, and post-fire safe shutdown capability).
Appendix R to Part 50, Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979	II. General Requirements ... The fire protection program shall extend the concept of defense-in-depth to fire protection in fire areas important to safety.
§50.69, Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors	(c) SSC Categorization Process. ,,, The process must: ... (iii) Maintain defense-in-depth".

Table 2-1. (continued).

10 CFR	Statement
§70.64, Requirements for new facilities or new processes at existing facilities	(b) Facility and system design and facility layout must be based on defense-in-depth practices.[1] The design must incorporate, to the extent practicable: (1) Preference for the selection of engineered controls over administrative controls to increase overall system reliability; and (2) Features that enhance safety by reducing challenges to items relied on for safety. ---------- FN 1. As used in §70.64, Requirements for new facilities or new processes at existing facilities, defense-in-depth practices means a design philosophy, applied from the outset and through completion of the design, that is based on providing successive levels of protection such that health and safety will not be wholly dependent upon any single element of the design, construction, maintenance, or operation of the facility. The net effect of incorporating defense-in-depth practices is a conservatively designed facility and system that will exhibit greater tolerance to failures and external challenges. The risk insights obtained through performance of the integrated safety analysis can be then used to supplement the final design by focusing attention on the prevention and mitigation of the higher-risk potential accidents.
§73.54, Protection of digital computer and communication systems and networks	(c) The cyber security program must be designed to: (2) Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks.
§73.55, Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage Subsection (b) General performance objective and requirements	(3) The physical protection program must be designed to prevent significant core damage and spent fuel sabotage. Specifically, the program must: ... (ii) Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program. (9) The licensee shall establish, maintain, and implement an insider mitigation program and shall describe the program in the Physical Security Plan (i): "The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent significant core damage and spent fuel sabotage.
§100.1, Reactor site criteria; purpose	(d) The Commission intends to carry out a traditional defense-in-depth approach with regard to reactor siting to ensure public safety.

2.1.2 NRC Policy Statements

Consideration of the defense-in-depth philosophy and its attributes has been included in several of NRC's policy statements. The 1986 Policy Statement on Safety Goals for the Operations of Nuclear Power Plants[7] states:

> *"The Commission recognizes the importance of mitigating the consequences of a core-melt accident and continues to emphasize features such as containment, siting in less populated areas, and emergency planning as integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy...*
>
> *To provide adequate protection of the public health and safety, current NRC regulations require conservatism in design, construction, testing, operation and maintenance of nuclear power plants. A defense-in-depth approach has been mandated in order to prevent accidents from happening and to mitigate their consequences. Siting in less populated areas is emphasized. Furthermore, emergency response capabilities are mandated to provide additional defense-in-depth protection to the surrounding population."*

NRC's Policy Statement on the Regulation of Advanced Reactors,[8] also published in 1986 (revised in 1994 and 2008), states:

> *"Among the attributes that could assist in establishing the acceptability or licensability of a proposed advanced reactor design, and therefore should be considered in advanced designs, are... [d]esigns that incorporate the defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for, and consequences of, severe accidents."*

The 1995 NRC Policy Statement on Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities[9] states:

> *"In the defense-in-depth philosophy, the Commission recognizes that complete reliance for safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant. Thus, the expanded use of PRA technology will continue to support the NRC's defense-in-depth philosophy by allowing quantification of the levels of protection and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry. Defense-in-depth is a philosophy used by NRC to provide redundancy for facilities with 'active' safety systems, e.g., a commercial nuclear power (sic), as well as the philosophy of a multiple-barrier approach against fission product releases."*

2.1.3 NRC Guidance

NRC guidance on defense-in-depth is stated in several Regulatory Guides (RGs) and the Standard Review Plan (SRP), NRC Report NUREG-0800. Appendix A identifies a number of RGs in which defense-in-depth is discussed. The following present several examples that provide useful examples for the NGNP Project approach:

- RG 1.174, "An Approach to Using PRA in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis,"[10] provides guidance in how defense-in-depth is to be addressed when considering plant changes. This RG has been a preferred reference in NRC efforts revising existing requirements to allow for risk-informed approaches in regulatory actions.

- RG 1.183, "Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors," RG 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," and Chapter 19 of the SRP provide further perspective on defense-in-depth and on the role that barriers play in providing defense-in-depth (summarized in more detail in Appendix A).
- The SRP provides a set of objectives and guidelines for consideration by NRC reviewers when reviewing licensee-proposed changes. In discussing the need to preserve multiple barriers against radioactivity release, SRP Chapter 19 includes a set of review objectives to ensure that the "appropriate safety within the defense-in-depth philosophy" is maintained. These objectives are reproduced in Table 3-3 along with an assessment of the NGNP Project approach for each of the objectives.

2.2 Other References

2.2.1 NGNP Licensing Strategy—Report to Congress

The NGNP Licensing Strategy—Report to Congress describes several licensing alternatives and options for adapting existing NRC technical requirements to the NGNP Project.[11] A more detailed summary is provided in Appendix A. The important elements of defense-in-depth that are considered in the statement of the technical approach to establishing the licensing basis are:

- *Establishment of licensing-basis event categories (i.e., abnormal occurrences, design-basis accidents, and beyond-design-basis accidents) based on the expected probability of event occurrence...*
- *Selection of the safety-significant systems, structures, and components (SSCs) relied on to prevent or mitigate the safety-significant licensing-basis events using deterministic judgment, complemented by insights from the NGNP PRA.*
- *Establishment of conservative design and acceptance criteria for core and safety-significant SSCs,...*
- *Verification of adequate safety margins to the integrity and performance of core and safety-significant SSCs...*
- *Establishment of special treatment requirements to ensure the required performance capability and reliability of the safety-significant SSCs...*
- *Use of consequence acceptance limits for onsite or offsite releases for licensing-basis events.....also, assessment of radiological consequences for licensing-basis events on the basis of event-specific mechanistic source terms.*
- *Consideration of containment functional performance requirements as a radionuclide barrier...*
- *Establishment of defense-in-depth design requirements....*

2.2.2 NRC Strategic Plan

NRC's most recent Strategic Plan[12] describes the importance of defense-in-depth in conjunction with the use of conservative and realistic practices in providing an adequate margin of safety:

> *"It is the responsibility of the NRC to ensure that its licensees operate nuclear facilities and use radioactive materials safely. The NRC employs a multi-faceted regulatory approach to safety that includes the following activities:*
>
> – *Develop and update risk-informed and performance-based standards and regulations, as appropriate and Federal regulations to enable the safe use of radioactive materials, using the*

"defense-in-depth" principles and appropriately conservative and realistic practices that provide an adequate margin of safety.

- *License individuals and organizations that intend to use radioactive materials for safe and beneficial civilian purposes.*
- *Maintain ongoing and consistent oversight of licensees, which includes inspection and enforcement, to ensure that they are conforming to the applicable regulations and the conditions of their licenses to ensure safety, and to provide timely and appropriate event assessment and response."*

The Strategic Plan then goes on to define defense-in-depth as:

> *"Defense-in-Depth: an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's Safety Philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility."*

2.2.3 Development of a Risk-Informed and Performance-Based Update to 10 CFR Part 50 Requirements

Following issuance of the PRA policy statement in 1995, the NRC embarked on a series of initiatives to both risk-inform existing regulatory requirements and to establish a new, risk-informed technology-neutral framework for future reactors. In SECY 2009-0056, *Staff Approach Regarding a Risk-Informed and Performance-Based Revision to Part 50 of Title 10 of the Code of Federal Regulations and Developing a Policy Statement on Defense-in-Depth for Future Reactors* [Ref. 34 of Appendix A], the NRC staff summarized the development of a technology-neutral regulatory framework.

> *"In accordance with Commission direction, the staff issued the technology-neutral framework as NUREG-1860, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," Volumes 1 and 2, in December 2007.[13] This NUREG documents a framework that provides an approach and criteria that (1) could be used to develop an alternative set of technical requirements to 10 CFR Part 50 applicable for future non-LWR nuclear power plants (the framework includes a proposed draft set of technical requirements), and (2) could be used to establish risk-informed licensing basis events and the safety classification of structures, systems, and components."*

NUREG 1860[13] provides extensive discussion of the topic of defense-in-depth as it relates to the risk-informed, performance-based (RIPB) structure for future plant licensing. It includes a definition of defense-in-depth that is the same as the glossary entry in NRC's Strategic Plan (NUREG-1614):

> *"Defense-in-depth is an element of NRC's safety philosophy that is used to address uncertainty by employing successive measures including safety margins to prevent and mitigate damage if a malfunction, accident or naturally caused event occurs at a nuclear facility"*

The NUREG includes a set of defense-in-depth principles for evaluating reactor designs:

- *"provide measures against intentional as well as inadvertent events;*
- *provide accident prevention and mitigation capability;*

- *ensure key safety functions are not dependent upon a single element of design, construction, maintenance or operation;*
- *ensure uncertainties in equipment and human performance are accounted for and appropriate safety margins provided;*
- *provide alternative capability to prevent unacceptable releases of radioactive material to the public; and*
- *be sited at locations that facilitate protection of public health and safety."*

The approach to defense-in-depth described in NUREG 1860 includes both deterministic and probabilistic. The two principal deterministic elements are:

- To ensure the implementation of all of the defense-in-depth protective strategies
- To ensure that defense-in-depth principles are followed to develop licensing potential requirements.

The probabilistic elements of the approach consist of:

- Using the PRA, to the extent possible, to search for and identify unexpected scenarios, including their associated uncertainties.
- Helping to establish adequate defense-in-depth measures, including safety margins, to compensate for those scenarios and their uncertainties that are quantified in the PRA model.

2.2.4 Advisory Committee on Reactor Safeguards Recommendations

The Advisory Committee on Reactor Safeguards (ACRS) reviews and provides recommendations to the NRC Commissioners in the development and implementation of NRC requirements and policy statements. The ACRS has also been engaged in NRC ongoing efforts to develop a technology-neutral regulatory approach for future reactors.

In a 1997 memorandum, the ACRS summarized the use of defense-in-depth statements in NRC's regulatory development history.[14] Later, in 1999, the ACRS provided the NRC with a detailed set of recommendations in a letter, "The Role of Defense in Depth in a Risk-Informed Regulatory System."[15] As with the earlier memorandum, this letter included an attached paper that described two views to defense-in-depth, one of a structuralist and a second of a rationalist:

> *"In one view (the "structuralist" view as described in the attached paper), defense in depth is considered to be the application of multiple and redundant measures to identify, prevent, or mitigate accidents to such a degree that the design meets the safety objectives. This is the general view taken by the plant designers. The other view (the "rationalist"), sees the proper role of defense in depth in a risk- informed regulatory scheme as compensation for inadequacies, incompleteness, and omissions of risk analyses. We choose here to refer to the inadequacies, incompleteness, and omissions collectively as uncertainties. Defense-in-depth measures are those that are applied to the design or operation of a plant in order to reduce the uncertainties in the determination of the overall regulatory objectives to acceptable levels. Ideally then, there would be an inverse correlation between the uncertainty in the results of risk assessments and the extent to which defense in depth is applied. For those uncertainties that can be directly evaluated, this inverse correlation between defense in depth and the uncertainty should be manifest in a sophisticated PRA uncertainty analysis."*

These concepts of structuralist and rationalist views are considered complementary. Their underlying premise is included within the NGNP Project licensing approach described in the Report to Congress (Section 2.2.1 above).

2.2.5 NRC Precedents Involving Gas-Cooled Reactors

2.2.5.1 Modular High-Temperature Gas-Cooled Reactor

At the request of the Department of Energy (DOE), the NRC in 1986 undertook a preapplication review of the modular high temperature gas-cooled reactor (MHTGR) design. Included was a review of defense-in-depth considerations for advanced reactor designs. NRC's review findings for the MHTGR are documented in NUREG-1338, "Draft Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor."[16]

In Section 1.5 "Review Approach and Criteria" of NUREG-1338, the NRC noted:

> *"Defense-in-depth was considered in the staff's review of the design and used as a basis for ensuring the MHTGR provides at least equivalent protection to the public and the environment as that provided by current-generation LWRs. Central to the staff's evaluation was the treatment of the policy issues discussed in Sections 1.4 and 3.2. Those policy issues arose because of the different approach used in the MHTGR design to accomplish key safety functions. The staff in its review attempted to develop criteria and a technical position to directly address the acceptability of the key features and policy issues associated with the MHTGR. For example, because of the high potential for preventing core damage in the MHTGR design, a mechanistic analysis of radionuclide releases for a range of low-probability bounding events (equivalent to severe accidents in LWRs and identified in Table 3.7) was proposed as a substitute for the traditional nonmechanistic large source term that is representative of a source term from a core-melt accident utilized in LWR siting. Guidance from the Commission's Safety Goal Policy Statement was used to help define the range of low-probability events to be considered; however, provision was maintained for engineering judgment to bound uncertainties in the selection of these events. Inherent in this approach is a shift in emphasis in defense-in-depth from accident mitigation to accident prevention and plant protection."*

NUREG-1338 also described NRC expectations for addressing defense-in-depth as applied to advanced reactors, and provided an overall conclusion as to the MHTGR defense-in-depth approach that is consistent with the NRC views:

> *"<u>Defense-in-Depth Principle As Applied to Advanced Reactors</u>. Defense-in-depth in nuclear power plant safety regulation is a philosophy that entails the use of various layers of requirements that help to ensure that safety is achieved through multiple, diverse, and complementary means. These layers of requirements address the different stages and aspects of plant safety that can be generally categorized as prevention, protection, mitigation, and emergency planning, and include items such as:*
>
> *(1) plant design using conservative assumptions, appropriate codes and standards, and quality in design, construction, operation, and maintenance to minimize the potential for accidents*
>
> *(2) high reliability, redundancy, and/or diversity in components, systems, and structures to adequately respond to and protect the plant and the barriers to radiation release in the event of an accident*

(3) mitigative capability to delay and limit the release of fission products to the environment in the event an accident leads to the failure of one or more barriers to radiation release

(4) emergency planning for protecting the public in the event radiation release from the plant exceeds acceptable limits

In general, DOE has attempted to maintain defense-in-depth in the MHTGR design by addressing all the categories listed above. However, the MHTGR designers have approached plant design and the means of maintaining defense-in-depth somewhat differently than the LWR designers. In general, the MHTGR design makes a shift in emphasis from mitigation features to highly reliable protection features. For example, MHTGR designers aim to achieve high reliability and protection through the use of simple and passive decay-heat-removal and reactor-shutdown methods, compared with high reliability through active systems as in LWR designs. These passive protection features are directed toward maintaining fuel integrity, even during very unlikely events. Mitigation is provided in the MHTGR design through different containment systems, through physical phenomena (fission product retention, plateout, and holdup), and through use of the long-time response of the reactor in accident sequences. This has resulted in a design that proposes to accomplish protection, mitigation, and emergency planning in ways different from those used for LWRs, and thus the issues discussed in Section 3.2.2 are raised.

In the development of the criteria discussed in the remaining part of this SER, requirements were included to ensure that each of the four categories of defense-in-depth listed above was addressed in the MHTGR design consistent with its unique characteristics, but with the objective of providing at least equivalent protection to the public when the defense-in-depth provisions are considered as a whole. In summary, the criteria relative to the accident-prevention aspects of defense-in-depth for the MHTGR are intended to require at least equivalent accident-prevention capabilities as those required for current-generation LWRs. The criteria for the protection and mitigation aspects of defense-in-depth are intended to provide equivalent protection to the public and environment against the release of radiation as for LWRs, when viewed together (that is, some tradeoff between protection and mitigation is allowed, such as the use of highly reliable passive plant-protection features versus a traditional containment building). The criteria for emergency planning are intended to provide an equivalent level of protection in consideration of the characteristics of the MHTGR."

2.2.5.2 Pebble Bed Modular Reactor

In 2001 and 2002, the NRC staff conducted a preapplication review of the PBMR at the request of Exelon. In a letter to Exelon dated March 26, 2002,[17] the NRC staff provided its assessment of the licensing approach proposed by Exelon, including the TLRC. With respect to defense-in-depth, the NRC staff stated:

"It is the staff's view that the TLRC approach does not provide a mechanism for consideration of defense-in-depth. The TLRC may be considered to be acceptance criteria for the mitigation aspect of defense-in-depth, but from a regulatory standpoint, it is very important to have criteria for prevention as well.... (Enclosure, pg. 10) [A figure presented by Exelon] seems to imply that the function can be met without controlling radionuclide transport from the reactor building and from the site, which appears to contradict the defense-in-depth philosophy. The role of a containment in the PBMR design will be specifically addressed and is expected to be presented to the Commission as a policy issue."

The PBMR preapplication project also included the submittal of a defense-in-depth white paper of the same name.[1] The PBMR paper was submitted to the NRC in December 2006 following earlier submittals of three white papers on PRA approach, LBE selection, and safety classification of SSCs. The NRC reviewed these papers and provided an integrated set of RAIs in September 2007.[5] Following a workshop to discuss the RAIs, PBMR's responses to the RAIs on the four white papers were submitted to the NRC in March 2008.[6] Specific issues raised in the PBMR RAIs relevant to the NGNP Project defense-in-depth approach are identified and discussed in appropriate locations in Section 3 of this NGNP paper. Additionally, Appendix C includes a complete listing of the PBMR defense-in-depth RAIs along with a cross-reference of where within this paper each RAI has been addressed.

2.2.6 NRC Precedents Involving LWRs

Design Certification and Combined License applicants are required to submit information on the diversity and defense-in-depth of their reactor protection systems and an assessment of how risk insights are used to support the plant design and operational programs.[18] The AP1000 design certification provides an example from which insights may be observed.

In their Safety Evaluation Report (SER) on the AP1000,[19] the NRC stated in Section 7.1.2:

> *"The AP1000 uses passive safety systems that rely on natural forces, such as density differences, gravity, and stored energy, to provide water for core and containment cooling. The active AP1000 systems are not classified as safety-related. Therefore, credit is not taken for these active systems in the design-basis accident analyses described in DCD Tier 2, Chapter 15, "Accident Analysis," unless their operation makes the consequences of an accident more limiting. The non-safety-related active systems in the AP1000 provide defense-in-depth functions and supplement the capability of the safety-related passive systems."*

Further discussion is provided in SER Chapter 19, "Severe Accidents," which discusses how the risk importance of the nonsafety systems enhances the defense-in-depth capabilities of the design:

> *"The AP1000 design incorporates several active systems that are capable of performing some of the same functions performed by the safety-related passive systems. The availability of such redundant systems minimizes the challenge to the safety-related passive systems by providing core cooling during normal plant shutdowns and a first line of defense during accidents." [SER 19.1.2.1.2]*
>
> * * *
>
> *"In addition, sensitivity studies were performed to investigate the impact of uncertainties on the PRA results assuming plant operation at power without credit for the non-safety-related defense-in-depth systems ("focused" PRA model). These studies provided additional insights about the risk importance of the defense-in-depth systems which were taken into account in selecting non-safety-related systems for regulatory treatment within the RTNSS process." [SER 19.1.3.1.5]*

In SER Chapter 22, "Regulatory Treatment of Non-Safety Systems," the NRC noted that the Electric Power Research Institute (EPRI) Utilities Requirements Document (URD) for passive plants specifies standards concerning design and performance of active systems and equipment that perform non-safety-related, defense-in-depth functions:

> *"The [Advanced Light Water Reactor (ALWR)] Utility Requirements Document (URD) for passive plants, issued by the Electric Power Research Institute (EPRI), includes*

standards related to the design and operation of active, non-safety-related systems. The URD recommends that the plant designer specifically define the active systems relied upon for defense-in-depth and necessary to meet passive ALWR plant safety and investment protection goals. Defense-in-depth systems provide long-term, post-accident plant capabilities. Passive systems should be able to perform their safety functions, independent of operator action or offsite support, for 72 hours after an initiating event. After 72 hours, non-safety or active systems may be required to replenish the passive systems or to perform core and containment heat removal duties directly.

* * *

The residual uncertainties associated with passive safety system performance increase the importance of active systems in providing defense-in-depth functions to back up the passive systems. Recognizing this, the NRC and EPRI developed a process to identify important active systems and to maintain appropriate regulatory oversight of those systems. This process does not require that the active systems brought under regulatory oversight meet all safety-related criteria, but rather that these controls provide a high level of confidence that active systems having a significant safety role are available when they are challenged."

2.3 Regulatory Basis Summary

The term *defense-in-depth* is used sparingly in NRC requirements, but where used, it is generally stated as a philosophy or a concept. Regulatory requirements are simply stated as "Defense-in-depth shall be maintained," with emphasis in the guidance on the use of risk-informed assessment to establish how much defense-in-depth is enough. Here, the definition provided in NRC's Strategic Plan is useful:

> *"Defense-in-Depth: an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's Safety Philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility."*

By analyzing the historical literature of NRC requirements, guidance, and policy papers, and by considering the principles described by the International Atomic Energy Agency (IAEA), the various attributes or elements of a defense-in-depth strategy were identified. These attributes include:

- Successive compensatory means to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility
- Implementation of a multiple barrier approach against fission product releases
- Redundancy in performance of safety functions
- Assurance that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility
- Features that enhance safety by reducing challenges to SSCs relied on for safety
- Evaluation of plant design features in an integrated manner as part of an overall risk management approach in which risk analysis is used to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities to reduce risk

- Assurance that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work
- Preference for the selection of engineered controls over administrative controls to increase overall functional reliability
- Addressing uncertainty by employing measures, including safety margins and special treatments, to ensure equipment reliability to the level assumed in the design.

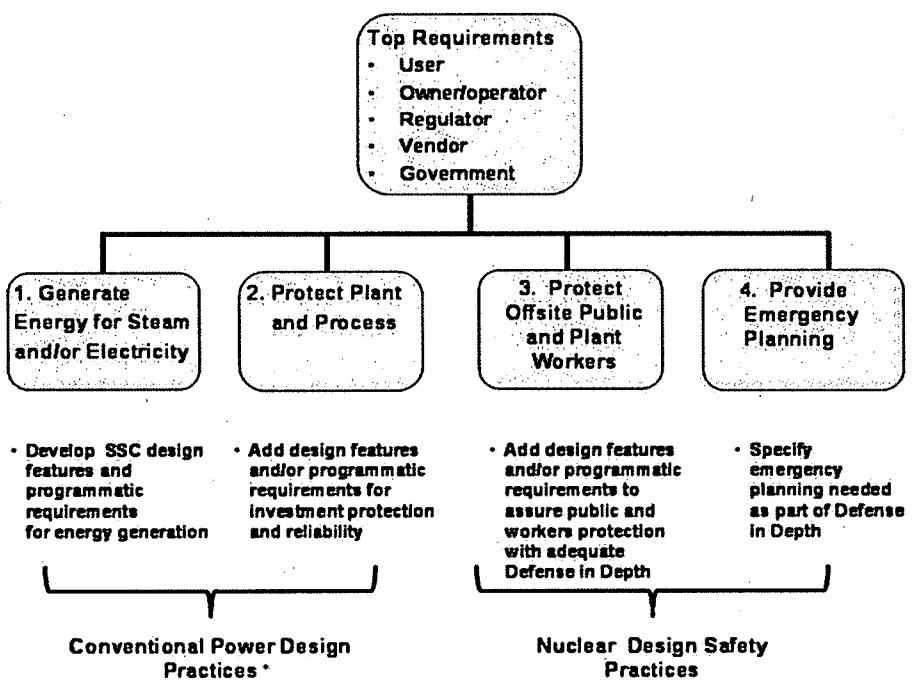
3. NGNP APPROACH TO DEFENSE-IN-DEPTH

One of the basic distinguishing objectives of nuclear plant design is the emphasis on providing reasonable assurance that radionuclides are controlled under virtually all conditions. Another prime objective is to reliably and economically operate the facility over its lifetime. To achieve the necessary level of assurance in meeting these objectives, the principle of defense-in-depth is applied throughout the plant life cycle, including design, construction, and operation. In order to demonstrate that the NGNP design will exhibit a sufficient level of defense-in-depth in the license application, it is first necessary to incorporate sufficient defense-in-depth capabilities in the plant design. Since defense-in-depth is an integral part of the design, the discussion of the approach to assuring adequate defense-in-depth begins with a description of the risk-informed and performance-based design process in Section 3.1, including an introduction to how the design process incorporates the risk insights that provide greater assurance of sufficient defense-in-depth in the management of radionuclides. With this perspective background, the definition of defense-in-depth adopted for the NGNP Project is expanded in Section 3.2. How this definition is applied is described in Section 3.3. Section 3.4 summarizes a process for demonstrating that the license application for the NGNP facility will exhibit a sufficient and adequate level of defense-in-depth.

3.1 Risk-Informed and Performance-Based Design Process

3.1.1 Design Process Overview

Figure 3-1 shows a simplified overview of the fundamental design considerations that are woven together in a power plant project. All power plant project designs begin the same way, with an understanding of the top level requirements for the project. These are derived from the user, owner, operator, regulators, vendors, and other government parties that have an interest in the project.



* Includes consideration of 3 and 4 if non-nuclear hazards exist.

Figure 3-1. Major elements of the NGNP design approach.

Public interests are reflected through the regulatory and government requirements and constraints on the project. These requirements address topics like output levels, fuel, siting, economics, schedule, availability, operations and maintenance, investment protection, and environmental goals. Once these top level requirements are established to the satisfaction of the owner, the design process begins in earnest. It begins in a manner that is essentially the same for all types of projects, following proven industry practices and procedures developed over the decades. The first step is selecting the basic design features: heat source and power conversion systems, building arrangements and operational modes, and states to fulfill product requirements. Once these features are selected, the design is further developed to add other features that assure adequate availability, reliability, and investment protection. These are conventional power plant practices. If a nuclear heat supply system is chosen, the design also includes special considerations to protect the offsite public and onsite workers from radioactive materials. These additional features include preventive and mitigative features established with the defense-in-depth principle in mind. The selection of a nuclear heat supply system also requires special siting considerations associated with radionuclide control, which also assures the ability to execute emergency planning actions in the unlikely event of a radiological release. The choice of a site and the inclusion of an emergency planning capability are part of the defense-in-depth strategy for nuclear plant projects. The design process also incorporates probabilistic risk assessment techniques as part of the strategy to assure adequate protection of the public and workers.

The NGNP facility is being designed with the risk-informed and performance-based design process characterized in Figure 3-2. This process is referred to as *risk-informed* because it is based on a foundation of deterministic requirements, decisions, and evaluations, and makes use of risk insights from a PRA. These insights further refine design decisions and contribute, beyond single failure analysis, to the deterministic selections of design basis accidents (DBAs), confirmation of necessary functionality, the related safety classification of SSCs, and the addition or refinement of special treatments applied to SSCs or programmatic features in the plant. The process is referred to as performance-based[c,d] because it builds from the top level requirements or "What" must be done and cascades the design decisions through a set of stages where it is determined "When" certain functionality must be available, "How" that function is achieved, and, as addressed in this paper, "How Well" the functionality of the plant meets the top level requirements. In the course of making design selections, uncertainties about SSC performance or functionality requirements may exist. For the NGNP design, new technology or technology with limited

---

c. In its Strategic Plan, NUREG-1614, the NRC defines performance-based as "...an approach to regulatory practice that establishes performance and results as the primary bases for decision making. Performance-based regulations have the following attributes: (1) measurable, calculable or objectively observable parameters exist or can be developed to monitor performance; (2) objective criteria exist or can be developed to assess performance; (3) licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes; and (4) a framework exists or can be developed in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern."

d. In their review of the PBMR US Design Certification white paper on defense-in-depth, the NRC staff requested in RAI DID-6 an identification of performance criteria other than site boundary dose that support defense-in-depth. The availability of a PRA early in the design process allows more detailed examination of single point or common mode vulnerabilities along with the consequences of their occurrence. This provides additional assurance that there are no single features of design, construction, operation, or maintenance whose failure would threaten public safety. The NGNP approach to special treatment is based on establishing the required degree of capability and reliability for SSCs in the prevention and mitigation of event sequences. It is expected that intermediate design performance or reliability metrics will be used to establish the special treatment requirements. Examples of such metrics would include component and system level reliability and availability targets that are derived from the results of the PRA in comparison with the TLRC. The approach being developed by the American Society of Mechanical Engineers (ASME) Special Working Group on HTGRs under Section XI is developing requirements for in-service inspection of helium pressure boundary (HPB) SSCs that are based in part on component level reliability targets. The general principles that have been applied to address the NRC Maintenance Rule to develop plant and component level reliability and availability targets would serve as good examples of how such individual performance metrics can be developed.

operating history is also being used to achieve the project objectives. This introduces the need for some technology development to address uncertainties or to validate assumptions about SSCs or operating conditions in the plant. Figure 3-2 illustrates how the technology development process fits within the overall design process and how the use of risk techniques is integrated into the design process.

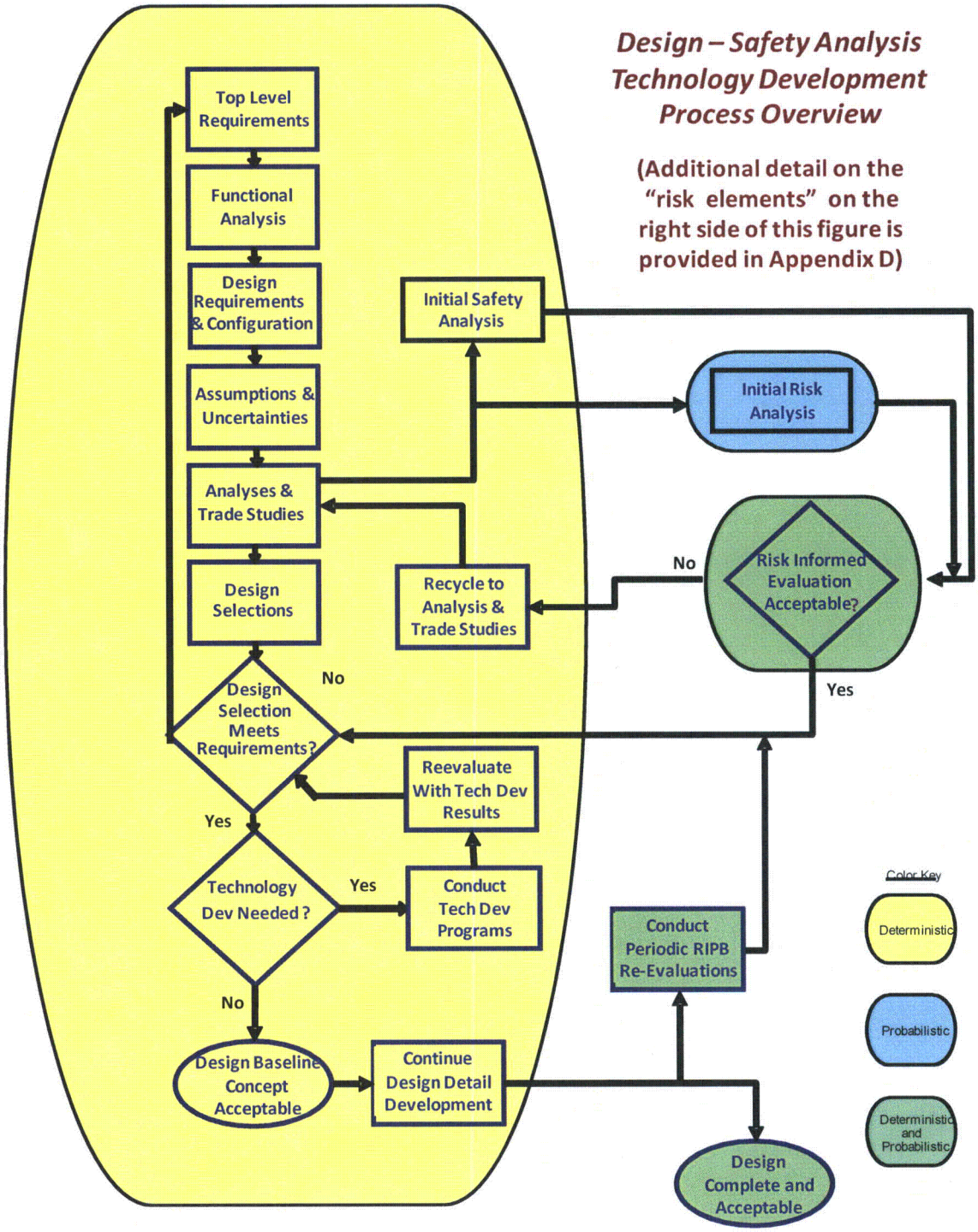


Figure 3-2. Design—safety analysis—technology development overview.

The NGNP Project is integrating the development of PRAs into the design process at an early stage when basic flow diagrams and functional relationships are being created. The purpose for early application of this engineering tool is to supplement conventional codes, standards, practices and conventions with a rigorous methodology that is intended to explore and identify interdependencies, better understand safety margins, quantify uncertainties, and apply more systematic adjustments to the design than can be done without the use of this process. Risk-informing the design enriches the engineering decisions for SSC configuration and equipment selection by providing different types of feedback on the more complicated events that could pose a risk to the public. In this way, it supplements traditional design and licensing practices by focusing on the truly important risk issues and assist in making practical engineering decisions to complete the design. The process shown in Figure 3-2 is highly iterative during the life cycle of the design, and sets the foundation for the continued use of risk insights in the operation, maintenance, and modification activities that follow construction.

3.1.2 Summary of Risk-Informed and Performance-Based Design Process

Defense-in-depth considerations are an integral part of the NGNP design process. Defense-in-depth is "built in" by first applying the rigorous and proven systems engineering and discipline engineering practices, procedures, industry codes and standards, and company methods to address the top level requirements for any project. This includes the appropriate application of engineering judgment to make assumptions about plant physical capabilities, operator performance, or other topics and to select design features that compensate for imperfect knowledge.

The NGNP design process supplements the conventional design process by the early integration of the use of probabilistic risk analysis that provides insights regarding functional reliability, performance uncertainty and margins in order to assist the designer in the selection of SSCs as well as programmatic actions that further increase the assurance of plant safety and performance. With the introduction of a risk informed and performance based element in the design process, designers (and regulators) can objectively assess whether there is adequate defense-in-depth in the protective and mitigative safety features of the design. This process provides greater assurance that there are no complex, undesirable event sequences that could be a safety threat. The inclusion of the risk informed and performance based evaluations also provide a solid foundation to support the operational phase of the plant's life cycle.

The details of how the design process incorporates risk methods and insights into the design are described in the remaining sections of this paper, including Appendix D.

3.2 NGNP Defense-in-Depth Framework

Section 2.3 summarized NRC's statements on defense-in-depth from which the various attributes or elements of a defense-in-depth strategy can be defined. This section clarifies the terms (derived primarily through the use of LWR concepts) necessary to apply these concepts to the NGNP facility.

NRC's Strategic Plan[12] provides a glossary of terms useful to the defense-in-depth strategy development. These terms, whose full definition is included in Appendix A, Section A.2, include:

> *Defense-in-Depth: an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility.....*
>
> *Performance-Based: an approach to regulatory practice that establishes performance and results as the primary bases for decision-making....*
>
> *Regulatory Framework: several interrelated aspects such as (1) the NRC's mandate from the Congress..., (2) the NRC's licenses, orders, and regulations..., (3) regulatory guides,*

review plans,..., (4) the licensing and inspection procedures ..., and (5) enforcement guidance.

Risk Assessment: a systematic method for addressing the three questions as they relate to the performance of a particular system, including the human component— "What can go wrong?" "How likely is it?" and, "What are the consequences?"

Risk Insights: the results and findings that come from risk assessments....

Risk-Informed: an approach to decision making in which risk insights are considered along with other factors such as engineering judgment,...

3.2.1 Overview

Defense-in-depth is an established safety philosophy in which multiple lines of defense, safety margins, and compensatory measures are applied to the design, construction, operation, maintenance, and regulation of nuclear plants to prevent and to mitigate accidents and to assure that the adequate protection of public health and safety. Each of the definitions summarized above brings out a different facet of this important safety philosophy. These definitions are regarded as applicable to the NGNP Project, but some interpretation of the details in these definitions is necessary (as noted in the introduction to Section 2). For example, the strategy of balancing prevention and mitigation of core damage has to be generalized somewhat before it can be meaningfully applied to an HTGR design. In addition, a large fraction of the regulatory history on this topic is written from the point of view of the regulator. However, the plant designer implements defense-in-depth to not only meet regulatory requirements, but also "investment protection" and reliable performance goals, which almost always results in designs that have more safety margin than necessary to meet the regulatory standard of adequate protection. It is therefore appropriate that the NGNP Project's approach to defining and evaluating defense-in-depth be clearly described.

The NGNP Project has adopted a risk-informed and performance-based framework for defense-in-depth (depicted in Figure 3-3) that is consistent with the NRC requirements and guidance statements. This approach recognizes three major elements: ***Plant Capability Defense-in-Depth***, ***Programmatic Defense-in-Depth***, and ***Risk-Informed Evaluation*** of defense-in-depth. This framework, used to define defense-in-depth interpretations, incorporates the concepts identified in previously published definitions of defense-in-depth with clarifications that are necessary in order to apply these concepts to the NGNP Project. An attempt is made to define the framework in a technology neutral manner so that the evaluation of the defense-in-depth's adequacy can be as objective as possible. This approach to defining defense-in-depth should be regarded as a means of capturing the established principles, rather than introducing new ones.

Recognizing these three elements enables the examination of defense-in-depth from different perspectives including those of:

- Designing the plant and specifying the capabilities of its SSCs in the performance of safety functions
- Defining the programs to ensure that the as-designed plant will be built and will operate safely throughout its lifetime and in a manner that preserves the defense-in-depth capabilities intended in the design
- Evaluating how the plant performs its safety functions in the prevention and mitigation of accidents in the context of a risk-informed and performance-based process in order to determine the adequacy and sufficiency of defense-in-depth.

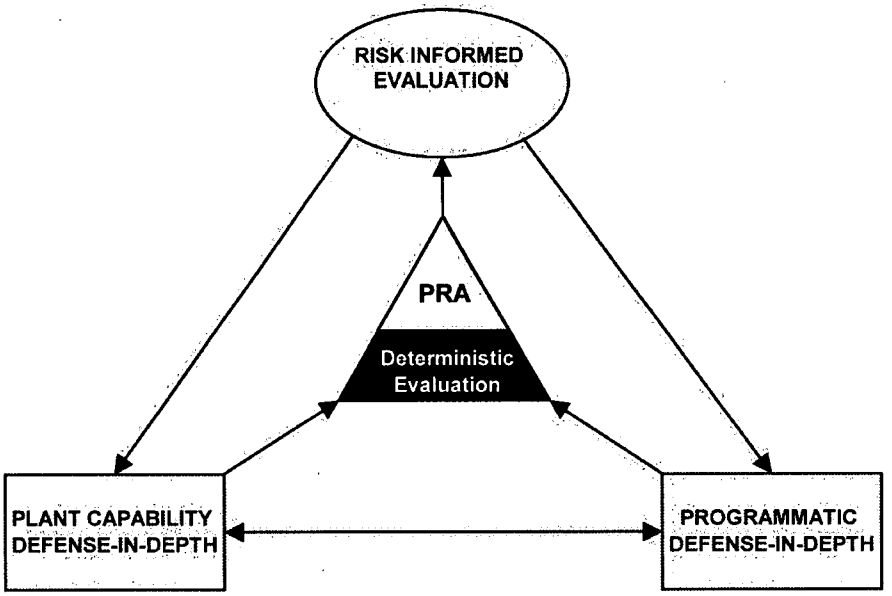


Figure 3-3. Elements of the defense-in-depth framework.

It is recognized that these elements of defense-in-depth are not exclusive, but rather represent complementary and overlapping perspectives from which to apply the same underlying defense-in-depth principles.

The current definitions and concepts of defense-in-depth have evolved over a long period of time in designing and regulating the current fleet of LWRs and have been modified in recent years to reflect the changes in philosophy brought about by risk-informed and performance-based regulation. As noted above, while the NRC definitions of defense-in-depth have evolved, clarifications are still required to make the definition applicable to the NGNP Project. The reason for having three major elements of defense-in-depth is to organize the means to address the underlying principles based on the definition of defense-in-depth with the clarifications discussed above. These elements recognize that defense-in-depth principles are applied in many areas of plant design, procurement, manufacturing, construction, operation, and regulation.

Plant Capability Defense-in-Depth reflects the decisions made by the designer to incorporate defense-in-depth into the functional capability of the physical plant. These decisions include the use of multiple lines of defense and conservative design approaches for the barriers and SSCs performing safety functions associated with the prevention and mitigation of accidents. ***Plant Capability Defense-in-Depth*** also includes the use of multiple barriers, diverse and redundant means to perform safety functions to protect the barriers, conservative design principles and safety margins, site selection, and other physical and tangible elements of the design that use multiple lines of defense and conservative design approaches to protect the public. For small reactors where economies of scale are not a primary economic opportunity, the design places a greater emphasis on prevention through inherent and passive features to reduce the dependence on active systems, thereby creating both safety value and economic value, without sacrificing defense-in-depth capability.

Programmatic Defense-in-Depth reflects the programmatic actions for designing, constructing, operating, testing, maintaining, and inspecting the plant so that there is a greater degree of assurance that the defense-in-depth factored into the plant capabilities during the design stage is maintained throughout the life of the plant.

Risk-Informed Evaluation of defense-in-depth is the structured use of information provided by the PRA to: identify the roles of SSCs in the prevention and mitigation of accidents, identify and evaluate uncertainties in the PRA results, devise deterministic approaches to address these uncertainties, and guide and provide risk insights to support deterministic judgments on the adequacy and sufficiency of defense-in-depth. The event scenario models developed in the PRA provide an objective means of defining the roles that SSCs play in the prevention and mitigation of accidents.

An important aspect of the ***Risk-Informed Evaluation*** of defense-in-depth is a logical process for deciding the adequacy and sufficiency of the defense-in-depth reflected in the plant capabilities and assurance programs. Important feedback loops are shown in Figure 3-3 that represent the incorporation of risk insights into the development and enhancement of the plant capabilities and programs as the design and program developments evolve.

Each of these elements of defense-in-depth is supported by a comprehensive PRA and a parallel set of deterministic evaluations that are performed to ensure that all decision making in these processes is systematically evaluated in a comprehensive risk-informed manner. The PRA is based on plant design, extensive deterministic bases, and a specification of the capabilities of the plant SSCs in the performance of their functions, including the plant safety functions. The results of the PRA expose the characteristics of the ***Plant Capability Defense-in-Depth*** and are dependent on the safety margin and reliability of each SSC modeled in the PRA. The reliability of the SSCs responsible for the ***Plant Capability Defense-in-Depth*** is assured by their design and by the elements of ***Programmatic Defense-in-Depth***. The PRA and the parallel deterministic evaluations are shown separate from the defense-in-depth elements in Figure 3-3 because information from these probabilistic and deterministic evaluations is used to support the design, provide input to the formulation of process requirements, and provide information to evaluate the adequacy and sufficiency of the defense-in-depth strategies. Conversely, the PRA and the parallel deterministic evaluations include models of the plant capabilities and how the plant is operated and maintained under the programmatic controls, as part of the modeling and quantification of the scenarios. The PRA provides critical input to the identification and evaluation of the uncertainties that are addressed in the ***Plant Capability*** and ***Programmatic Defense-in-Depth*** elements. Hence the PRA and the parallel deterministic evaluations are utilized in all elements of the defense-in-depth approach.

The defense-in-depth evaluation process includes several performance-based steps. First, an objective perspective on the adequacy and sufficiency of defense-in-depth is provided by comparing the frequencies and consequences of the LBEs and their uncertainties against the F-C Curve. Second, the plant capabilities include capabilities to monitor the plant performance against a set of parameters that confirm the safety operation of the plant. Third, the process of SSC safety classification and the definition of special treatment requirements provide an objective basis for monitoring the reliability and availability of the SSCs responsible for implementing safety functions. The level of special treatment applied to assure adequate reliability and capability of SSCs is commensurate with their risk significance.

A more detailed definition of the elements of the approach to defense-in-depth is provided in Figure 3-4 and in the following sections.

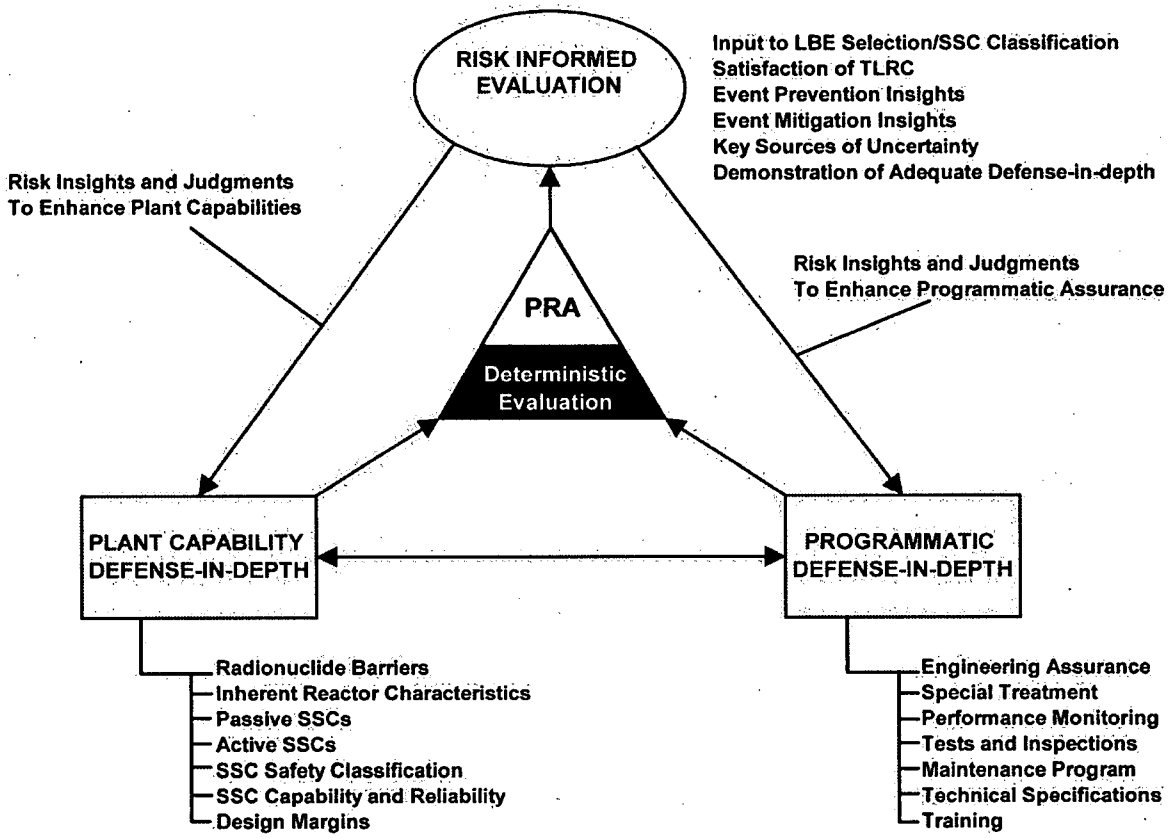


Figure 3-4. Detailed elements of defense-in-depth framework.

3.2.2 Plant Capability Defense-in-Depth

Plant Capability Defense-in-Depth refers to the use of multiple lines of defense and conservative design approaches in the design of structures, systems, and components (SSCs) that perform safety functions in a nuclear power plant. These lines of defense include inherent fuel and reactor characteristics, multiple barriers, and engineered features and SSCs whose safety functions serve to protect the integrity of these barriers. Barriers have two roles: that of preventing and mitigating radionuclide transport during normal operation, transients, and accidents, and that of protecting the plant and its SSCs performing safety functions from external hazards. The barriers include fuel design and physical barriers and associated safety systems and structures that prevent or block the movement of radionuclides, as well as intentional time delays in the transport that allow for the radioactive decay and deposition of radionuclides prior to their release to the environment. This important time delay element allows for effective implementation of emergency protective actions. The barriers also include siting considerations for both limiting public exposures and protecting the plant from external hazards.

Conservative design approaches that are used to provide ***Plant Capability Defense-in-Depth*** include the selection of inherent features and passive SSCs as a first line of defense in the performance of safety functions, and the use of conservative design margins to improve the capability of SSCs to withstand challenges that may exhibit uncertainties.

Conservative design approaches include the strategy of placing priority on the use of inherent features and passive SSCs to perform the safety functions, by providing additional active SSCs to provide

defense-in-depth in the performance of these functions, and to incorporate robust design margins to reduce the uncertainty in the capability of these passive and active SSCs to perform their roles in the prevention and mitigation of accidents. Conservatism is also employed in the design strategies to enhance the capability and reliability of barriers in the prevention and mitigation of accidents. Such strategies include:

- Multiple barriers to radionuclide release for each source of radioactive inventory
- Robust design of each barrier to be capable of mitigating expected failure modes of other barriers
- Concentric arrangement of the multiple barriers to enhance independence
- Application of conservative design margins to establish the capability and capacity of each barrier and to address uncertainties
- Selection of a power conversion cycle that minimizes the potential for pressurization induced breaches of the helium pressure boundary.

Conservatism is also applied in the design strategies to enhance the capability and reliability of SSCs performing safety functions that protect the integrity of the barriers. Examples of such strategies include:

- Diverse means of fulfilling required safety functions using combinations of inherent characteristics, passive SSCs, and active SSCs
- Design requirements to maintain independence between functionally redundant means of fulfilling required safety functions
- Use of diversity and redundancy to achieve the necessary degree of reliability and capability for the passive and active SSCs performing safety functions
- Application of conservative design margins to establish the capability and capacity of each SSC and to assure a high degree of reliability in light of uncertainties.

Conservatism is also applied in the detailed design decisions to ensure the adequate capacity of normal operational systems, barriers, and engineered features meeting requirements set in ***Plant Capability Defense-In-Depth***. Such decisions occur in the following aspects of the design process:

- Selection of design codes and standards
- Establishing design margin for:
  - Normal operating margins for reliable operations
  - Investment protection
  - Allowances for wear and performance degradation
  - Maintenance during operations and shutdown
- Specifying additional control and monitoring equipment for:
  - Identifying off-normal conditions or incipient failures
  - Monitoring against performance requirements
- Capability to meet conservative safety assessment performance requirements such as:
  - Selection of safety-related SSCs
  - Safety analysis with deterministic conditions using safety related SSCs
  - Safety margins from deterministic safety evaluations including uncertainties.

A fundamental starting point for many of the historical definitions of defense-in-depth is the concept of multiple barriers to radionuclide transport. In this concept, a set of multiple physical barriers is introduced between the hazard (the inventory of radioactive material in the reactor) and the environment. This concept applies to existing and advanced reactors. This concept for the NGNP Project, as shown in Figure 3-5, consists of fuel particle coatings, a reactor coolant system pressure boundary, and a reactor building barrier (e.g., containment or confinement) representing the last barrier to an environmental release. Provisions for siting the reactor at a distance in relation to the surrounding population are also included as a fourth barrier as illustrated in the figure. When the barriers are concentric a higher degree of independence among the barriers can be assured as barrier bypass pathways are minimized. In this case any scenario involving a release from the fuel to the public must involve failure or degradation of all the barriers.

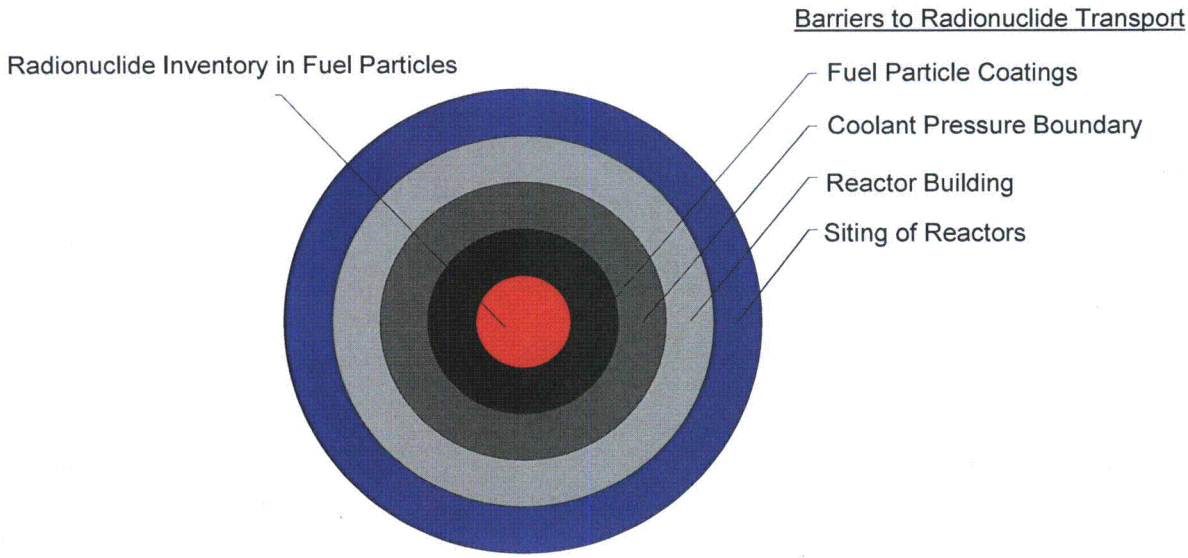


Figure 3-5. Barriers to radionuclide transport included in plant capability defense-in-depth.

Barriers used in ***Plant Capability Defense-in-Depth*** need to be concentric and independent so that the failure of one barrier does not adversely impact the effectiveness of another. An important insight from PRAs is the fact that when these barriers are not fully concentric, risk significant accident sequences associated with bypass of a barrier may result. Another insight is that the extent to which independence between the barriers can be assured is largely determined by the interactions between the inherent characteristics of the reactors and the barriers themselves during potential accident sequences. The use of barriers as part of ***Plant Capability Defense-in-Depth*** is most effective when the barriers are concentric and when the postulated failure modes of one barrier do not lead to the likely failure of another barrier or to significant increases in the probability of failure of that barrier. Full independence among barriers may not be feasible for any reactor concept, but the extent of independence is an important attribute to consider in evaluating the adequacy of defense-in-depth. As illustrated in Figure 3-6, the elements of the safety design approach for the reactor provide a starting point for developing the ***Plant Capability Defense-in-Depth***.

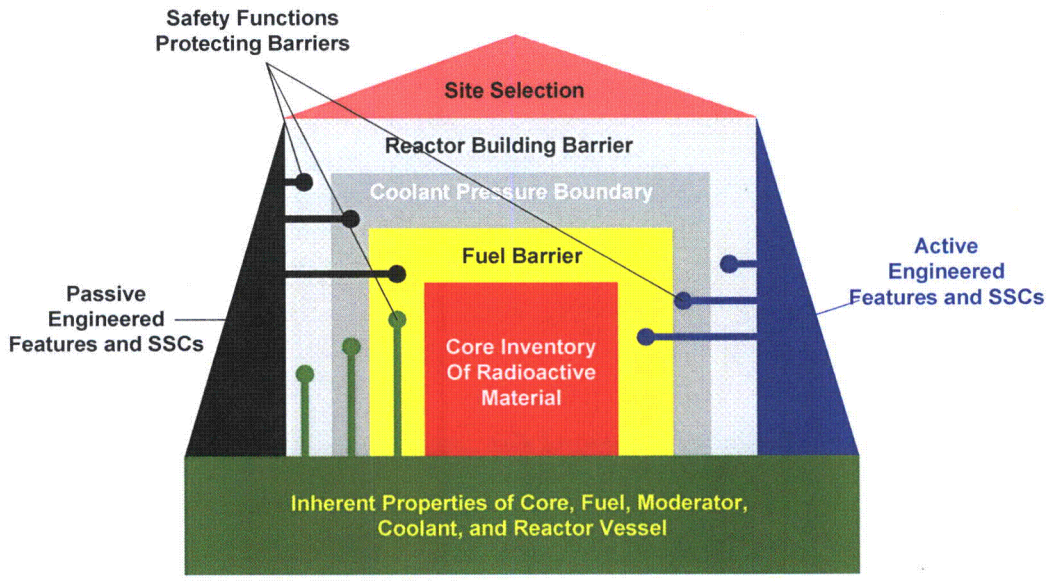


Figure 3-6. Elements of safety design approach incorporated into ***Plant Capability Defense-in-Depth***.

The safety design approach utilizes the inherent features and characteristics of the reactor defined by the selection of materials and basic design aspects of the reactor core and associated fuel elements, the selection of materials and basic design aspects of the moderator (in the case of advanced thermal reactors), and the selection of the reactor coolant. These reactor characteristics are inherent to the reactor concept and provide the foundation for the safety case by contributing to the integrity of the radionuclide barriers directly, by dictating the requirements for engineered features that are provided to support barrier integrity, or by a combination of these. Such features also dictate the time available to implement emergency measures such as accident management and offsite protective actions. For any reactor concept, its safety is determined by the combination of inherent and engineered features and how these features interact to prevent and to mitigate accidents that may challenge the integrity of the barriers to radionuclide release.

Once the inherent safety features are defined, the safety functions that must be satisfied to achieve safe sequence end states and to protect the radionuclide barriers can be determined. While there are different approaches to defining safety functions, one approach that seems to fit all reactors is to define the safety functions as those necessary to protect the integrity of one or more barriers. Different inherent features of the reactors will necessarily lead to sets of different minimum safety functions that need to be supported to protect the barriers, thereby achieving a given level of safety. For example, coolant inventory control is an essential safety function for light water reactors, as failure to control inventory would lead to core damage and large releases from the fuel. By contrast, for HTGRs, coolant inventory control, while necessary to produce electric power, is not required to protect the integrity of the fuel. In modular HTGRs, the safety significance of the helium pressure boundary is not to primarily control the helium inventory, but rather to provide a barrier to fission product release and protect against chemical attack, regardless of the helium inventory level. The fundamental safety functions for all reactors are those necessary and sufficient to protect the radionuclide transport barriers. The specific safety functions required to accomplish this are reactor specific and determined by the properties of the inherent features and other key elements of the safety design approach.

Both passive and active strategies need to be considered in the design of the engineered features used to support each safety function. It is generally accepted that passive safety features, such as negative temperature coefficient of reactivity and passive means of heat removal, are more reliable than systems

requiring the operation of active components, so long as the material condition of the components and structures that perform the passive functions are adequately maintained. The need and importance of any engineered active features is evident once the inherent and engineered passive features are understood.

An important element of ***Plant Capability Defense-in-Depth*** is the decision to use the PRA as a tool to support design decisions and to optimize the allocation of resources that are applied in the design to prevent and mitigate accidents. As explained previously, this is an iterative process that provides an opportunity for the use of risk insights into the safety design philosophy and to develop understanding of how the defense-in-depth principles have been applied at an early stage of the design.

So, in summary, ***Plant Capability Defense-in-Depth*** is comprised of the use of multiple diverse and independent barriers between the radioactivity hazard and the environment, and conservative design strategies to ensure the integrity of the barriers under normal and accident conditions. These design strategies include the selection of inherent features, the use of concentric and independent barriers, and additional engineered features to provide each reactor specific safety function. Engineered features include passive features such as the barriers themselves and, where appropriate, additional active safety systems to support the integrity of the barriers. It is important to note the explicit representation of the inherent safety features of the reactor because they provide the foundation for the design of the barriers, dictate what safety functions must be provided to support these barriers, and dictate options available to use passive rather than active safety systems to support these functions. This characterization makes it possible, at least in principle, to objectively assess defense-in-depth strategies employed in a reactor design in the context of its inherent characteristics.

The major elements of ***Plant Capability Defense-in-Depth*** are listed in Table 3-1. In contrast with the definitions of defense-in-depth reviewed in Section 2, this definition includes explicit consideration of inherent features that play an important role in the performance of safety functions and the delineation of engineered safety functions into those features that employ active and passive design principles. The intent of this definition of ***Plant Capability Defense-in-Depth*** is to capture all the lines of defense that are implemented by the designer to ensure safe operation of the plant. The strategies of conservative design approaches, redundancy, diversity, and independence of the barriers and SSCs performing safety functions are part of the available tools to assure that SSCs serving as barriers and performing safety functions have the adequate reliability and capability to perform these functions.

3.2.3 Programmatic Defense-in-Depth

Programmatic Defense-in-Depth refers to the use of multiple lines of defense in the programs that are put into place to ensure that SSCs responsible for performing safety functions have adequate reliability and capability, to provide protection against uncertainties in plant design and operation, and to support effective implementation of emergency management. These programs include the special treatment requirements for safety classified SSCs, tests and inspections, monitoring of plant and SSC performance, and oversight.

The approach focuses on the license application related aspects of ***Programmatic Defense-in-Depth*** by the application of conservative safety margins and deterministic elements in each step of the risk-informed and performance-based licensing approach, including the definition of the F-C Curve, selection of LBEs, safety classification of SSCs, and formulation of special treatment requirements for the safety classified SSCs.

In general, the sequences in the PRA lay out a set of event sequences which are organized into event sequence families for the definition of LBEs. The process for organizing and grouping the event sequences into event sequence families and LBEs uses conservative assumptions to ensure that the selected LBE conditions bound the set of event sequences assigned to the LBE.

Table 3-1. Elements of ***Plant Capability Defense-in-Depth***.

- Inherent features of reactor important to safety:
  - Fundamental properties of core/fuel elements
  - Fundamental properties of reactor coolant
  - Fundamental properties of moderator
  - Fundamental properties of reactor vessel
  - Extended time available to implement transient and emergency measures.
- Use of multiple barriers to prevent release and protect SSCs from external hazards:
  - Fuel barrier design features
  - Coolant pressure boundary design features
  - Suitable barriers for spent fuel storage
  - Reactor building barrier design features
  - Independence and concentricity of barriers.
- Selection of robust systems for normal operation and expected transients:
  - Redundant and diverse features for start-up, shutdown, and anticipated transients
  - Operational control systems for reliable plant operation
  - Investment protection features.
- Engineered features to protect barrier integrity:
  - Reactor specific safety functions to protect barriers
  - Passive engineered SSCs to perform safety functions
  - Active engineered SSCs to perform safety functions
  - Operator actions needed to implement safety functions.
- Conservative design approaches to improve the reliability and capability of SSCs performing safety functions:
  - Use of inherent characteristics to perform safety functions
  - Use of passive SSCs
  - Conservative design margins
  - Redundancy where active SSCs are employed to perform safety functions
  - Diversity and independence among functionally redundant SSCs that perform safety functions.
- Selection of appropriate reactor sites.
- Time available to implement emergency measures.

When the frequencies and consequences for each LBE are compared against the F-C Curve, the associated uncertainties are included. Hence, the resulting classification of each LBE as an anticipated operational occurrence (AOO), design basis event (DBE), or beyond design basis event (BDBE) inherently accounts for the uncertainties. The dose criteria embodied in the TLRC and the F-C Curve are much lower than the surrogate dose criterion commonly associated with the NRC Safety Goal Quantitative Health Objective (QHO) for individual risk of prompt fatality. Therefore, experience has shown that designs which meet the TLRC and include appropriate design and analysis margins and defense-in-depth also meet the Safety Goal policy surrogates, often by orders of magnitude.[20] Additional conservatism is introduced by the requirement to demonstrate that each deterministically selected DBA can be sufficiently mitigated with only the safety-related SSCs being credited. Finally, there are safety margins and conservative assumptions applied in the assignment of special treatment requirements for safety classified SSCs to assure that they have sufficient reliability and capability to perform their safety functions.

The ***Programmatic Defense-in-Depth*** element includes those steps taken to assure that the ***Plant Capability Defense-in-Depth*** as influenced by the ***Programmatic Defense-in-Depth*** is realized in the final plant. The programs include design reviews, operator training and practices, emergency operating procedures and their implementation, establishment and implementation of accident management

guidelines, development of and adherence to technical specifications, maintenance practices, owner implemented nuclear safety oversight, quality assurance, and evaluation of operating experience to assure adequate and timely correction of any deficiency identified, and the full implementation of a corrective action program.

The key elements of ***Programmatic Defense-in-Depth*** are listed in Table 3-2. The bases for the specific requirements are derived from ***Risk-Informed Evaluation*** of defense-in-depth, as described below. A major goal of this review is to work out the specific expectations for establishing the proper level of ***Programmatic Defense-in-Depth*** for the NGNP design. These expectations will need to be developed in the context of the NGNP Project's approach to using the PRA, selecting LBEs, safety classifying SSCs, and deriving special treatment requirements for SSCs.[e,f]

As discussed more fully in Section 3.1, defense-in-depth is an integral part of the NGNP design process and is introduced at an early stage. It is not feasible to put those elements that are only performed to meet requirements into one bin and those elements that only have a defense-in-depth role in another bin. Any element of defense-in-depth serves a role in preventing or mitigating accidents, or in reducing the uncertainties identified in the probabilistic and deterministic evaluations. By accomplishing this, such elements also contribute to meeting the requirements.

3.2.4 Risk-Informed Evaluation of Defense-in-Depth

3.2.4.1 Scope of Risk-Informed Evaluation

Risk-Informed Evaluation of defense-in-depth refers to the multiple lines of defense reflected in the definition of scenarios that form the basis of the deterministic and probabilistic safety evaluations that will be performed to support the NGNP licensing application. The structure of these scenarios, in a manner that permits the identification of prevention and mitigation measures, assures that the strategies of ***Plant Capability Defense-in-Depth*** and ***Programmatic Defense-in-Depth*** have been adequately implemented. The strategies for preventing and mitigating accidents are identified and evaluated in ***Risk-Informed Evaluation*** of defense-in-depth based in part on a review of the PRA, whose results have been structured to identify the roles of SSCs in preventing and mitigating accidents. Prevention and mitigation strategies for the NGNP Project are defined somewhat more broadly than for currently licensed reactors, which focus on preventing and mitigating core damage. In the case of the NGNP Project, prevention and mitigation are defined with respect to limiting the release of significant amounts of radioactive material as a result of event sequences that could occur with this design.[g]

---

e In their review of the PBMR US Design Certification white paper on Defense-in-Depth [Ref. 5], the NRC staff questioned in RAI DID-1 how the selection of codes and standards would be classified between ***Plant Capability Defense-In-Depth*** and ***Programmatic Defense-in-Depth***. In the NGNP approach to defense-in-depth, the selection of design codes is part of ***Plant Capability Defense-In-Depth***. However, codes and standards that address tests, inspections, maintenance, repair and replacement, engineering assurance, and other activities that are done to assure that the plant capabilities assumed in the designed are put in place and maintained over the life of the plant are part of ***Programmatic Defense-in-Depth***.

f In their review of the PBMR US Design Certification white paper on Defense-in-Depth [Ref. 5], the NRC Staff noted in RAI DID-4 that the PBMR approach to identifying contributions to defense-in-depth incorporated practically all good engineering practices that were classified as such. The staff questioned why specific measures, which were only performed to support defense-in-depth beyond just meeting the requirements, were not separated out. The approach proposed for NGNP does not attempt to separate good practices that are needed for defense-in-depth in meeting performance and safety requirements from those that are needed to assure that specific safety and design criteria are met. The approach recognizes the importance of understanding the safety role of all SSCs, all special treatments, and the role of all engineering, manufacturing, construction, testing, operations, and maintenance activities to assure adequate protection of the public. It is also recognized that these same design characteristics and activities contribute to meeting plant performance, economics, and reliability goals.

g. For HTGR designs, including the NGNP, no appreciable core damage is expected to occur for any DBE or BDBE.

Table 3-2. Elements of ***Programmatic Defense-in-Depth***.

- Engineering assurance programs:
  - Special treatment requirements
  - Independent design reviews
  - Separate effects tests.
- Organizational and human factors programs:
  - Training and qualification of personnel
  - Emergency operating procedures
  - Accident management guidelines.
- Technical specifications:
  - Limiting conditions for operation
  - Surveillance testing requirements
  - Allowable outage (completion) times.
- Plant construction and start-up programs:
  - Equipment fabrication
  - Construction
  - Factory testing and qualification
  - Start-up testing.
- Maintenance and monitoring of SSC performance programs.
  - Operation
  - In-service testing
  - In-service inspection
  - Maintenance of SSCs
  - Monitoring of performance against performance indicators.
- Quality assurance program:
  - Inspections and audits
  - Procurement
  - Independent reviews
  - Software verification and validation.
- Corrective action programs:
  - Event trending
  - Cause analysis
  - Closure effectiveness.
- Emergency Planning.

Prevention strategies are defined as those strategies employed to reduce the frequency of accidents by improving the reliability of SSCs whose failure would cause initiating events and/or adversely affect the ability to mitigate an event sequence. Mitigation strategies are those employed to improve the capability of SSCs that serve to mitigate the consequences of events and event sequences that may challenge them. Hence, prevention and mitigation are directly correlated to the reliability and capability of the SSCs responsible for providing the ***Plant Capability Defense-in-Depth***. Evaluating the prevention and mitigation effectiveness of SSCs in the probabilistic and deterministic safety analysis is the domain of the ***Risk-Informed Evaluation*** of defense-in-depth.

Risk-Informed Evaluation of defense-in-depth reflects the evaluation of all plant SSCs to manage daily operational activities, transients, and accidents, including the evaluation of strategies of accident prevention and mitigation. This element of the approach to defense-in-depth provides the best estimate of plant performance for deterministic and probabilistic safety evaluations, and thereby helps determine how well various prevention and mitigation strategies have been implemented. This provides a risk-informed framework to delineate the scenarios that the plant design features could be exposed to, as well as a

framework for defining programs that contribute to defense-in-depth. The scenario framework used in this evaluation defines the challenges to the plant safety features to be included in the plant design basis and the scope of all deterministic and probabilistic safety evaluations. This framework is useful for incorporating information and insights from the PRA and formulating strategies that can be implemented in both the ***Plant Capability*** and ***Programmatic Defense-in-Depth*** elements.

3.2.4.2 Role of Deterministic and Probabilistic Approaches

This element of the defense-in-depth approach is referred to as risk-informed because it is comprised of both probabilistic and deterministic evaluations in demonstrating the adequacy of defense-in-depth. A set of deterministic principles, derived from the regulatory foundation in Section 2, is used to provide the criteria for the deterministic evaluation. The probabilistic aspect of this part of the approach is the systematic identification and evaluation of uncertainties that are exposed by the PRA and by the structured method of examining the PRA results.

3.2.4.3 Demonstrating Adequacy of Defense-in-Depth

A primary goal of the ***Risk-Informed Evaluation*** of defense-in-depth is to establish the adequacy and sufficiency of the application of defense-in-depth principles for licensing. The approach to addressing this challenge is defined by a set of defense-in-depth principles that were derived from the regulatory foundation reviewed in Section **2** and decision logic for applying these principles in evaluating the plant capabilities and programs that comprise the major elements of defense-in-depth. The defense-in-depth principles selected for use in this evaluation are derived from two sources: the defense-in-depth objectives from Chapter 19 of the SRP[18] and the advanced reactor design attributes from the NRC policy on Regulation of Advanced Nuclear Power Plants.[8] The former captures the approach to defense-in-depth being used for risk-informed evaluations of changes to currently licensed plants, whereas the latter reflect considerations for defining defense-in-depth strategies that are suitable for advanced reactors.

The defense-in-depth objectives from Chapter 19 of the SRP are listed in Table 3-3 together with an evaluation of how these objectives could be used to evaluate the NGNP design.[h] It is noted that the formulation of these SRP objectives, which were developed after the current fleet of reactors were licensed, reflects a safety design approach that relies on active engineered systems to perform the required safety functions for the design basis events.

---

h. In their review of the PBMR US Design Certification white paper on Defense-in-Depth [ref. 5], the NRC staff questioned in RAI DID-8 the use of SRP, Chapter 19 criteria as a basis for assessing defense-in-depth in new reactor designs. The NGNP approach to ***Risk-Informed Evaluation of Defense-in-Depth*** adopts these same principles. The NRC's point was that these criteria were developed to evaluate risk informed changes to the licensing basis for existing reactors rather than criteria for helping to decide whether a given reactor had sufficient defense-in-depth. However, the principles of risk-informed regulation outlined in Regulatory Guide 1.174,[10] including the principle of maintaining current levels of defense-in-depth and these SRP criteria, were listed as criteria to make sure that there was no reduction in the level of defense-in-depth. Upon review of the entire regulatory basis in Section 2 of this white paper, it is judged that the principles in Chapter 19 adequately cover all the principles identified in the regulatory basis. Finally, the defense-in-depth principles that have been derived from Chapter 19 criteria have been revised for application to a new design.

Table 3-3. Derivation of defense-in-depth principles from Standard Review Plan, Chapter 19.

Defense-in-Depth Objectives from SRP, Chapter 19 for Risk-Informed Evaluation of License Amendment Requests	Underlying Defense-in-Depth Principles for Evaluating the NGNP Design
1. The change does not result in a significant increase in the existing challenges to the integrity of the barriers.	The barriers to radionuclide release are sufficiently robust to withstand challenges identified for the design.
2. The proposal does not significantly change the failure probability of any individual barrier.	The failure probability of each barrier is acceptably low in response to identified challenges.
3. The proposal does not introduce new or additional failure dependencies among barriers that significantly increase the likelihood of failure compared to the existing conditions.	The multiple barriers to radionuclide release are designed, built, and maintained in a manner that minimizes dependencies. This implies that the frequency of events that may challenge the integrity of two or more barriers is acceptably low and that the postulated failure of one barrier should not significantly increase the failure probability of another barrier.
4. The overall redundancy and diversity among the barriers is sufficient to ensure compatibility with the risk acceptance guidelines.	The overall redundancy and diversity among the barriers is sufficient to ensure compatibility with the top level safety criteria.
5. A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and mitigation of consequences.	A reasonable balance is preserved between the prevention and mitigation of accidents involving the potential release of significant quantities of radioactive material.
6. The proposal avoids over-reliance on programmatic activities to compensate for weaknesses in plant design.	The safety design approach avoids over-reliance on programmatic activities to compensate for weaknesses in the plant design.
7. The proposed change preserves system redundancy, independence, and diversity commensurate with the expected frequency of challenges, consequences of failure of the system, and associated uncertainties.	The safety design approach provides for system redundancy, independence, and diversity commensurate with the expected frequency of challenges, consequences of failure of the system, and associated uncertainties.
8. The proposal preserves defenses against potential common cause failures and assesses the potential introduction of new common cause failure mechanisms.	The safety design approach provides adequate defenses against potential common cause failure mechanisms.
9. The proposed change does not degrade the independence of barriers.	The underlying defense-in-depth principle for this item is covered by item 3.
10. The proposed change preserves defenses against human errors.	The safety design approach evaluates the likelihood and consequences of human error and provides defenses against human errors that can lead to significant radioactive material release.
11. The proposal fulfils the intent of the General Design Criteria in Appendix A to 10 CFR Part 50.	The design meets the intent of the applicable General Design Criteria in Appendix A to 10 CFR 50 and the reactor specific regulatory design criteria derived from the risk-informed performance-based licensing approach.

Although this formulation is reasonable for the current fleet of plants, it does not explicitly address some key attributes of advanced reactor designs that are recognized in the advanced reactor policy statement. Such attributes include the use of inherent characteristics and passive approaches to accomplish safety functions, use of enhanced safety margins, designs with reduced complexity, and other approaches to reduce uncertainty and increase the level of confidence that safety criteria will be met. By factoring in the design attributes of the NRC Advanced Reactor Policy statement and organizing the principles according to the NGNP Project's approach to defense-in-depth outlined in the previous section, the defense-in-depth principles of Table 3-4 were developed. Table 3-4 combines the strengths of the two source documents and is restructured to better align with the NGNP Project approach to defense-in-depth.

One significant change in Table 3-4 in relation to the SRP objectives is that diversity and redundancy are applied not only to barriers and systems, but also to combinations of inherent characteristics, passive SSCs, and active SSCs that support safety functions. Also, consistent with the discussion in Chapter 19 of the SRP, the roles of safety margins and other conservative design approaches, such as the use of reliable SSCs to reduce the frequency of challenging the safety functions, are explicitly recognized. This formulation of the defense-in-depth criteria is appropriate for evaluating the NGNP design. An integral part of ***Risk-Informed Evaluation*** of defense-in-depth is to ensure that these principles are adequately applied in the plant capabilities and programs that comprise defense-in-depth. This is the set of defense-in-depth criteria that NGNP Project proposes to use in licensing.

A logical approach for evaluating the adequacy and sufficiency of defense-in-depth as part of the risk-informed evaluation is shown in Figure 3-7. The intent of this approach is to systematically ensure that the defense-in-depth principles of Table 3-4 have been adequately applied. The first step towards meeting these principles is to meet the frequency-dose requirements within the TLRC by meeting the criteria in the F-C Curve. This implies that the reliabilities and capabilities of the SSCs that are modeled in the LBEs are adequate to prevent the DBEs and BDBEs from migrating up into the more frequent LBE category, and are adequate to mitigate the consequences of the LBEs within the respective TLRC dose limits.

The next logical step in Figure 3-7 accomplishes the principle of achieving an appropriate level of prevention and mitigation by examining the PRA results in a structured way in order to provide an objective definition of what is meant by prevention and mitigation in the design and to identify the specific SSCs responsible for the prevention and mitigation of each LBE. This structured approach is summarized in the next section.

The next logical steps identify key safety margins and uncertainties by performing and reviewing the PRA and the deterministic safety analysis, which provide an important perspective for evaluating safety margins in the design and safety analysis and for evaluating the adequacy of programs that, together with the plant capabilities, will comprise the elements of an acceptable approach to defense-in-depth.

The final step in Figure 3-7 is the risk-informed evaluation of the adequacy of defense-in-depth, which is performed to ensure that the principles of Table 3-4 have been adequately applied. The main elements of the *Risk-Informed Evaluation* of defense-in-depth are summarized in Table 3-5.

An important element of the risk informed evaluation is to evaluate the cause and effect relationship between the programs that are included in the ***Programmatic Defense-in-Depth*** and the impact these programs will have on reducing the uncertainties, frequencies, or consequences of the LBEs in relation to the TLRC. Only proposed programs that make significant contributions to reducing uncertainties and enhancing plant capabilities with respect to the TLRC will be retained and implemented.

Table 3-4. Principles for establishing the adequacy of defense-in-depth.

- ***Plant Capability Defense-in-Depth Principles***

  The safety design approach shall provide multiple, robust barriers to radionuclide release. (SRP Principles 1 and 2 in Table 3-3).

  The barriers and SSCs that perform safety functions shall employ defense-in-depth strategies that are sufficient to ensure adequate levels of reliability and capability to meet the top level regulatory criteria. (SRP Principles 1, 2, and 4 in Table 3-3). These strategies include the use of:

  - Active SSCs that work in concert with the inherent characteristics and passive SSCs to maintain the plant within normal conditions for transients and upset conditions and reduce the frequency of challenges to barriers and safety related SSCs
  - Appropriate combinations of inherent fuel and reactor characteristics, passive SSCs, and active SSCs in the performance of safety functions
  - Redundant, diverse, and independent means of fulfilling each safety function (SRP Principles 3, 7, and 9 in Table 3-3)
  - Adequate safety margins and conservative design approaches to address uncertainties in barrier and SSC performance (Use of SRP Principle 7 in Table 3-3)
  - Strategies to identify and defend against significant human errors and common cause failures that could challenge barriers to significant radioactive material release (SRP Principles 8 and 10 in Table 3-3)
  - A design that meets the intent of the applicable General Design Criteria in Appendix A to 10 CFR 50 and the reactor specific regulatory design criteria derived from the risk-informed performance-based licensing approach. (SRP Principle 11 in Table 3-3).

- ***Programmatic Defense-in-Depth Principles***

  The principles of defense-in-depth shall be applied with an appropriate set of programs that ensure defense-in-depth capabilities intended in the design are reflected in the as-built and as-operated plant and are maintained throughout the plant life time. These programs:

  - Avoid over-reliance on programmatic approaches to compensate for design weaknesses (SRP Principle 6 in Table 3-3)
  - Address significant uncertainties identified in the performance and review of the PRA (SRP Principle 7 in Table 3-3)
  - Shall be sufficient to provide confidence that SSCs will have sufficient reliabilities and capabilities to perform safety functions for the licensing basis events (SRP Principles 1 and 2 in Table 3-3).

- ***Risk-Informed Evaluation of Defense-in-Depth Principles***

  In evaluating the capabilities of the barriers and SSCs performing safety functions to respond to challenges, the following risk-informed and performance-based defense-in-depth principles shall be demonstrated:

  - Barrier and SSC reliability and independence are sufficient commensurate with the expected frequency of the challenge and the consequences of failure (SRP Principles 3, 7, and 9 in Table 3-3)
  - There is a reasonable balance between the prevention and mitigation of accidents involving release of significant quantities of radioactive material (SRP Principle 5 in Table 3-3)
  - There are no events with a significant frequency of occurrence that rely on a single element of design in protecting the public from a radioactive material release whose dose would exceed the TLRC (SRP Principle 3 in Table 3-3)
  - The safety design approach provides adequate defenses against common cause failures and human errors as required to ensure that barriers and SSCs providing safety functions have adequate reliabilities and capabilities (SRP Principles 8 and 10 in Table 3-3)
  - Deterministic requirements are met (SRP Principle 11 in Table 3-3).

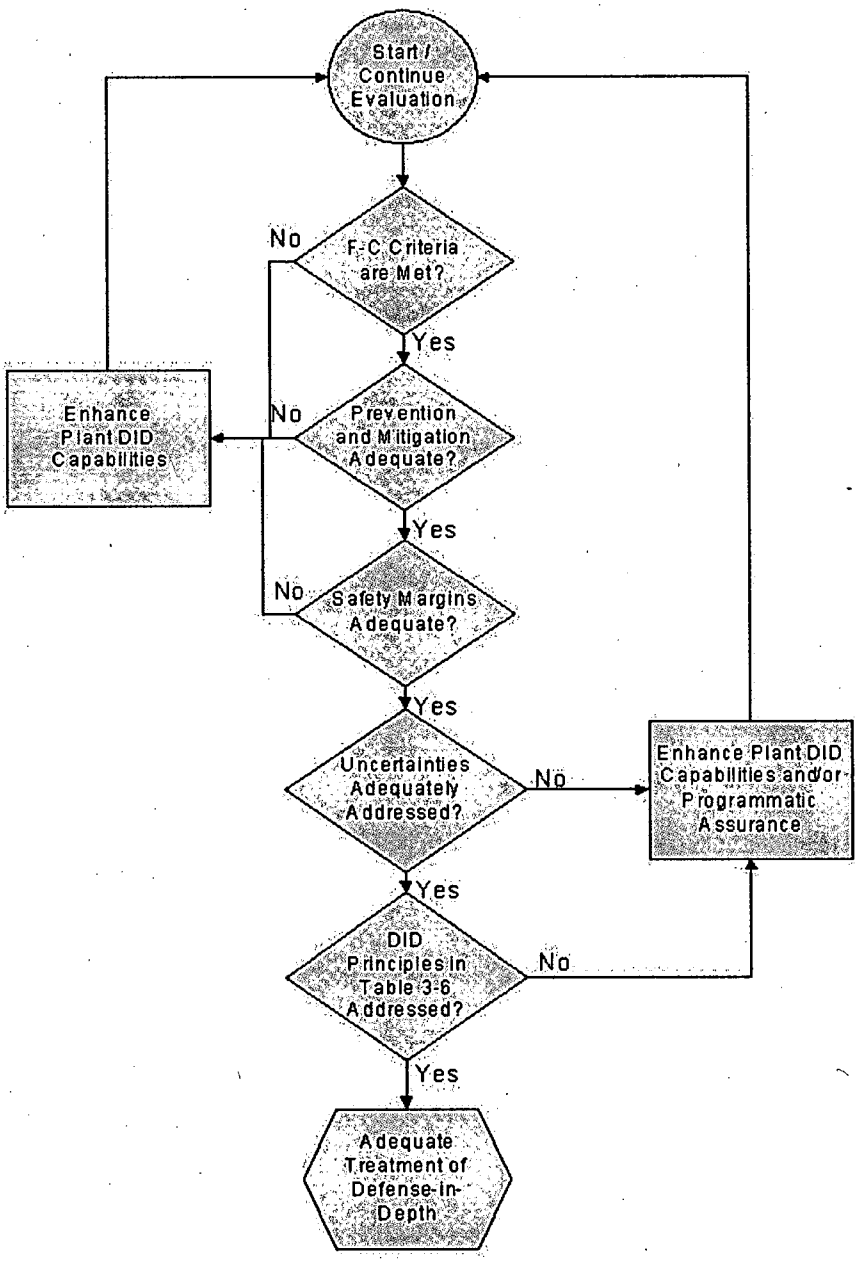


Figure 3-7. Logic for implementing ***Risk-Informed Evaluation*** of defense-in-depth.

Table 3-5. Elements of ***Risk-Informed Evaluation*** of defense-in-depth.

- Definition of a comprehensive set of challenges to barrier integrity:
  - Internal event scenarios
  - Internal plant hazard scenarios (e.g. fires and floods)
  - External events scenarios (e.g. seismic events and aircraft crashes).
- Interface with the risk-informed performance-based licensing approach:
  - Input to selection of licensing basis events
  - Input to safety classification of SSCs
  - Input to definition of special treatment requirements.
- Evaluation of event prevention strategies:
  - Strategies to prevent initiating events
  - Strategies to reduce frequency of challenges to safety systems
  - Strategies to prevent initiating events from progressing to accidents
  - Strategies to prevent accidents from exceeding the design basis
  - Strategies to preclude events with potentially high consequences.
- Evaluation of event mitigation strategies:
  - Strategies to limit impact of challenges and loads to barriers and SSCs
  - Strategies to retain and delay transport of radionuclides from barriers during accidents
    - Retention and delay within fuel
    - Retention and delay within helium pressure boundary
    - Retention and delay within reactor building
    - Strategies to provide offsite protective actions.
- Development of risk insights to achieve defense-in-depth:
  - Feedback to enhance plant capabilities
  - Feedback to enhance assurance programs
  - Demonstration of adequacy and sufficiency of defense-in-depth.
- Demonstration that defense-in-depth principles have been adequately applied.

3.2.4.4 Consistency with IAEA Approach

The prevention and mitigation strategies evaluated in the ***Risk-Informed Evaluation*** of defense-in-depth are consistent with the definition of defense-in-depth developed by the IAEA (described in Appendix A.4). The effectiveness of these strategies is highly correlated to the degree of independence that can be applied to each step in the process. A major goal of the PRA and supporting deterministic evaluations is to identify the dependencies and interactions that may influence the probability that each step is unsuccessful in protecting the public. An understanding of how defense-in-depth is applied in a range of conditions within and outside the design basis involves the examination of a suitable spectrum of scenarios from a quality and full scope PRA. The scenario-based defense-in-depth framework advanced by the IAEA provides a useful model to examine how specific design features contribute to the prevention and mitigation of accidents as will be demonstrated in the next section. Whereas ***Plant Capability Defense-in-Depth*** and ***Programmatic Defense-in-Depth*** are primarily responsible for delivering the capabilities of accident prevention and mitigation, ***Risk-Informed Evaluation*** of defense-in-depth provides the means of evaluating their effectiveness in both deterministic and probabilistic safety evaluations.

3.2.4.5 Use of PRA to Evaluate Roles of SSCs in Accident Prevention and Mitigation

A foundation of the ***Risk-Informed Evaluation*** of defense-in-depth is a PRA that identifies a reasonably complete set of accident sequences for the plant, estimates the frequencies and radiological consequences of these sequences, and includes a quantification and characterization of the uncertainty in these frequency and consequence estimates. The PRA provides important inputs to the selection of LBEs and the results of the PRA help establish that TLRC are met. The PRA is also used to establish system reliability targets and to evaluate changes to the plant design and operation throughout the plant life cycle. PRA has also demonstrated its usefulness in interpreting the safety significance of reactor incidents and accidents and the results of inspections. The NGNP Project approach to defense-in-depth includes a specific way to structure the information provided by the PRA in order to effectively apply the steps of the ***Risk-Informed Evaluation*** of defense-in-depth that are outlined in Figure D-5. In this approach, the results of the PRA are structured in a way that facilitates the evaluation of the roles of SSCs in the prevention and mitigation of accidents.

3.3 Demonstrating Defense-in-Depth Adequacy

3.3.1 Implementation of Plant Capability Defense-in-Depth

For the NGNP Project, the strategies to employ ***Plant Capability Defense-in-Depth*** begin with the definition and design of the radionuclide barriers and the application of inherent and passive safety features to anchor the safety case. To be clear on the meanings of inherent and passive, the following definitions are offered: Passive design features are defined as design features engineered to meet their functional requirements without a) needing successful operation of systems with mechanical components such as pumps, blowers, heating, ventilation, and air-conditioning (HVAC), sprays that require an external power source; b) depending on alternating current of electric power; or c) relying on operator actions. Inherent reactor characteristics are those characteristics that are associated with the reactor concept and the properties of the materials selected for the basic reactor components. NGNP passive design features utilize inherent characteristics and properties associated with the fuel, moderator, and helium coolant as discussed previously to achieve passive safety.

The ***Plant Capability Defense-in-Depth*** strategies also include the use of active SSCs and the application of redundancy, diversity and independence to achieve the necessary reliability and capability of the barriers and the SSCs that provide safety functions supporting the integrity of the barriers.

3.3.1.1 Radioactive Sources and Barriers to Radionuclide Transport

The sources of radioactive material and the physical passive barriers to the transport of radioactive material for the NGNP design are listed in Table 3-6. The most significant radionuclide inventories in the plant are those associated with the fuel inside the reactor vessel. There are additional significant radionuclide inventories in the spent fuel storage system within which inventory accumulates during the plant lifetime. If the core is off-loaded for unplanned maintenance inside the reactor vessel, up to a full reactor core inventory may be temporarily removed, which would also represent a large radionuclide inventory outside the core.

The primary barrier to radionuclide transport for all the sources associated with the reactor spent, used, and new fuel is TRISO coated particles within the spherical graphite fuel spheres (see Figure 3-8).

Table 3-6. Radioactive sources and barriers.

Radioactive Material Source	Barriers to Radionuclide Transport
Fuel in the core	Coated particles, graphite matrix, helium pressure boundary, reactor compartment, and reactor building
Fuel outside the core	Coated particles, graphite matrix, fuel handling and storage system equipment (e.g., storage containers), and building structures
Non-core sources within the power system	Helium pressure boundary, reactor building
Other sources	V tanks, piping systems and containers, and reactor building or ancillary buildings housing waste management equipment

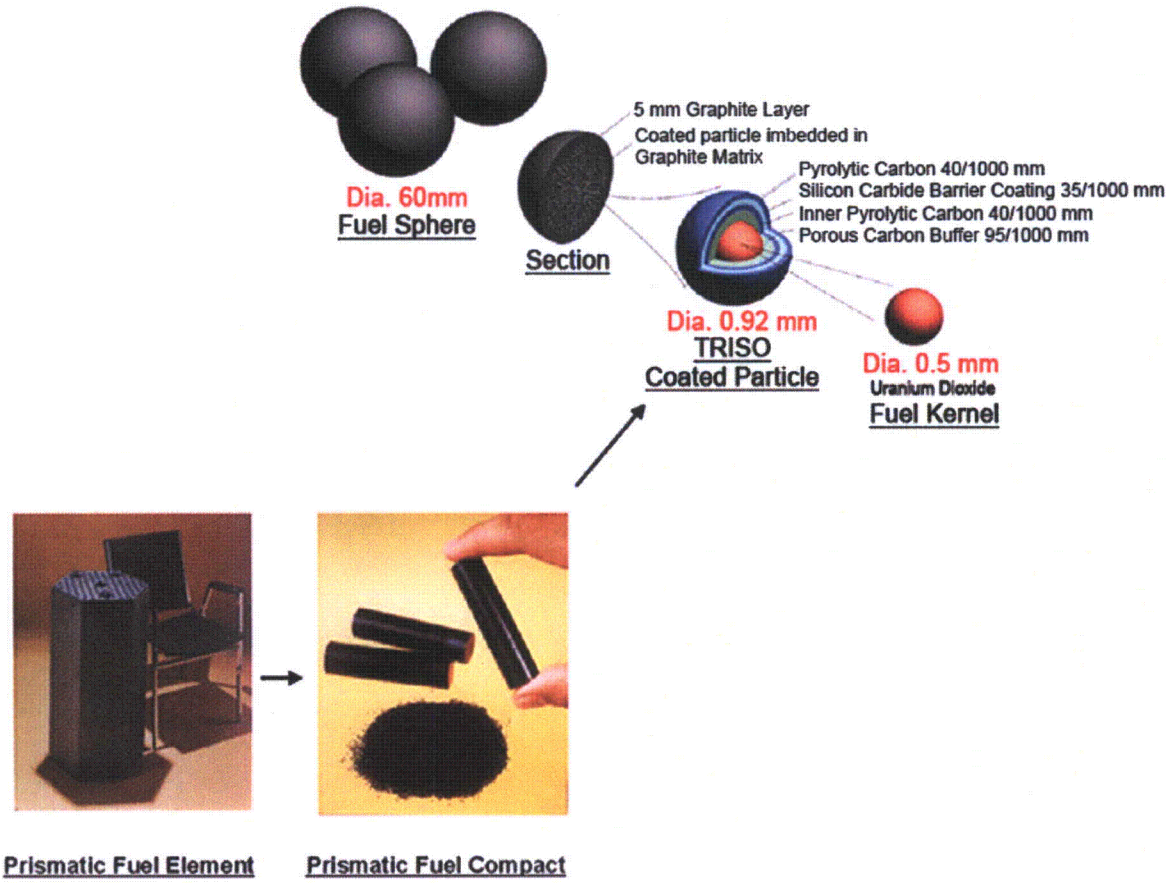
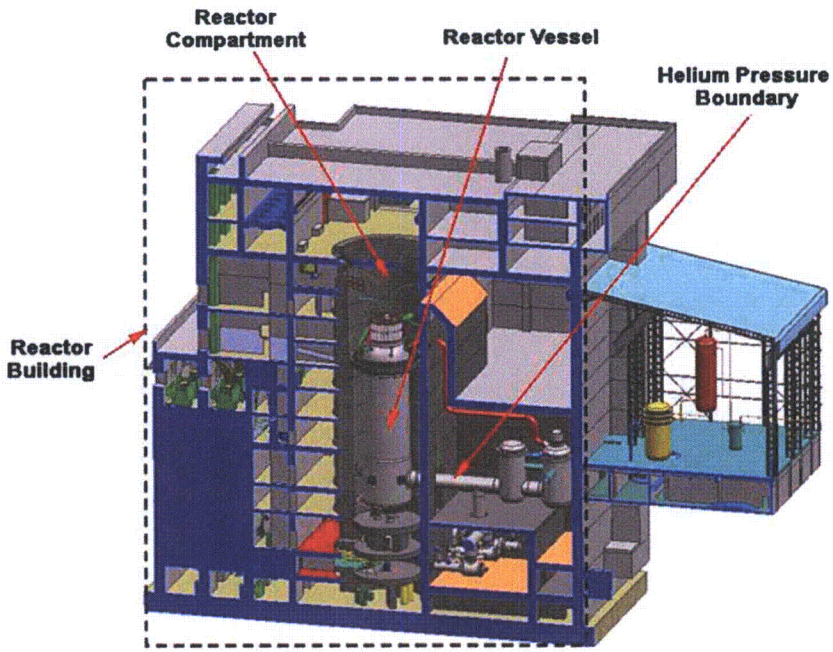
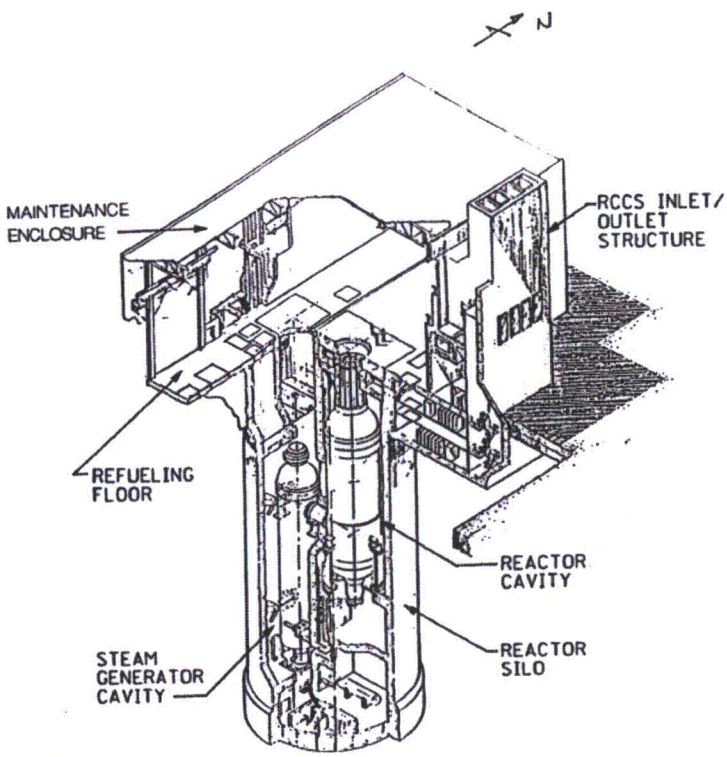


Figure 3-8. Fuel primary barrier to radionuclide transport.

For the fuel in the core and the other sources of radioactive material within the main power system there are multiple physical and passive barriers to restrict the transport of radioactive material. These include the fuel particle protective coatings, the helium pressure boundary, the reactor compartment, and the reactor building confinement (examples shown in Figure 3-9). Hence, there are multiple barriers as part of the ***Plant Capability Defense-in-Depth*** for the radionuclide sources within the reactor building. These barriers are concentric to eliminate bypass pathways and are designed to operate independently consistent with the principles of defense-in-depth.



PBMR



MHTGR

Figure 3-9. Example of major components and structures in HTGR designs.

3.3.1.2 Safety Functions

The NGNP safety design approach is framed in terms of reactor specific safety functions that were developed from the top goal of containing the inventory of radioactive material and then considering the specific functions that, when satisfied, would protect the integrity of the fuel and other radionuclide transport barriers. The top down logic used to define these functions is shown in Figure D-3 where the functions shown with shading are required safety functions, meaning that SSCs selected to perform these functions are required to operate to meet the deterministic dose requirements for DBEs. The functions shown without shading are not required but are included in the design to provide an element of ***Plant Capability Defense-in-Depth*** and to meet user requirements for plant availability and investment protection. The required safety functions include those to:

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

3.3.1.3 Selection of Inherent Features

The NGNP design is based on meeting the following objectives that specifically incorporate the approach to defining defense-in-depth:

- Provide safe, economic, and reliable power
- Select compatible fuel, moderator, and coolant with inherent safety characteristics
- Utilize proven technologies to the maximum extent practical
- Design reactor with inherent characteristics and passive safety features sufficient to protect the public as the primary strategy for ***Plant Capability Defense-in-Depth***
- Supplement with active design features and SSCs for investment protection and as a secondary strategy for ***Plant Capability Defense-in-Depth***.

Among the inherent passive characteristics of the design, the following are viewed as especially important in providing this component of the NGNP approach to defense-in-depth:

- Ceramic-coated pebble fuel:
  - Capability to maintain integrity at high temperatures
  - Chemically compatible with coolant and moderator
- Graphite moderator:
  - Capability to maintain integrity at high temperatures
  - High heat capacity
  - Chemically compatible with fuel and coolant
  - Large neutron migration length for neutron stability
- Helium coolant:
  - Single phase over all normal and accident conditions

- Chemically and neutronically inert
- Low stored thermal energy.

In addition to these characteristics, the NGNP design has both passive and active features to perform defense-in-depth functions, as discussed below.

3.3.1.4 Design Features Supporting Required Safety Functions

As noted above, the safety design approach is used to provide inherent characteristics and passive SSCs that are sufficient to protect the public, meet the TLRC, and provide the primary strategy for ***Plant Capability Defense-in-Depth***, and then to provide additional active SSCs to provide additional levels of defense-in-depth as well as to meet user requirements for plant availability and investment protection. A summary of the inherent characteristics and passive SSCs available to support each required safety function, as well as the additional active SSCs that support these functions, is provided in Table 3-7.

Table 3-7. Examples of design features and SSCs providing plant capability defense-in-depth.

Safety Function	Inherent Features and Passive SSCs	Active SSCs*
Control of Radionuclides	• Fuel barrier - Coated particle barrier - Graphite matrix - Graphite reflectors and other reactor internal surfaces • Primary heat transport system (PHTS); helium pressure boundary (HPB) barrier • Reactor building (RB) barrier - Radionuclide retention functions of RB - RB pressure relief system	• RB depressurization system • RB HVAC filtration system
Control of Heat Generation	• Strong negative temperature coefficient of reactivity	• Control and protection systems - Operational control system - Equipment protection system - Reactor protection system • Reactivity control systems - Reactivity control system trip release of control rod drives - Reserve shutdown system release of small absorber spheres

Table 3-7. (continued).

Safety Function	Inherent Features and Passive SSCs	Active SSCs*
Control of Heat Removal	• Large thermal heat capacity • Passive core heat removal • Core size, power density, geometry • Core, un-insulated reactor vessel, and reactor cavity configuration • Passive reactor cavity cooling system (RCCS)	• Active RCCS • Heat Transport System • Core conditioning or shutdown cooling system
Control of Chemical Attack	• PHTS HPB high reliability piping and pressure vessels • High purity specifications for inert helium coolant • RB air displaced by Helium during depressurization events reduces air concentration in RB • PRS relief blow-out panels or dampers protect RB structure • Multi-compartment design reduces He-air ingress potential	• RB dampers limit air ingress to RB and He-air ingress to PHTS • Isolation valves in PHTS interfacing systems provide means of isolating HPB breach in some locations • Helium purification system maintains high purity levels of Helium coolant
Maintain Core and Reactor Vessel Geometry	• Reactor core and structures • Reactor pressure vessel and structures • Reactor cavity structure • Reactor building structure	• Active RCCS maintains acceptable reactor vessel support and concrete temperatures

* 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.

In summary, there are inherent, passive design features available to support each of the safety functions, including the use of multiple, independent, and concentric barriers to radionuclide transport. This is the primary strategy to assure ***Plant Capability Defense-in-Depth*** for the NGNP Project. There are also redundant and diverse active systems available to support safety functions and prevent the challenges to the inherent and passive design features. As shown in Table 3-7, satisfaction of these safety functions is not dependent on a single element of the design, but rather is provided through redundant and diverse means. The application of defense-in-depth principles in the NGNP safety design approach has produced the following characteristics that comprise strong points of the safety case:

- The design has three concentric and independent radionuclide barriers:
  - The primary barrier to radionuclide transport for all the sources associated with the reactor spent, used, and new fuel is the multiple-coating feature of the TRISO coated particles within the graphite fuel elements. This barrier is specifically designed to contain the radionuclide inventory during all envisioned normal, upset, and accident conditions.
  - The Helium Pressure Boundary (HPB) provides an independent, passive, and concentric barrier to radionuclide transport. The inherent properties of the fuel, moderator, and helium coolant, such as the absence of pressurization mechanisms, minimize the potential for adverse fuel-coolant-pressure boundary interactions to enhance the independence of this barrier.

- The reactor building provides an additional independent and concentric passive barrier and several design features that perform safety functions to minimize PHTS-reactor building (RB)-environment gas exchange and enhance retention of airborne radionuclides.

- The coated particle fuel, helium coolant, and graphite moderator are chemically and physically compatible under all conditions.
- The fuel has very large temperature margins to radioactivity release in normal and accident conditions.
- The performance of safety functions is not dependent on the presence of the helium heat transport fluid.
- The response times of the reactor during transients are very long (days as opposed to seconds or minutes).
- There is no inherent mechanism for runaway reactivity excursions or power excursions. The capability to insert positive reactivity is inherently limited because of the low level of excess reactivity and on-line refueling capability for the PBMR based NGNP design.
- There is passive reactor shutdown capability because of a negative temperature coefficient under any transient involving under-cooling conditions.
- The design has two independent and diverse systems for reactivity control in addition to passive control via the negative temperature coefficient of reactivity
- The design has three independent and diverse systems for core heat removal, one of which operates using passive design principles.

3.3.2 Implementation of Programmatic Defense-in-Depth

The NGNP Project approach to ***Programmatic Defense-in-Depth*** includes the application of conservative safety margins and deterministic elements in the definition of the F-C Curve, selection of LBEs, safety classification of SSCs, and formulation of special treatment requirements for the safety classified SSCs. Those aspects of the RIPB licensing approach that are considered part of the approach to ***Programmatic Defense-in-Depth*** involve the application of conservative assumptions and are responsible for safety margins.

3.3.2.1 Selection of the F-C Curve

As summarized in Section 3.2.3, designing a plant to meet the dose criteria embodied in the TLRC and F-C Curve provides significant margin against the NRC Safety Goal QHO surrogates, often by orders of magnitude. When the LBE frequencies and consequences and associated uncertainties are compared against the F-C Curve, special requirements provide margin. For example, the NGNP Project has imposed its own user requirement that the consequences of the LBEs are to be met at the site boundary (not require credit for emergency planning beyond the site boundary to meet the frequency vs. dose thresholds embodied in the F-C Curve). Hence, a significant part of ***Programmatic Defense-in-Depth*** is simply demonstrating that the F-C Curve is met.

3.3.2.2 Definition of LBEs

In general, the sequences in the PRA lay out sets of event sequences that are organized into event sequence families for the definition of LBEs.[i] The process for organizing and grouping the event

i. As described in Section 1.6, a companion paper on LBE selection is being prepared.

sequences into event sequence families and LBEs uses conservative assumptions to ensure that the selected LBE conditions bound the set of event sequences assigned to the LBE. When the frequencies and consequences and associated uncertainties for each LBE are compared to the F-C Curve, the classification of each LBE as an AOO, DBE, or BDBE already conservatively accounts for the uncertainties. If the 95th percentile frequency of the LBE is above the breakpoint for separating the AOOs from the DBEs or the DBEs from the BDBEs, the LBE is assigned to the higher frequency category where more stringent dose criteria apply. The 95th percentile from the consequence uncertainty distribution is required to be within the associated F-C Curve. This evaluation of uncertainties is expected to result in the formulation of deterministic top level design criteria (TLDC) that are applied as part of the ***Programmatic Defense-in-Depth***.

3.3.2.3 Selection of Safety-Related SSCs

An important element of ***Programmatic Defense-in-Depth*** is applied in the safety classification of SSCs.[j] SSCs are classified based on criteria derived for the prevention and mitigation of LBEs. The SSC classification process includes a comprehensive review of the options available to perform each safety function for all LBEs, and includes additional classifications needed to prevent DBEs. The approach does not exclude certain LBEs that exceed the single failure criterion from the safety classification process and would naturally include all risk significant event sequences, especially those considered beyond design basis events. Hence, the risk-informed process of selecting safety related SSCs is expected to augment defense-in-depth for the NGNP design in comparison with the traditional approach to performing this function. As there will be improved opportunities to focus resources on risk significant SSCs, the principles of ***Programmatic Defense-in-Depth*** will be well served by this step in the approach.

3.3.2.4 Deterministic DBA Requirements

Additional conservatism is introduced by the requirement to demonstrate that each deterministically selected DBA can be sufficiently mitigated with only the safety-related SSCs being credited. Safety margins and conservative assumptions are also applied in the assignment of special treatment requirements for safety classified SSCs to assure that they have sufficient reliability and capability to perform their safety functions, as explained more fully below.

3.3.2.5 Selection of Special Treatment Requirements

As with currently licensed reactors, the principles of ***Programmatic Defense-in-Depth*** are applied in the formulation of special treatment requirements for non-safety-related SSCs. The NGNP Project will apply ***Programmatic Defense-in-Depth*** in the same manner to ensure that the safety-related SSCs have the adequate reliability and capability to perform their safety functions. While specific special treatment requirements for the NGNP design have not yet been defined, it is expected that such requirements will be applied using the principles of ***Programmatic Defense-in-Depth***. As such they will include conservative requirements and application of safety margins that provide confidence that the SSCs will perform their functions with an appropriate level of reliability and capability. Additionally, SSCs needed to prevent or mitigate other LBEs will have special treatment applied, commensurate with their importance to safety, in order to achieve the reliabilities and capabilities assumed in the PRA.

The risk-informed approach to defining special treatment requirements is being addressed in part by the American Society of Mechanical Engineers (ASME) Section XI Committee through the development of a new Division 2 of ASME Section XI for passive metallic components in MHTGRs. The Division 2 process being advanced is referred to as, "Reliability and Integrity Management (RIM)," rather than "in-

---

j. As described in Section 1.6, a companion paper on SSC classification is being prepared.

service inspection" because it addresses a wide range of activities, including design, leak monitoring, and nondestructive examinations, that can be used to influence the reliability of passive components and maintain high reliability throughout the plant's service life. This division of the code is in the process of ASME balloting. The RIM approach was developed by the ASME Section XI Special Working Group on HTGRs and demonstrated in a pilot study that was carried out for the PBMR Demonstration Power Plant.

3.3.3 Implementation of Risk-Informed Evaluation of Defense-in-Depth

The NGNP license application will use the logic diagram shown in Figure D-1 and the defense-in-depth criteria in Table 3-4 to conduct the ***Risk-Informed Evaluation*** of defense-in-depth and to justify that the plant capabilities and programs described in the license application provide an adequate application of defense-in-depth principles for the NGNP design. A cross reference table will be provided to show where in the license application the NRC will find objective evidence that each of the defense-in-depth criteria in Table 3-4 have been adequately addressed.

The NGNP license application will include an evaluation of the SSCs responsible for prevention and mitigation of accidents using the methodology outlined in Section 3.2.4.5. As discussed in Section 1.6, a white paper on SSC classification will be submitted that describes the strategy for identification of safety-related SSCs and the development of special treatment requirements for safety classified SSCs for the NGNP design.

3.4 Summary of Defense-in-Depth Insights for the NGNP Project

The regulatory foundation for defense-in-depth was reviewed in Section 2 of this paper. Among the various regulations and guidance documents that were reviewed, the defense-in-depth objectives in Chapter 19 of the *Standard Review Plan*[18] and the design attributes for advanced reactors from the NRC's policy on advanced reactor regulation[8] were selected as the basis for defense-in-depth criteria to be used for the NGNP license application (see Table 3-4). These criteria will be used in the ***Risk-Informed Evaluation*** of defense-in-depth as indicated in Table 3-5 and Figure 3-7 to demonstrate that the approach to defense-in-depth is adequate for the license application. As shown in Table 3-8 the NGNP license application will include sufficient information to judge the sufficiency of its approach to defense-in-depth in accordance with these criteria.

Table 3-8. Approach to addressing defense-in-depth principles of Table 3-5.

Defense-in-Depth Principles	Project Approach
Plant Capability Defense-in-Depth	
The safety design approach shall provide multiple, robust barriers to radioactive material release.	The design includes multiple robust barriers to radioactive material release. The license application will provide sufficient information to support a deterministic review of the design characteristics of each barrier. Challenges to barrier integrity and independence will be addressed in the PRA submitted to support the license application.
The barriers and SSCs that perform safety functions shall employ defense-in-depth strategies that are sufficient to ensure adequate levels of reliability and capability to meet the TLRC. These strategies include the use of: • Active SSCs that work in concert with inherent characteristics to maintain the plant within normal conditions for transients and upset conditions and reduce the frequency of challenges to barriers and safety related SSCs. • Appropriate combinations of inherent reactor characteristics, passive SSCs, and active SSCs in the performance of safety functions • Redundant, diverse, and independent means of fulfilling each safety function • Adequate safety margins and conservative design approaches to address uncertainties in barrier and SSC performance • Strategies to identify and defend against significant human errors and common cause failures that could challenge barriers to significant radioactive material release • A design that meets the intent of the applicable General Design Criteria in Appendix A to 10 CFR 50 and the reactor specific regulatory design criteria derived from the risk-informed performance-based licensing approach	The safety design approach is consistent with these criteria. Objective evidence will be included in the license application to demonstrate that each criterion is met.
Programmatic Defense-in-Depth	
The principles of defense-in-depth shall be applied with an appropriate set of programs that ensure that the defense-in-depth capabilities intended in the design are reflected in the as-built and as-operated plant and are maintained throughout the plant life time. These programs include:	The specific elements of programmatic defense-in-depth to be applied to the design will be documented in the license application.
• Avoid over-reliance on programmatic approaches to compensate for design weaknesses.	Sufficient information will be provided in the license application to demonstrate that there are no weaknesses in the design that rely on programmatic approaches to compensate.
• Address significant uncertainties identified in the performance and review of the PRA.	The PRA will include a comprehensive treatment of uncertainties. These and any additional uncertainties that may arise from PRA reviews will be addressed with appropriate programmatic requirements.
• Be sufficient to provide confidence that SSCs will have sufficient reliabilities and capabilities to perform safety functions for the licensing basis events.	The safety classification approach and special treatment requirements applied to SSCs will be described in the license application.

Defense-in-Depth Principles	Project Approach
Risk-Informed Evaluation of Defense-in-Depth	
In evaluating the capabilities of the barriers and SSCs performing safety functions to respond to challenges, the following risk-informed and performance-based defense-in-depth principles shall be demonstrated:	
• Barrier and SSC reliability and independence are sufficient commensurate with the expected frequency of the challenge and the consequences of failure.	The design information to be presented in the license application will describe the qualitative factors and specifications that support the reliability and capability of each SSC. Dependencies among SSCs that have significant risk impact will be described. The systematic search for initiating events in the PRA will identify credible barrier failure modes including HPB failure modes and challenges to the fuel barrier, HPB, and RB structural integrity from internal events and internal and external plant hazards. Dependencies and interactions among barrier and other SSC failure modes will be identified and included in the PRA. The structuring of PRA results will reveal any significant dependencies and provide a framework for the NRC to review to determine sufficient independence.
• There is a reasonable balance between the prevention and mitigation of accidents involving release of significant quantities of radioactive material.	The approach to safety classification of SSCs will document the SSCs available to support each safety function for each DBE. The structuring of PRA results will explicitly identify the roles of SSCs in the prevention and mitigation of accident sequences and will quantify the extent to which the accidents are prevented and mitigated. This approach will facilitate NRC review and enable judgments to be made about the adequacy of the strategies of prevention and mitigation.
• There are no events with a significant frequency of occurrence that rely on a single element of design in protecting the public from a radioactive material release whose dose would exceed the TLRC.	This will be demonstrated in the presentation of the PRA results.
• The safety design approach provides adequate defenses against common cause failures and human errors as required to ensure that barriers and SSCs providing safety functions have adequate reliabilities and capabilities.	The PRA will include a comprehensive treatment of human errors and common cause failures that contribute to the frequency of each modeled event sequence and LBE. The contributions of human errors and common cause failures to LBE frequencies will be clearly documented.
• Deterministic requirements are met.	The license application will include objective evidence that this principle is met.

In summary, the approach to defining and implementing the defense-in-depth safety philosophy has been described in this section. The NGNP Project has reviewed the regulatory foundation for defense-in-depth and has developed a definition of defense-in-depth that captures the principles found in the regulatory foundation and defines how these principles have been applied to the NGNP design.

The following conclusions are supported by the information presented in this section:

- Defense-in-depth is a well established safety philosophy in which multiple lines of defense are applied to the design, operation, and regulation of nuclear plants to assure that the public health and safety are adequately protected.

- NGNP Project has embraced defense-in-depth in the formulation of the safety design approach it expects to follow for licensing the design.
- The approach to defense-in-depth has three major elements: ***Plant Capability Defense-in-Depth***, ***Programmatic Defense-in-Depth***, and ***Risk-Informed Evaluation*** of defense-in-depth. All three elements of this approach to defense-in-depth are expected to play a significant role in the licensing of the NGNP plant.
- The definition of ***Plant Capability Defense-in-Depth*** proposed in this paper emphasizes the role of inherent and passive design features in supporting defense-in-depth, while retaining the traditional elements of redundancy, diversity, and independence. The elements of ***Plant Capability Defense-in-Depth*** include inherent and passive design features, concentric and independent radionuclide barriers, and passive as well as active SSCs to protect the integrity of the barriers.
- The NGNP design has three concentric and independent radionuclide barriers.
  - The primary barrier to radionuclide transport for the sources associated with the reactor spent, used, and new fuel is the multiple-coating feature of the TRISO coated particles within the graphite fuel elements. This barrier is specifically designed to contain the radionuclide inventory during all envisioned normal, upset, and accident conditions.
  - The HPB provides an independent, passive, and concentric barrier to radionuclide transport. The inherent properties of the fuel, moderator, and helium coolant, such as the absence of pressurization mechanisms, minimize the potential for adverse fuel-coolant-pressure boundary interactions to enhance the independence of this barrier.
  - The NGNP design provides concentric passive barriers including the reactor building structure, as well as active and passive SSCs to minimize helium-air exchange and provide enhanced retention of airborne radionuclides.
  - The inherent and passive design features have been deployed in a manner to enhance the degree of independence among the barriers and to protect the integrity of the fuel barrier under normal, upset, and accident conditions identified though the use of a full scope PRA. The roles of the secondary (PHTS HPB) and tertiary (RB) barriers compensate for conditions in which failure of the fuel barrier is postulated.
- The design includes passive and active SSCs to perform safety functions associated with protecting the integrity of the fuel and the other barriers to radionuclide transport. Where appropriate and applicable, the design principles of redundancy and diversity have been applied to achieve a sufficient degree of independence as required to deliver the appropriate degree of reliability and capability needed to meet the TLRC with residual defense-in-depth in the design.
- The NGNP license application will include a structured approach to define the roles of SSCs in the prevention and mitigation of accidents so that the extent of defense-in-depth and the balance of these strategies may be objectively measured and weighed. This approach is a key element in the application and evaluation ***Risk-Informed Evaluation*** of defense-in-depth principles for the NGNP Project.
- The components of ***Programmatic Defense-in-Depth*** will be applied in the form of conservative TLRC, selection of LBEs, safety classification of SSCs, and formulation of special treatment requirements.
- A set of principles derived from Chapter 19 of the SRP and the NRC Policy on Advanced Reactor Regulation provide a reasonable basis for judging the adequacy of the application of defense-in-depth principles in the NGNP license application.

- The defense-in-depth principles and the approach described above are consistent with the technical licensing approach recommended as part of the joint DOE and NRC Licensing Strategy Report to Congress.

4. ISSUES FOR RESOLUTION

4.1 NRC Discussion Topics

Section 1.4 introduced a set of issues to be addressed in this paper. These issues are framed in terms of the following questions about the approach to defense-in-depth that will be implemented as part of the NGNP design and license application:

- What is an appropriate definition of defense-in-depth for the NGNP Project?
- Is the definition of defense-in-depth suitable to allow objective evaluation of plant safety?
- What are the elements of defense-in-depth for the NGNP safety design philosophy, design approach and analyses, and assurance programs to ensure that defense-in-depth is achieved throughout the life of the plant?
- How is the defense-in-depth philosophy reflected in the proposed risk-informed licensing approach?
- How are the defense-in-depth strategies of accident prevention and mitigation defined and evaluated for the NGNP Project?
- Does the defense-in-depth approach described in this paper adequately address the technical elements as outlined in the NGNP Licensing Strategy Report to Congress?
- Is the defense-in-depth approach described in this paper sufficient to enable the NRC to evaluate the adequacy of the defense-in-depth capability in the NGNP license application?

4.2 Outcome Objectives

The objective of this paper is to solicit NRC feedback and agreement on an appropriate definition of defense-in-depth sufficient to support NGNP licensing, including relevant elements of a nuclear plant life cycle. Specifically, feedback is requested regarding NRC agreement with the following statements, or that the NRC provide an alternative set of statements that would be acceptable.

1. The definition of defense-in-depth presented in Section 3 of this paper, which recognizes three elements of a defense-in-depth approach: ***Plant Capability Defense-in-Depth***, ***Programmatic Defense-in-Depth***, and ***Risk-Informed Evaluation*** of defense-in-depth, is consistent with available definitions summarized in the regulatory foundation and is appropriate for the NGNP license application.
2. The ***Plant Capability Defense-in-Depth*** element, which includes multiple independent and diverse barriers to radionuclide transport, the use of inherent features and passive and active SSCs to perform the required safety functions, and conservative design strategies, is appropriate for the license application.
3. The ***Programmatic Defense-in-Depth*** element represents an acceptable approach to incorporation of defense-in-depth principles into the definition of programs that will provide assurance that the plant capabilities to assure safety and defense-in-depth will have sufficient reliability and be maintained throughout the lifetime of the plant and that uncertainties are adequately addressed by compensatory actions.
4. The ***Risk-Informed Evaluation*** of defense-in-depth element provides an acceptable balance of deterministic and probabilistic assessments and evaluation criteria. Further, this element includes an acceptable event sequence framework for the definition of accident prevention and mitigation, and for the evaluation of the roles of design features and SSCs responsible for prevention and mitigation for demonstrating the safety case. Finally, the balanced use of deterministic and probabilistic evaluations

provides a logical process to establish the adequacy and sufficiency of defense-in-depth for the NGNP Project.

5. When the approach described in this paper is applied in the NGNP license application, the NRC will have sufficient information on which to judge the adequacy of the defense-in-depth provisions. This information will include:

   a. A definition of defense-in-depth that is appropriate for the NGNP Project.

   b. The roles of each barrier to radioactive material retention for each significant inventory of radionuclides in providing the plant capabilities for defense-in-depth.

   c. How the reliability, capability, and independence of each barrier are defined and evaluated in terms of their plant capabilities for defense-in-depth.

   d. How the safety functions are defined and how they support the integrity of each barrier in providing the plant capabilities for defense-in-depth.

   e. The roles of diverse combinations of inherent and passive design features and SSCs that are used as well as active engineered systems to perform the safety functions as part of the plant capabilities for defense-in-depth.

   f. How the reliability, capability, and independence of each SSC providing a safety function is defined and evaluated as it relates to the plant capabilities for defense-in-depth.

   g. How the principles of design margins, redundancy, diversity, and independence have been applied in providing the plant capabilities for defense-in-depth.

   h. An appropriate definition of accident prevention and mitigation and a means to evaluate the impact of the defense-in-depth strategies on maintaining acceptable risk levels.

   i. The roles and effectiveness of specific barriers and SSCs in the prevention and mitigation of accidents.

   j. The role design safety margins reflected in the applied codes and standards play in providing a robust design with defense-in-depth.

   k. How compensating measures and other aspects of ***Programmatic Defense-in-Depth*** are applied to address uncertainties.

   l. How a set of deterministic principles derived from the regulatory foundation is applied in the risk-informed evaluation of the adequacy and sufficiency of defense-in-depth for the NGNP Project.

   m. How the elements of the safety design approach are used to evaluate plant design features in an integrated manner as part of an overall risk management approach in which risk analysis is used to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities to reduce risk.

NRC documentation of its responses to the above objectives and corresponding revisions to this paper will provide an agreed basis for related issues to be properly addressed in the NGNP license application.

5. REFERENCES

1. PBMR Letter, Subject: PBMR White Paper: Defense-in-Depth Approach, USDC20061213-1, Pebble Bed Modular Reactor (Proprietary) Ltd., December 13, 2006.

2. PBMR Letter, Subject: PBMR White Paper: PRA Approach, USDC20060613-1, Pebble Bed Modular Reactor (Proprietary) Ltd., June 13, 2006.

3. PBMR Letter, Subject: PBMR White Paper: LBE Selection, USDC20060703-1, Pebble Bed Modular Reactor (Proprietary) Ltd., July 3, 2006.

4. PBMR Letter, Subject: PBMR White Paper: SSC Classification, USDC20060828-1, Pebble Bed Modular Reactor (Proprietary) Ltd., August 28, 2006.

5. U.S. Nuclear Regulatory Commission Letter, Subject: Requests for Additional Information Regarding Pebble Bed Modular Reactor (PBMR) Preapplication White Papers, September 24, 2007.

6. PBMR Letter, Subject: Response to Requests for Additional Information, USDC20080321-1, Pebble Bed Modular Reactor (Proprietary) Ltd., March 21, 2008.

7 U.S. Nuclear Regulatory Commission, 'Safety Goals for the Operations of Nuclear Power Plants; Policy Statement', Federal Register, Vol. 51, No. 149, pp.28044-28049, August 4, 1986 (republished with corrections, Vol. 51, No. 160, pg. 30028-30023, August 21, 1986).

8. U.S. Nuclear Regulatory Commission, "Policy Statement on the Regulation of Advanced Reactors; Final Policy Statement," Federal Register, Vol. 73, No. 199, pg. 60612-60616, October 14, 2008.

9. U.S. Nuclear Regulatory Commission, "Policy Statement on Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," Federal Register, Vol. 60, No. 158, pg. 42622-42629, August 16, 1995.

10. Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk Informed Decisions on Plant-Specific Changes to the Licensing Basis," U.S. Nuclear Regulatory Commission, Revision 1, November 2002.

11. "Next Generation Nuclear Plant Licensing Strategy – A Report to Congress," Joint Report of the U.S. Department of Energy and the U.S. Nuclear Regulatory Commission, August 2008.

12. NUREG-1614, "U.S. Nuclear Regulatory Commission, FY 2008-2013 Strategic Plan,", U.S. Nuclear Regulatory Commission, Volume 4, February 2008.

13. NUREG-1860, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," U.S. Nuclear Regulatory Commission, December 2007.

14. ACRS Memorandum, Subject: Historical Notes on Defense in Depth," Advisory Committee on Reactor Safeguards, October 15, 1997.

15. ACRS Letter, "The Role of Defense in Depth in a Risk-Informed Regulatory System," Advisory Committee on Reactor Safeguards, May 19, 1999.

16. NUREG-1338, "Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)," U.S. Nuclear Regulatory Commission, March 1989.

17. U.S. Nuclear Regulatory Commission, "NRC Staff's Preliminary Findings Regarding Exelon Generation's (Exelon's) Proposed Licensing Approach For The Pebble Bed Modular Reactor (PBMR)," March 26, 2002.

18. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," U.S. Nuclear Regulatory Commission (Sections 7.2 and 19).

19. NUREG-1793, "Final Safety Evaluation Report (FSER) Related to Certification of the AP1000 Standard Design," U.S. Nuclear Regulatory Commission, September 2004.

20. Wallace, E.W., F.A. Silady, and K.N. Fleming, 'Selection of Licensing Basis Events for the U.S. Design Certification of the PBMR', Proceedings of ICAPP'06, Reno NV, June 2006.

Appendix A

Regulatory Requirements Overview

Appendix A
Regulatory Requirements Overview

A.1 Nuclear Regulatory Commission Requirements

Nuclear Regulatory Commission (NRC) regulatory requirements, codified in 10 CFR (Code of Federal Regulations), contain only a handful of instances that specifically mention "defense-in-depth." An early requirement appeared in 1980 when 10 CFR §50.48 and Appendix R, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979," were added. A general statement that, "The fire protection program shall extend the concept of defense-in-depth to fire protection in fire areas important to safety...," was added without clarification in the Statement of Considerations that accompanied the rulemaking.[1]

Twenty years later, a requirement for the design of fuel cycle facilities was added that provides better clarity in understanding NRC's use of the term. This requirement, included in 10 CFR §70.64, "Requirements for new facilities or new processes at existing facilities," states:

> *"(b) Facility and system design and facility layout must be based on defense-in-depth practices.*[1] *The design must incorporate, to the extent practicable:*
> *(1) Preference for the selection of engineered controls over administrative controls to increase overall system reliability; and*
> *(2) Features that enhance safety by reducing challenges to items relied on for safety."*

Footnote 1 to this requirement provides a definition for defense-in-depth that may be considered nontechnology specific:

> *"As used in § 70.64, Requirements for new facilities or new processes at existing facilities, defense-in-depth practices means a design philosophy, applied from the outset and through completion of the design, that is based on providing successive levels of protection such that health and safety will not be wholly dependent upon any single element of the design, construction, maintenance, or operation of the facility. The net effect of incorporating defense-in-depth practices is a conservatively designed facility and system that will exhibit greater tolerance to failures and external challenges. The risk insights obtained through performance of the integrated safety analysis can be then used to supplement the final design by focusing attention on the prevention and mitigation of the higher-risk potential accidents."*

Several requirements are stated simply as, "defense-in-depth is to be maintained." In 10 CFR §50.69(c), "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors," one of the requirements for classification of SSCs is that the classification process must "[m]aintain defense-in-depth." In 10 CFR §73.54(c)(2), a recently added requirement is to "[a]pply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks." 10 CFR §73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," has recently added two requirements: one in subsection §73.55(b)(3)(ii) to "[p]rovide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program." A second requirement is included in §73.55(b)(9)(i): "The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely

affect, either directly or indirectly, the licensee's capability to prevent significant core damage and spent fuel sabotage."

The concept of emergency planning as a programmatic element of defense-in-depth was described in the 1996 rulemaking updating 10 CFR Part 100, "Reactor Site Criteria,"[2] (which relocated source term and dose calculations to 10 CFR Part 50). In the Statement of Considerations for this rule, the NRC stated:

> *"that emergency planning is required as a matter of prudence and for defense-in-depth, and that the adequacy of an emergency plan was to be judged on the basis of its meeting the 16 planning standards given in 10 CFR 50.47(b). Hence, the characteristics of the site, which determine the evacuation time for the plume exposure pathway emergency planning zone, have not entered into the determination of the adequacy of an emergency plan."*

This rulemaking then added text to 10 CFR §100.1(d) that specifically mentions defense-in-depth:

> *"The Commission intends to carry out a traditional defense-in-depth approach with regard to reactor siting to ensure public safety."*

One recent rulemaking addresses the use of risk-informed assessments in evaluating defense-in-depth when addressing compliance with emergency core cooling requirements for LWRs.[3] Here, a new requirement §50.46a(f)(3)(i) is proposed to be added, similar to that in §50.69, that when changes are proposed, "[a]dequate defense in depth is [to be] maintained." The Statement of Considerations accompanying this proposed rule addition describes how defense-in-depth is to be assessed:

> *"The revised proposed rule is based upon the regulatory premise that the acceptability of all licensee-initiated changes made under the rule should be judged in a risk-informed manner. The risk-informed assessment process must include methods for evaluating compliance with the risk criteria, defense-in-depth criteria, safety margin criteria, and performance measurement criteria in Sec. 50.46a(f). These attributes have been identified by the Commission as a necessary set of risk evaluation tools to ensure that changes to the facility do not endanger public health and safety."*

Speaking specifically to defense-in-depth, the Statement of Considerations notes:

> *"Defense-in-depth is an element of the NRC's safety philosophy that employs successive measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. As conceived and implemented by the NRC, defense-in-depth provides redundancy in addition to a multiple barrier approach against fission product releases. Defense-in-depth continues to be an effective way to account for uncertainties in equipment and human performance. The NRC has determined that retention of adequate defense-in-depth must be ensured in all risk-informed regulatory activities."*

In describing the risk-informed evaluation process, the Statement of Considerations notes:

> *"The revised proposed rule is based upon the regulatory premise that the acceptability of all licensee-initiated changes made under the rule should be judged in a risk-informed manner. The risk-informed assessment process must include methods for evaluating compliance with the risk criteria, defense-in-depth criteria, safety margin criteria, and performance measurement criteria in Sec. 50.46a(f). These attributes have been identified by the Commission as a necessary set of risk evaluation tools to ensure that changes to the facility do not endanger public health and safety.*

Compliance with the risk criteria plays a key role in the regulatory structure of the proposed rule. A risk-assessment must be used to determine the change in risk associated with facility changes. Inasmuch as PRA methodologies are generally recognized as the best current approach for conducting risk assessments suitable for making decisions in areas of potential safety significance, Sec. 50.46a(f)(4) of the revised proposed rule would require that a technically adequate PRA be used in demonstrating compliance with the requirements of Sec. 50.46a that would affect the regulatory decision in a substantive manner. However, the NRC recognizes that non-quantitative PRA assessment methodologies and approaches could also be used to complement or supplement the quantitative aspects of a PRA, especially when performance of a quantitative PRA methodology of the level needed to support a particular decision is not justifiable because the safety significance of the decision does not warrant the level of technical sophistication inherent in a PRA. Accordingly, Sec. 50.46a(f)(5) is written to recognize that non quantitative risk assessment may also be "utilized.

A.2 NRC Policy Statements

Consideration of the defense-in-depth philosophy and its attributes has been included in several of NRC's policy statements. The 1986 Policy Statement on Safety Goals for the Operations of Nuclear Power Plants[4] states:

> *"The Commission recognizes the importance of mitigating the consequences of a core-melt accident and continues to emphasize features such as containment, siting in less populated areas, and emergency planning as integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy...*
>
> *To provide adequate protection of the public health and safety, current NRC regulations require conservatism in design, construction, testing, operation and maintenance of nuclear power plants. A defense-in-depth approach has been mandated in order to prevent accidents from happening and to mitigate their consequences. Siting in less populated areas is emphasized. Furthermore, emergency response capabilities are mandated to provide additional defense-in-depth protection to the surrounding population."*

NRC's Policy Statement on the Regulation of Advanced Reactors,[5] also published in 1986 (revised in 1994 and 2008), states:

> *"Among the attributes that could assist in establishing the acceptability or licensability of a proposed advanced reactor design, and therefore should be considered in advanced designs, are... [d]esigns that incorporate the defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for, and consequences of, severe accidents."*

The 1995 NRC Policy Statement on Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities[6] states:

> *'In the defense-in-depth philosophy, the Commission recognizes that complete reliance for safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant. Thus, the expanded use of PRA technology will continue to support the NRC's defense-in-depth philosophy by allowing quantification of the levels of protection and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry. Defense-in-depth is a philosophy used by NRC to provide redundancy for facilities with 'active'*

safety systems, e.g., a commercial nuclear power (sic), as well as the philosophy of a multiple-barrier approach against fission product releases.'

As part of its efforts in developing a risk-informed regulatory framework for future reactors, the NRC staff recommended to the Commission that a policy statement specific to defense-in-depth be developed. The staff described the history and status of this effort in SECY 2009-0056.[7]

> *"In SECY-03-0047, the staff recommended that the Commission approve the development of a policy statement or description on DID for nuclear power plants. In its SRM on SECY-03-0047, the Commission approved the staff's recommendation and stated that the staff should consider whether it can accomplish the same goals by updating the Commission Policy Statement on Use of Probabilistic Risk Assessment (PRA) Methods in Nuclear Regulatory Activities. In SECY-07-0101, the staff stated that stakeholders supported development of a separate policy statement on DID because they believed that DID is broader than, and not limited to, PRA. In its SRM on SECY-07-0101, the Commission directed the staff to develop a draft policy statement on DID for future plants for Commission consideration and stated that this draft policy could be evaluated using the insights gained through the development of the NGNP licensing strategy or completion of the PBMR preapplication review."*

While not strictly speaking from a policy statement, NRC's most recent Strategic Plan[8] describes the importance of defense-in-depth in conjunction with the use of conservative and realistic practices in providing an adequate margin of safety:

> *"It is the responsibility of the NRC to ensure that its licensees operate nuclear facilities and use radioactive materials safely. The NRC employs a multi-faceted regulatory approach to safety that includes the following activities:*
>
> - *Develop and update risk-informed and performance-based standards and regulations, as appropriate and Federal regulations to enable the safe use of radioactive materials, using the "defense-in-depth" principles and appropriately conservative and realistic practices that provide an adequate margin of safety.*
> - *License individuals and organizations that intend to use radioactive materials for safe and beneficial civilian purposes.*
> - *Maintain ongoing and consistent oversight of licensees, which includes inspection and enforcement, to ensure that they are conforming to the applicable regulations and the conditions of their licenses to ensure safety, and to provide timely and appropriate event assessment and response."*

The Strategic Plan then goes go to define defense-in-depth as:

> *"<u>Defense-in-Depth</u>: an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's Safety Philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility."*

Other useful definitions included in the Strategic Plan include:

> *"<u>Performance-Based</u>: an approach to regulatory practice that establishes performance and results as the primary bases for decision making. Performance-based regulations*

have the following attributes: (1) measurable, calculable or objectively observable parameters exist or can be developed to monitor performance; (2) objective criteria exist or can be developed to assess performance; (3) licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes; and (4) a framework exists or can be developed in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern."

Regulatory Framework: several interrelated aspects such as (1) the NRC's mandate from the Congress in the form of enabling legislation, (2) the NRC's licenses, orders, and regulations in Title 10 of the Code of Federal Regulations, (3) regulatory guides, review plans, and other documents that clarify and guide the application of NRC requirements that amplify those regulations, (4) the licensing and inspection procedures used by NRC employees, and (5) enforcement guidance.

Risk Assessment: a systematic method for addressing the three questions as they relate to the performance of a particular system, including the human component— "What can go wrong?" "How likely is it?" and, "What are the consequences?"

Risk Insights: the results and findings that come from risk assessments. They may include improved understanding of the likelihood of possible outcomes, sensitivity of the results to key assumptions, relative importance of the various system components and their potential interactions, and the areas and magnitude of the uncertainties.

Risk-Informed: an approach to decision making in which risk insights are considered along with other factors such as engineering judgment, safety limits, and redundant and/or diverse safety systems. Such an approach is used to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety."

A.3 NRC Guidance

NRC guidance on defense-in-depth is stated in several Regulatory Guides and the Standard Review Plan (SRP), NUREG-0800. Regulatory Guide (RG) 1.174, "An Approach to Using PRA in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis,"[9] provides guidance in how defense-in-depth is to be addressed when considering plant changes. This RG has been a preferred reference in NRC efforts revising existing requirements to allow for risk-informed approaches in regulatory actions. As an example, the Statement of Considerations accompanying the recent rulemaking that would permit use of risk-informed assessments in evaluating changes to LWR emergency core cooling requirements (described in section A.1 above) ties together NRC's statements on defense-in-depth included in RG 1.174 with those of the probabilistic risk assessment (PRA) policy statement.

"To implement the [PRA] policy statement, the NRC developed guidance on the use of risk information for reactor license amendments and issued Regulatory Guide (RG) 1.174, "An Approach for Using Probabilistic Risk Assessments in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis," (ADAMS Accession No. ML023240437). This RG provided guidance on an acceptable approach to risk-informed decision-making consistent with the Commission's policy, including a set of key principles. These principles include: (1) Being consistent with the defense-in-depth philosophy; (2) Maintaining sufficient safety margins; (3) Allowing only changes that result in no more than a small increase in core damage frequency or risk (consistent with the intent of the Commission's Safety Goal Policy Statement); and (4) Incorporating monitoring and performance measurement strategies. Regulatory Guide 1.174 further

clarifies that in implementing these principles, the NRC expects that all safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities to reduce risk; and not just to eliminate requirements that a licensee sees as burdensome or undesirable."

Regulatory Guide 1.183, "Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors,"[10] provides additional guidance on the use of PRA in evaluating the sufficiency of defense-in-depth:

"Although probabilistic risk assessments (PRAs) can provide useful insights into system performance and suggest changes in how the desired depth is achieved, defense in depth continues to be an effective way to account for uncertainties in equipment and human performance. The NRC's policy statement on the use of PRA methods (Ref. 4) calls for the use of PRA technology in all regulatory matters in a manner that complements the NRC's deterministic approach and supports the traditional defense-in-depth philosophy."

In discussing risk metrics, Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,"[11] notes:

"Issues related to the reliability of barriers (in particular, containment integrity and consequence mitigation) are addressed through other parts of the decision-making process, such as consideration of defense-in-depth."

Regulatory Guide 1.201, "Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to their Safety Significance,"[12] in endorsing Nuclear Energy Institute 00-04, 10 CFR 50.69 SSC Categorization Guideline,[13] notes:

"[T]he integrated decision-making process must systematically consider the quantitative and qualitative information available regarding the various modes of plant operation and initiating events, including PRA quantitative risk results and insights (e.g., CDF, LERF, and importance measures); deterministic, traditional engineering factors and insights (e.g., defense-in-depth, safety margins, and containment integrity); and any other pertinent information (e.g., industry and plant-specific operational and performance experience, feedback, and corrective actions program) in the categorization of SSCs."

Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition),"[14] notes:

"For a passive safety system design that relies exclusively on natural forces to perform design-basis safety functions, and includes active systems to provide defense-in-depth capabilities for reactor coolant makeup and decay heat removal, the applicant should describe how the passive system reliability and the impact of adverse system interactions on the safety functions were considered."

Regulatory Guide 1.206 also notes the need to establish the risk importance of defense-in-depth systems:

"[F]or designs using passive safety systems and active "defense-in-depth" systems, sensitivity studies should be performed to investigate the impact of uncertainties on PRA results under the assumption of plant operation without credit for the non-safety-related "defense-in-depth" systems. These studies provide additional insights about the risk

importance of the "defense-in-depth" systems that are taken into account in selecting non-safety-related systems for regulatory oversight according to the RTNSS process."

A roadmap as to how defense-in-depth is to be evaluated is provided in SRP Chapter 19, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-informed Decision making: General Guidance."[15] This SRP chapter provides the following definition of defense-in-depth:

> *"Defense in depth is defined as a philosophy that ensures that successive measures are incorporated into the design and operating practices for nuclear plants to compensate for potential failures in protection and safety measures. In risk-informed regulation, the intent is to ensure that the defense-in-depth philosophy is maintained, not to prevent changes in the way defense in depth is achieved. The defense-in-depth philosophy has been and continues to be an effective way to account for uncertainties in equipment and human performance. In some cases, risk analysis can help quantify the range of uncertainty; however, there will likely remain areas of large uncertainty or areas not covered by the risk analysis. Where a comprehensive risk analysis can be performed, it can help determine the approximate extent of defense in depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) to ensure protection of public health and safety. However, because PRAs do not reflect all aspects of defense-in-depth, appropriate traditional defense-in-depth considerations should also be used to account for uncertainties...."*

Chapter 19 of the SRP provides further perspective on the role that barriers play in providing defense-in-depth by stating:

> *"Defense in depth can be evaluated on the basis of considerations involving the barriers that prevent or mitigate radioactivity release. Release of radioactive materials from the reactor to the environment is prevented by a succession of passive barriers, including the fuel cladding, reactor coolant pressure boundary, and containment structure. These barriers, together with an imposed exclusion area and emergency preparedness, are the essential elements for accident consequence mitigation. Given these multiple barriers, safety is ensured through the application of deterministic safety criteria for the performance of each barrier and through the design and operation of systems to support the functional performance of each barrier."*

The SRP continues by providing a set of objectives and guidelines for consideration by NRC reviewers when reviewing licensee proposed changes:

> *"In maintaining consistency with the defense-in-depth philosophy, the proposed license amendment should not result in any substantial change in the effectiveness of the barriers. Consequently, reviewers should consider the following objectives to ensure that the proposed change maintains appropriate safety within the defense-in-depth philosophy:*
>
> - *The change does not result in a significant increase in the existing challenges to the integrity of the barriers.*
> - *The proposal does not significantly change the failure probability of any individual barrier.*
> - *The proposal does not introduce new or additional failure dependencies among barriers that significantly increase the likelihood of failure compared to the existing conditions.*
> - *The overall redundancy and diversity among the barriers is sufficient to ensure compatibility with the risk acceptance guidelines.*

In demonstrating that the proposal fulfils the objectives listed above, the staff expects that the proposed change will meet the following guidelines:

- *A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and mitigation of consequences.*
- *The proposal avoids over-reliance on programmatic activities to compensate for weaknesses in plant design.*
- *The proposed change preserves system redundancy, independence, and diversity commensurate with the expected frequency of challenges, consequences of failure of the system, and associated uncertainties.*
- *The proposal preserves defenses against potential common cause failures and assesses the potential introduction of new common cause failure mechanisms.*
- *The proposed change does not degrade the independence of barriers.*
- *The proposed change preserves defenses against human errors.*
- *The proposal fulfils the intent of the General Design Criteria in Appendix A to 10 CFR Part 50.*

Reviewers can assess fulfillment of the above guidelines by using qualitative or traditional engineering arguments or by using PRA results contained in the accident sequences or cut-sets."

In discussing the need to preserve multiple barriers against radioactivity release, SRP Chapter 19 includes a set of review objectives to ensure that the "appropriate safety within the defense-in-depth philosophy" is maintained. These objectives are reproduced in Table 3-3 above along with an assessment of the approach for each of the objectives.

A.4 International Atomic Energy Agency Guidance

The International Atomic Energy Agency (IAEA) has discussed defense-in-depth in several of its expert consultant reports as well as in safety standards. This section describes several of the primary reports on the topic.

The International Nuclear Safety Advisory Group (INSAG) of the IAEA published INSAG-3, *Basic Safety Principles for Nuclear Power Plants*, in 1988. INSAG-3 states:

> *"All safety activities, whether organizational, behavioral or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defense in depth, and it is repeatedly used in the specific safety principles that follow."*

The document then goes on to define a concept of defense-in-depth:

> *"To compensate for potential human and mechanical failures, a defense in depth concept is implemented, centered on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barrier by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective."*

In 1996, INSAG-10, *Defense in Depth in Nuclear Safety*, was published.[16] INSAG-10 starts by quoting the concept of defense-in-depth that was defined in INSAG-3. The report then summarizes the historical development of safety concepts and discusses the concept of defense-in-depth in terms of objectives, strategy, physical barriers and levels of protection. Table 1 of INSAG-10 describes five levels of defense-in-depth. This table is reproduced below.

Table A-1. Levels of defense-in-depth.

Levels of Defense-in-Depth	Objective	Essential Means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and failures	Control, limiting, and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered features and accident procedures
Level 4	Control of severe plant conditions, including prevention or accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

Source: INSAG-10, Table 1

In 1999, the IAEA published INSAG-12, *Basic Safety Principles for Nuclear Power Plants.*[17] INSAG-12 was published as Revision 1 to the earlier 75-INSAG-3, *Basic Safety Principles for Nuclear Power Plants.* This report describes defense-in-depth as one of the fundamental nuclear safety principles, and includes the following high level definition:

> *"46. Principle: To compensate for potential human and mechanical failures, a defense in depth concept is implemented, centered on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective."*

In addition to this definition of the over-arching principle, INSAG-12 discusses the strategies for implementing defense-in-depth, including the following statements:

> *"47. The defense in depth concept provides an overall strategy for safety measures and features of nuclear power plants. When properly applied, it ensures that no single human or equipment failure would lead to harm to the public, and even combinations of failures that are only remotely possible would lead to little or no harm. Defense in depth helps to establish that the three basic safety functions (controlling the power, cooling the fuel and confining the radioactive material) are preserved, and that radioactive materials do not reach people or the environment.*
>
> *48. The principle of defense in depth is implemented primarily by means of a series of barriers which would in principle never be jeopardized, and which must be violated in turn before harm can occur to people or the environment. These barriers are physical,*

providing for the confinement of radioactive material at successive locations. The barriers may serve operational and safety purposes, or may serve safety purposes only. Power operation is only allowed if this multibarrier system is not jeopardized and is capable of functioning as designed.

49. The strategy for defense in depth is twofold: first, to prevent accidents and second, if prevention fails, to limit the potential consequences of accidents and to prevent their evolution to more serious conditions. Defense in depth is generally structured in five levels. The objectives of each level of protection and the essential means of achieving them in existing plants are shown in Table I [same as the table above], which is reproduced from INSAG-10. If one level were to fail, the subsequent level comes into play, and so on. Special attention is paid to hazards that could potentially impair several levels of defense, such as fire, flooding or earthquakes. Precautions are taken to prevent such hazards wherever possible and the plant and its safety systems are designed to cope with them.

50. The reliability of the physical barriers is enhanced by applying the concept of defense in depth to them in turn, protecting each of them by a series of measures. Each physical barrier is designed conservatively, its quality is checked to ensure that the margins against failure are retained, its status is monitored, and all plant processes capable of affecting it are controlled and monitored in operation. Human aspects of defense in depth are brought into play to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, independent regulation, operating limits, personnel qualification and training, and safety culture. Design provisions including both those for normal plant systems and those for engineered safety systems help to prevent undue challenges to the integrity of the physical barriers, to prevent the failure of a barrier if it is jeopardized, and to prevent consequential damage of multiple barriers in series. Safety system designers ensure to the extent practicable that the different safety systems protecting the physical barriers are functionally independent under accident conditions.

51. All the levels of defense are available at all times that a plant is at normal power. Appropriate levels are available at other times. The existence of several levels of defense in depth is never justification for continued operation in the absence of one level. Severe accidents in the past have been the result of multiple failures, both human and equipment failures, due to deficiencies in several components of defense in depth that should not have been permitted.

52. System design according to defense in depth includes process controls that use feedback to provide a tolerance of any failures which might otherwise allow faults or abnormal conditions to develop into accidents. These controls protect the physical barriers by keeping the plant in a well defined region of operating parameters where barriers will not be jeopardized. Care in system design prevents cliff edge effects which might permit small deviations to precipitate grossly abnormal plant behavior and cause damage.

53. Competent engineering of the barriers and the measures for their protection coupled with feedback to maintain operation in optimal ranges leads to a record of smooth, steady performance in producing electricity on demand. This indicates the proper implementation of the most important indicator of the success of defense in depth, which is operation with little or no need to call on safety systems.

54. The multibarrier system protects humans and the environment in a wide range of abnormal conditions. Preplanned countermeasures are provided, as a further component of defense in depth, against the possibility that radioactive material might still be released from the plant."

The above defense-in-depth principle and strategies to achieve it are supplemented by further supporting principles of prevention and mitigation:

"56. Principle: Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents, particularly any which could cause severe core damage.

63. Principle: In-plant and off-site mitigation measures are available and are prepared for that would substantially reduce the effects of an accidental release of radioactive material.

A report in IAEA's Safety Reports Series, *Assessment of Defense in Depth for Nuclear Power Plants*,[18] was published in 2005 to provide additional guidance for implementation of the principles described in INSAG-10 and INSAG-12. This report defines defense-in-depth as:

"consist[ing] of a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive material and workers, the public or the environment, during normal operation, anticipated operational occurrences (AOOs) and, for some barriers, accidents at the plant."

The report notes the need to understand the fundamental safety functions, and states its focus as one of protecting barriers against radioactive material release:

"The aim of the defense in depth provisions is to protect the barriers and to mitigate the consequences if the barriers against the release of radioactive material are damaged."

The emphasis is placed on maintaining independence between the different levels of defense that are described in Table 1 of INSAG-10, but allows that "*[t]he levels are intended to be independent to the extent practicable.*"

Technical document IAEA-TECDOC-1570, *Proposal for a Technology-Neutral Safety Approach for New Reactor Designs*,[19] summarizes the importance of using a risk-informed approach in evaluating a plant's defense-in-depth capability:

"The experience gained in decades of design and licensing, combined with the development of risk-based concepts, has provided insights that will form the basis for new safety rules and requirements. Many lessons learned acknowledge the importance of such concepts as safety goals and defense in depth and the benefits of integrating risk insights early in an iterative design process. A new safety approach will incorporate many of the new developments in these concepts. For example, the probabilistic elements of defense in depth will help define the cumulative provisions to compensate for uncertainty and incompleteness of our knowledge of accident initiation and progression."

The method described in this TECDOC "...proposes an integration of deterministic and probabilistic considerations with established principles and concepts such as safety goals and defense-in-depth."

A.5 Other References

A.5.1 Next Generation Nuclear Plant Licensing Strategy - Report to Congress

The Next Generation Nuclear Plant (NGNP) Licensing Strategy Report to Congress describes several licensing alternatives and options for adapting existing NRC technical requirements to the NGNP Project.[20] The recommended licensing process uses the single step Combined Licensing (COL) approach included in 10 CFR Part 52. The report, in noting "...there are several technical options for establishing the NGNP licensing basis, each placing progressively greater emphasis on the use of PRA techniques and risk insights...," recommends "...that the overall NGNP licensing strategy should comprise Option 2 – a risk-informed, performance-based approach to adapting technical requirements." Option 2 is defined as:

> ***"Option 2: Risk-Informed and Performance-Based Approach.*** *This option uses deterministic engineering judgment and analysis, complemented by NGNP design-specific PRA information, to establish the licensing basis (including selecting licensing basis events) and licensing technical requirements. The use of the PRA would be commensurate with the quality and completeness of the PRA presented with the application."*

This recommendation is further described as:

> *"With regard to technical licensing requirements, the Secretary of Energy and the Commission determined that the best option for licensing the NGNP prototype would be to use a risk-informed and performance-based technical approach, in particular, Option 2 (i.e., use of deterministic judgment and analysis, complemented by NGNP-specific PRA information) to adapt the existing LWR technical requirements and to establish the NGNP-unique requirements that are not addressed by existing LWR requirements and guidance."*

Defense-in-depth is considered in the statement of the technical approach to establishing the licensing basis:

> *"The technical approach to establishing the NGNP licensing basis and requirements is expected to include the following:*
>
> - *establishment of licensing-basis event categories (i.e., abnormal occurrences, design-basis accidents, and beyond-design-basis accidents) based on the expected probability of event occurrence; within each category, selection of licensing basis events using deterministic engineering judgment complemented by insights from the NGNP PRA.*
> - *selection of the safety-significant systems, structures, and components (SSCs) relied on to prevent or mitigate the safety-significant licensing-basis events using deterministic judgment, complemented by insights from the NGNP PRA.*
> - *establishment of conservative design and acceptance criteria for core and safety-significant SSCs, consistent with the applicable LWR requirements and recognizing the design and technology aspects unique to the NGNP.*
> - *verification of adequate safety margins to the integrity and performance of core and safety-significant SSCs using a conservative analysis or a best-estimate analysis with consideration of uncertainties.*
> - *establishment of special treatment requirements to ensure the required performance capability and reliability of the safety-significant SSCs using deterministic engineering judgment, complemented by insights and information from the plant PRA.*

- *use of consequence acceptance limits for onsite or offsite releases for licensing-basis events that are consistent with current dose limits for LWRs in 10 CFR Part 20, "Standards for Protection Against Radiation," and 10 CFR 50.34, "Contents of Construction Permit and Operating License Applications; Technical Information"; also, assessment of radiological consequences for licensing-basis events on the basis of event-specific mechanistic source terms.*
- *consideration of containment functional performance requirements as a radionuclide barrier in the context of design and performance of such NGNP features as the core, fuel, and cooling systems.*
- *establishment of defense-in-depth (DID) requirements using deterministic engineering judgment, complemented by risk insights, as appropriate."*

A.5.2 Development of a RIPB Update to 10 CFR Part 50 Requirements

Following issuance of the PRA policy statement in 1995, the NRC embarked on a series of initiatives to both risk-inform existing regulatory requirements and to establish a new, risk-informed technology-neutral framework for future reactors. In SECY 2009-0056, *Staff Approach Regarding a Risk-Informed and Performance-Based Revision to Part 50 of Title 10 of the Code of Federal Regulations and Developing a Policy Statement on Defense-in-Depth for Future Reactors*, [Ref. 34], the NRC staff summarized the development of a technology-neutral regulatory framework.

> *"In accordance with Commission direction, the staff issued the technology-neutral framework as NUREG-1860, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," Volumes 1 and 2, in December 2007. [Ref. 21] This NUREG documents a framework that provides an approach and criteria that (1) could be used to develop an alternative set of technical requirements to 10 CFR Part 50 applicable for future non-LWR nuclear power plants (the framework includes a proposed draft set of technical requirements), and (2) could be used to establish risk-informed licensing basis events and the safety classification of structures, systems, and components.*
>
> *In its letter dated August 31, 2001 [Ref. 22], Exelon submitted a white paper describing and documenting its proposed risk-informed and performance-based licensing approach to be used in a PBMR COL application. At the time that Exelon terminated its preapplication interactions with the staff, there remained a number of technical issues that had been identified and remained unresolved. Subsequently, in 2006, to address these unresolved issues and to provide additional details on its proposed risk-informed licensing approach for the PBMR, PBMR (Pty) Ltd. submitted four follow-on, more detailed white papers to the NRC for consideration. In its March 21, 2008, letter, PBMR (Pty) Ltd. responded to staff requests for additional information on these topics. Since then, however, the staff has not had the resources needed to review and document its evaluation of these aspects of the proposed PBMR licensing approach. The NRC needs to conduct additional technical evaluations on the different risk-informed, performance-based licensing approaches presented in NUREG-1860 and by PBMR (Pty), Ltd. The staff continues to evaluate how to develop a risk-informed and performance-based set of requirements that could be used to license the PBMR, or support rulemaking for risk-informed and performance-based reactor requirements for future reactors."*

NUREG 1860 provides extensive discussion of the topic of defense-in-depth as it relates to the RIPB structure for future plant licensing. It includes a definition of defense-in-depth that is the same as the glossary entry in NRC's Strategic Plan (NUREG-1614):

"Defense-in-depth is an element of NRC's safety philosophy that is used to address uncertainty by employing successive measures including safety margins to prevent and mitigate damage if a malfunction, accident or naturally caused event occurs at a nuclear facility"

The NUREG includes a set of defense-in-depth principles for evaluating reactor designs:

- *"provide measures against intentional as well as inadvertent events;*
- *provide accident prevention and mitigation capability;*
- *ensure key safety functions are not dependent upon a single element of design, construction, maintenance or operation;*
- *ensure uncertainties in equipment and human performance are accounted for and appropriate safety margins provided;*
- *provide alternative capability to prevent unacceptable releases of radioactive material to the public; and*
- *be sited* at locations that facilitate protection of public health and safety."

The approach to defense-in-depth described in NUREG 1860 includes both deterministic and probabilistic elements. The two principal deterministic elements are:

- To ensure the implementation of all of the defense-in-depth protective strategies
- To ensure that defense-in-depth principles are followed to develop licensing potential requirements.

The probabilistic elements of the approach consist of:

- Using the PRA, to the extent possible, to search for and identify unexpected scenarios, including their associated uncertainties.
- Helping to establish adequate defense-in-depth measures, including safety margins, to compensate for those scenarios and their uncertainties, which are quantified in the PRA model.

In describing these elements, NUREG-1860 recognizes PRA as a useful tool for searching for the unexpected and for identifying uncertainties:

"Consequently, PRA has a role to play, along with deterministic considerations, in establishing what constitutes adequate defense-in-depth. ... Although PRA cannot compensate for the unknown and identify all unexpected events, this approach uses risk assessment to:

(1) identify some originally unforeseen scenarios,

(2) identify where some of the uncertainties lie in the plant design and operation, and, for some uncertainties,

(3) quantify the extent of the uncertainty."

With respect to uncertainty, the probabilistic elements of defense-in-depth are the aggregate of provisions made to compensate for uncertainty and incompleteness in knowledge of accident initiation and progression.

"The probabilistic elements are used to determine how much defense-in-depth is needed to compensate for the uncertainties that can be quantified. The deterministic elements compensate for the unquantified uncertainties, especially the unexpected threats resulting from completeness uncertainty."

In selecting both the LBEs and the safety significant SSCs, risk information from the PRA is used to focus attention on the risk-significant aspects of the design.

"LBEs derived from the PRA need to meet stringent probabilistic acceptance criteria and, depending on their frequency, need to meet additional deterministic (defense-in-depth) criteria. In this manner, the LBEs provide additional assurance that the design has adequate defense-in-depth in the form of sufficient margin to account for uncertainties. The LBEs also include a deterministically selected event, used in assessing site suitability."

Additionally,

"The selection of LBEs based on event sequences from the PRA also serves as a more realistic assessment of the impact on risk of equipment failures that are modeled in the analysis. As such, it serves as a replacement for the traditional "single failure criterion" applied in the current licensing process. Accordingly, in the criteria that are proposed in the Framework, a single-failure type of criterion is included only for defense-in-depth purposes for key safety functions, such as redundant, diverse, independent means of reactor shutdown."

A.5.3 Advisory Committee on Reactor Safeguards Recommendations

The ACRS reviews and provides recommendations to the NRC Commissioners in the development and implementation of NRC requirements and policy statements (see sections A.1 and A.2 above). The ACRS has also been engaged in NRC's ongoing efforts to develop a technology-neutral regulatory approach for future reactors. In one notable memorandum, the ACRS summarized the use of defense-in-depth statements in NRC's regulatory development history.[23]

In May 1999, the ACRS provided the NRC with a detailed set of recommendations in a letter entitled, "The Role of Defense in Depth in a Risk-Informed Regulatory System."[24] As with the memorandum (mentioned in the above paragraph), this letter included an attached paper that described two views to defense-in-depth, one of a "structuralist" and a second of a "rationalist." The concepts of "structuralist" and "rationalist" are considered complementary. Their underlying premise is included within the NGNP licensing approach described in the Report to Congress (see section A.5.1 above).

A.6 References

1. U.S. Nuclear Regulatory Commission, "Fire Protection Program for Operating Nuclear Power Plants; Final Rule," Federal Register, Vol. 45, No. 225, pg. 76602-76616, November 19, 1980.

2. U.S. Nuclear Regulatory Commission, "Reactor Site Criteria Including Seismic and Earthquake Engineering Criteria for Nuclear Power Plants; Final Rule," Federal Register, Vol. 61, No. 239 pg. 65157-65177 December 11, 1996.

3. U.S. Nuclear Regulatory Commission, "Risk-Informed Changes to Loss-of-Coolant Accident Technical Requirements; Supplemental Proposed Rule," Federal Register, Vol. 74, No. 152, pg. 40006-40052, August 10, 2009.

4 U.S. Nuclear Regulatory Commission, 'Safety Goals for the Operations of Nuclear Power Plants; Policy Statement', Federal Register, Vol. 51, No. 149, pp.28044-28049, August 4, 1986 (republished with corrections, Vol. 51, No. 160, pg. 30028-30023, August 21, 1986).

5. U.S. Nuclear Regulatory Commission, "Policy Statement on the Regulation of Advanced Reactors; Final Policy Statement," Federal Register, Vol. 73, No. 199, pg. 60612-60616, October 14, 2008.

6. U.S. Nuclear Regulatory Commission, "Policy Statement on Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," Federal Register, Vol. 60, No. 158, pg. 42622-42629, August 16, 1995.

7. SECY 2009-0056, "Staff Approach Regarding a Risk-Informed and Performance-Based Revision to Part 50 of Title 10 of the Code of Federal Regulations and Developing a Policy Statement on Defense-in-Depth for Future Reactors," April 7, 2009.

8. NUREG-1614, "U.S. Nuclear Regulatory Commission, FY 2008-2013 Strategic Plan,", U.S. Nuclear Regulatory Commission, Volume 4, February 2008.

9. Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk Informed Decisions on Plant-Specific Changes to the Licensing Basis," U.S. Nuclear Regulatory Commission, Revision 1, November 2002.

10. Regulatory Guide 1.183, "Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors," U.S. Nuclear Regulatory Commission, Revision 0, July 2000.

11. Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," U.S. Nuclear Regulatory Commission, Revision 2, March 2009.

12. Regulatory Guide 1.201, "Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to their Safety Significance," U.S. Nuclear Regulatory Commission, Revision 1, May 2006.

13. Nuclear Energy Institute 00-04, "10 CFR 50.69 SSC Categorization Guideline," Revision 0, July 2005.

14. Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)," U.S. Nuclear Regulatory Commission, Revision 0, June 2007.

15. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Section 19, *Use of Probabilistic Risk Assessment in Plant-Specific, Risk-informed Decisionmaking: General Guidance*, U.S. Nuclear Regulatory Commission, November 2002.

16. INSAG-10, 'Defense in Depth in Nuclear Safety,' International Atomic Energy Agency, 1996.

17. INSAG-12, "Basic Safety Principles for Nuclear Power Plants," International Nuclear Safety Advisory Group, October 1999.

18. Safety Reports Series, "Assessment of Defense in Depth for Nuclear Power Plants," No. 46, International Atomic Energy Agency, February 2005.

19. TECDOC-1570, "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs," International Atomic Energy Agency, September 2007.

20. "Next Generation Nuclear Plant Licensing Strategy – A Report to Congress," Joint Report of the U.S. Department of Energy and the U.S. Nuclear Regulatory Commission, August 2008.

21. NUREG-1860, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," U.S. Nuclear Regulatory Commission, December 2007.

22. Exelon Letter, Subject: Exelon Generation Company's Proposed Licensing Approach for the Pebble Bed Modular Reactor (PBMR) in the United States, August 31, 2001.

23. ACRS Memorandum, Subject: Historical Notes on Defense in Depth," Advisory Committee on Reactor Safeguards, October 15, 1997.

24. ACRS Letter, "The Role of Defense in Depth in a Risk-Informed Regulatory System," Advisory Committee on Reactor Safeguards, May 19, 1999.

Appendix B

Bibliography of Related Documents

Appendix B
Bibliography of Related Documents

B.1 Federal Register Notices

U.S. Nuclear Regulatory Commission, "Fire Protection Program for Operating Nuclear Power Plants; Final rule," *Code of Federal Regulations*, Office of the Federal Register, Vol. 45, No. 225, pp. 76602–76616, November 19, 1980.

U.S. Nuclear Regulatory Commission, "Reactor Site Criteria Including Seismic and Earthquake Engineering Criteria for Nuclear Power Plants; Final Rule," *Code of Federal Regulations*, Office of the Federal Register, Vol. 61, No. 239 pp. 65157–65177, December 11, 1996.

U.S. Nuclear Regulatory Commission, "Risk-Informed Changes to Loss-of-Coolant Accident Technical Requirements; Supplemental Proposed Rule," *Code of Federal Regulations*, Office of the Federal Register, Vol. 74, No. 152, pp. 40006–40052, August 10, 2009.

U.S. Nuclear Regulatory Commission, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement", *Code of Federal Regulations*, Office of the Federal Register, Vol. 51, No. 149, pp. 28044–28049, August 4, 1986 (republished with corrections, Vol. 51, No. 160, pp. 30028–30023, August 21, 1986).

U.S. Nuclear Regulatory Commission, "Policy Statement on the Regulation of Advanced Reactors; Final Policy Statement," *Code of Federal Regulations*, Office of the Federal Register, Vol. 73, No. 199, pp. 60612–60616, October 14, 2008.

U.S. Nuclear Regulatory Commission, "Policy Statement on Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," *Code of Federal Regulations*, Office of the Federal Register, Vol. 60, No. 158, pp. 42622–42629, August 16, 1995.

B.2 SECY Papers

SECY 1988-0203, "Key Licensing Issues Associated with DOE Sponsored Advanced Reactor Designs," July 15, 1988 (described in section 15.1.1 of NUREG-1338 (March 1989) as including discussion of DOE's "overall approach to the safety analyses, including considerations for defense-in-depth").

SECY 1998-0144, "White Paper on Risk-Informed and Performance-Based Regulation (Revised)," June 22, 1998, and SRM dated March 1, 1999.

SECY 1999-0186, "Staff Plan for Clarifying How Defense-in-Depth Applies to the Regulation of a Possible Geologic Repository at Yucca Mountain, Nevada," July 16, 1999.

SECY 2000-0198, "Status Report on Study of Risk-Informed Changes to the Technical Requirements of 10 CFR Part 50 (Option 3) and Recommendations on Risk-Informed Changes to 10 CFR Part 50.44 (Combustible Gas Control)," September 14, 2000, and SRM dated January 19, 2001.

SECY 2002-0057, "Update to SECY-01-0133, 'Fourth Status Report on Study of Risk-Informed Changes to the Technical Requirements of 10 CFR Part 50 (Option 3) and Recommendations on Risk-Informed Changes to 10 CFR 50.46 (ECCS Acceptance Criteria)'," March 29, 2002, and SRM dated March 31, 2003.

SECY 2005-0006, "Second Status Paper on the Staff's Proposed Regulatory Structure for New Plant Licensing and Update on Policy Issues Related to New Plant Licensing," January 7, 2005

(Attachment 3 provides a description of a model and approach for evaluation of defense-in-depth for new reactor designs).

SECY 2005-0138, "Risk-Informed and Performance-Based Alternatives to the Single-Failure Criterion," August 2, 2005, and SRM dated September 21, 2005.

SECY 2006-0217, "Improvement to and Update of the Risk-Informed Regulation Implementation Plan," October 24, 2006.

SECY 2009-0056, "Staff Approach Regarding a Risk-Informed and Performance-Based Revision to Part 50 of Title 10 of the Code of Federal Regulations and Developing a Policy Statement on Defense-in-Depth for Future Reactors," April 7, 2009.

B.3 Advisory Committee on Reactor Safeguards (ACRS) Letters

ACRS Letter, "Diversity," February 17, 1994.

ACRS Letter, "Probabilistic Risk Assessment Framework, Pilot Applications, and Next Steps to Expand the Use of PRA in the Regulatory Decision-Making Process," April 23, 1996.

ACRS Letter, "Risk-Informed, Performance-Based Regulation and Related Matters," August 15, 1996.

ACRS Letter, "Proposed Standard Review Plan Sections and Regulatory Guides for Risk-Informed, Performance-Based Regulation," March 17, 1997 (ACRS comments on development of guidance documents as "starting point for the integration of traditional engineering approaches to safety, such as defense-in-depth, and the new probabilistic approach").

ACRS Memorandum, "Historical Notes on Defense-in-Depth," October 15, 1997.

ACRS Letter, "Recommendations Regarding the Implementation of the Defense-in-Depth Concept in the Revised 10 CFR Part 60," October 31, 1997.

ACRS Letter, "Credit for Containment Overpressure to Provide Assurance of Sufficient Net Positive Suction Head for Emergency Core Cooling and Containment Heat Removal Pumps," December 12, 1997 ("margins in net positive suction head afforded by the DBA approach constitute a level of defense-in-depth").

ACRS Letter, "Treatment of Uncertainties Versus Point Values in the PRA-Related Decisionmaking Process," December 16, 1997 (recitation of historical use of defense-in-depth concepts).

ACRS Letter, "Proposed Commission Paper Concerning Options for Risk-Informed Revisions to 10 CFR Part 50 - "Domestic Licensing of Production and Utilization Facilities"," December 14, 1998.

ACRS Letter, "The Role of Defense in Depth in a Risk-Informed Regulatory System," May 9, 1999.

ACRS Letter, "Implementing a Framework for Risk-informed Regulation in the Office of Nuclear Material Safety and Safeguards," November 12, 1999.

ACRS Letter R-1893, "Use of Defense in Depth in Risk-Informing NMSS Activities," May 25, 2000.

ACRS Letter, "Nuclear Energy Institute Letter Dated January 19, 2000, Addressing NRC Plans for Risk-Informing the Technical Requirements in 10 CFR Part 50," July 20, 2000.

ACRS Letter, "Proposed Framework for Risk-Informed Changes to the Technical Requirements of 10 CFR Part 50," December 21, 2000.

ACRS Letter R-1997, "Policy Issues Related to Advanced Reactor Licensing," June 17, 2002.

ACRS Letter R-2013, "Draft Commission Paper on Policy Issues Related to Non-Light-Water Reactor Designs," December 13, 2002.

ACRS Letter R-2108, "Interim Letter – Regulatory Structure for New Plant Licensing: Technology-Neutral Framework," December 9, 2004.

ACRS Letter R-2244, "Technology-Neutral Framework for Future Plant Licensing," April 20, 2007

ACRS Letter R-2264, "Technology-Neutral Framework for Future Plant Licensing," April 20, 2007.

ACRS Letter R-2251, "Draft Commission Paper on Staff Plan Regarding a Risk-Informed and Performance-Based Revision to 10 CFR Part 50," May 16, 2007.

ACRS Letter R-2267, "Development of a Technology-Neutral Regulatory Framework," September 26, 2007.

NRC Presentation to ACRS, "Defense-in-Depth Policy Statement," December 5, 2008.

ACRS Letter, "Safety Evaluation for the Mitsubishi Heavy Industries Topical Report MUAP-07006-P, Revision 2, "Defense-In-depth and Diversity," Related to the US-APWR Design," June 25, 2009.

B.4 NUREGs

NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," U.S. Nuclear Regulatory Commission, March 1979.

NUREG-0553, "Beyond Defense-In-Depth: Cost & Funding of State & Local Government Radiological Emergency Response Plans & Preparedness in Support of Commercial Nuclear Power Stations," U.S. Nuclear Regulatory Commission, October 1979.

NUREG-1338, "Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)," U.S. Nuclear Regulatory Commission, (Draft) March 1989 (sections 15.3.3.4, "Evaluation of Defense-in-Depth" and 15.3.4.2, 'Adequacy of Defense-in-Depth").

NUREG-1860, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," U.S. Nuclear Regulatory Commission, December 2007 (sections 2.3, "Element 2: Defense-in-Depth"; 4, "Defense-in-Depth: Treatment of Uncertainties"; 8.2.4, "Defense-in-depth Considerations"; Appendix C.3.1, "Policy Issue – Defense-in-Depth"; Appendix E.3.2, "Selection of Defense-in-Depth Requirements"; and Appendices L.2.7.3 and L.2.8, industry comments on ANPR).

NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," U.S. Nuclear Regulatory Commission, December 1994.

B.5 Other Documents

IAEA Nuclear Energy Series No. NP-T-2.2, "Design Features to Achieve Defense in Depth in Small and Medium Sized Reactors," International Atomic Energy Agency, 2009.

Appendix C

Table of Cross References to PBMR Requests for Additional Information on Defense-In-Depth

Appendix C
Table of Cross References to PBMR Requests for Additional Information on Defense-In-Depth

This appendix provides a table that cross-references the responses to defense-in-depth "Requests for Additional Information" (RAIs) that were provided to the Nuclear Regulatory Commission (NRC) as part of the Pebble Bed Modular Reactor (PBMR) U.S. Design Certification program to the sections of this white paper where those responses are incorporated.[a]

RAI No.	RAI Statement	Section(s) in Which the Response Is Addressed
DID-1	It is stated (p.12) that "Programmatic Defense-in-Depth is also germane to the selection of design codes and standards for the PBMR..." However, Page 33 indicates that the selection of codes and standards is part of the plant capability defense-in-depth. Please explain the different characterizations of codes and standards treatment.	Section 3.2.3, footnote e.
DID-2	It is stated (p.26) that "...off-site emergency planning is a licensing consideration that is outside the scope of a design certification." Explain how the defense-in-depth framework and the probabilistic risk assessment (PRA) will be used to examine plant siting and emergency planning during applications for early site permits and combined licenses, given that the PRA only expresses accident consequences in terms of dose at the site boundary (PRA White Paper, Page 27).	The response provided was for a Design Certification application and is not directly applicable to the Next Generation Nuclear Plant (NGNP) Project, which will address an expected site(s). Emergency P is included as a level of defense-in-depth as indicated throughout this paper, including Sections 2.1.2, 2.2.2, 3.1.1, 3.2.2, and 3.2.3

a. Ref. PBMR Letter, Subject: Response to Requests for Additional Information, USDC20080321-1, Pebble Bed Modular Reactor (Proprietary) Ltd., March 21, 2008.

RAI No.	RAI Statement	Section(s) in Which the Response Is Addressed
DID-3	It is stated (p. 28) that "Defense-in-depth is an established philosophy in which multiple lines of defense and safety margins are applied to the design, operation, and regulation of nuclear plants to assure that the public health and safety are adequately protected." This definition is vague and not particularly helpful in understanding the PBMR approach to defense-in-depth because it does not provide a basis for deciding the necessity and sufficiency of defense-in-depth (e.g., How many multiple lines of defense are needed? What safety margin is adequate?). Please clarify your approach by revising your definition of defense-in-depth to include a basis for determining necessity and sufficiency. For reference purposes, the Commission-approved definition for defense-in-depth, as presented in the NRC's Strategic Plan is as follows: *"Defense-in-Depth: an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's Safety Philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility."*	Sections 2.3, 3.2, and 3.3
DID-4	The PBMR proposed approach for defense-in-depth (DID) apparently credits practically all engineering good practices and plant attributes (see Tables 2, 3, 6, and 9). How does the PBMR approach separate the additional plant features provided for defense-in-depth from the plant features needed to assure that the TLRC, RDC, and other acceptance criteria are met?	Section 3.2.3, footnote f.
DID-5	It is stated (p. 30) that the "Risk-Informed Evaluation of defense-in-depth is the structured use of information provided by the PRA to identify the roles of SSCs in the prevention and mitigation of accidents, to identify and evaluate uncertainties in the PRA results, to devise deterministic approaches to address these uncertainties, and to guide and provide risk insights to support deterministic judgments on the adequacy and sufficiency of defense-in-depth." However, the discussion on Pages 39–45 is limited to evaluating accident prevention and mitigation. Explain how deterministic judgment is used in the establishment of DID to compensate for uncertainties (in particular, completeness uncertainties) in the PRA.	In the NGNP approach for Risk-Informed Evaluation of defense-In-depth, this is accomplished using the process described in Figure 3-7 to demonstrate that there are adequate compensating measures to address these uncertainties. The set of deterministic principles derived from the regulatory foundation and summarized in Table 3-4 is used for this purpose. Hence, the Risk-Informed Evaluation of defense-In-depth incorporates both deterministic as well as probabilistic evaluations.

RAI No.	RAI Statement	Section(s) in Which the Response Is Addressed
DID-6	The white paper indicates an aspiration (p. 30) for a risk-informed and performance-based approach to defense-in-depth. The Commission's definition of a performance-based approach (NRC's Strategic Plan, NUREG-1614, Vol. 3) has a key provision that states (in part): "...a framework exists or can be developed in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern". What performance criteria other than dose at the site boundary exist to support defense-in-depth? Significant radiological dose at the site boundary implies that an immediate safety concern could occur if this criterion is the only measure used.	Section 3.1.1, footnote d.
DID-7	Discuss the "multiple barrier" approach defined by LWRs vs. HTGRs and their implications to defense-in-depth against fission product releases. Figures 7 and 8 indicate that the MHTGR (i.e., surrogate for the PBMR) barriers are multiple orders of magnitude different in their capabilities. All do not appear to be fully capable to meet dose acceptance criteria but are required multiple barriers that are all needed to meet acceptance criteria.	It is noted that this is true for all reactor designs. The examples given in the PBMR white paper for the MHTGR and the PWR, and repeated in this paper, both show that the roles of SSCs in preventing and mitigating releases including the roles of the barriers vary from sequence to sequence. In some sequences, prevention dominates and in others, mitigation prevails. The concept of barrier independence is met to varying degrees for any reactor design but is never fully reached for all barriers across the complete event sequence spectrum. There will always exist challenges to multiple barriers (e.g. seismic event that exceeds the seismic design capacity) that can be postulated. By applying the defense-in-depth principle of barrier independence, these challenges need to be systematically identified and prevented as much as possible. The technology of PRA provides a systematic way to identify these challenges so that compensating measures can be addressed to minimize their safety significance.
DID-8	The PBMR approach (p. 40) relies heavily on the defense-in-depth principles from Standard Review Plan (SRP) Chapter 19. These are principles that are to be maintained given a licensing change (e.g., design change) to the plant. These principles assumed that there is already adequate DID, and as such, does not define what is meant by DID. For a new design, an explicit definition of DID is needed, and therefore, the criteria for determining when there is enough DID (i.e., the basis for defining the minimal needed DID). Please provide such a definition and basis.	Section 3.2.4.3, footnote h.

RAI No.	RAI Statement	Section(s) in Which the Response Is Addressed
DID-9	It is stated (p. 40) that "Prevention strategies as defined as those strategies that are employed to reduce the frequency of accidents by improving the reliability of SSCs whose failure would cause initiating events and/or adversely affect the ability to mitigate an event sequence. Mitigation strategies are those that are employed to improve the capability of SSCs that serve to mitigate the consequences of events and event sequences that may challenge them." Figure 7 (p. 53) makes these definitions explicit by indicating that, in the PBMR, "prevention" refers to reducing the accident sequence frequency and "mitigation" refers to reducing the accident sequence consequences. Explain why these definitions are chosen over the ones traditionally used for LWRs, e.g., "accident prevention" refers to preventing core damage and can be assessing by examining the core damage frequency (CDF), and "accident mitigation" refers to preventing offsite releases, and can be assessed by examining the large early release frequency (LERF). Would it be helpful to define "prevention" in terms of frequency of significant releases from the fuel, and "mitigation" in terms of frequency of significant releases to the environment?	The safety design approach for the NGNP facility has addressed prevention of large releases from the fuel by selection of inherent reactor characteristics and design selections that have enabled prevention of large releases from the fuel by passive means. It is recognized, however, that the HTGR has the potential for accidents that could result in a release of radioactive material, not only from the fuel but from other sources. The prevention-mitigation model described above is more general than the one used on current LWR designs exclusively using active safety systems and hence provides a more complete coverage of accidents, whether there is core damage or not. This model can also be used to address non-core sources of radioactive material and is technology neutral. There is a risk of leaving something out if prevention would only consider core damage. By the same token, there is in principle no exclusion of event sequences using the above model.
DID-10	Referring to Table 5 (p. 43), how is the table used in practice? Will the design certification application include documentation that identifies the plant features that provide defense-in-depth, classifies them as either plant capability or programmatic, provides their risk reduction factors, demonstrates that they meet the defense-in-depth principles listed in Table 5, etc.? For example, how will it be demonstrated that there is not over-reliance on programmatic approaches to compensate for design weaknesses (i.e., the principle in Table 5). How does engineering judgment factor into this demonstration?	Section 3.4, Table 3-8
DID-11	Discuss how the PBMR defense-in-depth approach addresses aspects of the plant design that have unknowingly been omitted from the risk analysis (i.e., the "unknown unknowns").	Appendix D, Section D.1.16, footnote t.
DID-12	The staff finds that Figure 5 (p. 44) is not consistent with parts of the discussion in the paper. Please revise or clarify Figure 5 to make it consistent with the discussion in the white paper.	Section 3.2.4.3, Figure 3-7
DID-13	What is the role of the single failure criterion in the PBMR's defense-in-depth framework? Is it the intent of the white paper to propose a risk-informed alternative to the single failure criterion? If so, please articulate and justify that alternative. As context for developing the responses, it may be useful to consider the alternatives the staff has identified in SECY-05-0138, "Risk-Informed and Performance-Based Alternatives to the Single-Failure Criterion."	Appendix D, Section D.1.14, footnote r.
DID-14	For each LBE in each event category, do the SSCs that provide defense-in-depth have sufficient capability to meet the TLRC when the credited SSCs (e.g., the safety-related SSCs for DBAs) are assumed to fail? For LBEs in general, discuss the level of performance capability that will be required by the SSCs performing a defense-in-depth role to ensure that the TLRC and other criteria are met.	Appendix D, Section D.1.14, footnote s.

Appendix D

Expanded Description of Process for Risk Informing the Design

Appendix D
Expanded Description of Process for Risk Informing the Design

The following subsections provide an expanded discussion of the specific 16 sub elements of the approach in Figure D-1 to risk-inform a design.

D.1 Initial Deterministic Elements of Design Approach

D.1.1 Design and Technology Development Process (Box 1 in Figure D-1)

The process begins in Box 1 with an initial design. The design and technology development process is illustrated in Figure D-1, which shows the initial design and design evaluation activities that are completed as part of the Next Generation Nuclear Plant (NGNP) preconceptual design. Top level requirements are formulated with input from all stakeholders, including user requirements for such things as energy production, capital costs, operating and maintenance costs, safety, availability, investment protection, siting, and commercialization requirements. This approach is an integrated, iterative, and systematic top-down process. Technology development is identified in order to validate design assumptions and enhance confidence that user requirements will be satisfied.

The selection of the inherent reactor characteristics for the NGNP Project, those characteristics of a modular high temperature gas-cooled reactor (HTGR) including the power level, fuel, moderator, negative moderator temperature coefficient and inert helium coolant, are primarily driven by user requirements for a reactor that can safely deliver process heat using proven technology at required temperatures and pressures as well as an achieving efficient co-production of electricity. Examples of the kinds of decisions that are made in this step include selection of the thermodynamic cycle, parameters of the cycle and energy balance, and evaluation of options such as fuel type (pebble or prismatic), indirect versus direct cycle, passivel versus active safety systems, working fluids for secondary cycles, selection of materials and design codes for major structures, systems, and components (SSCs), and other high level design decisions driven by the top level requirements and results of the trade studies. The decision to use inherent characteristics and passive SSCs as the primary means of assuring safety functions, supplemented by active systems that add the defense-in-depth to the prevention and mitigation of events are requirements of particular relevance to this design.

D.1.2 Definition of Plant and System Functional Requirements (Box 1 in Figure D-1)

At an early stage of design, a comprehensive set of plant level and system level functional requirements are developed. Examples of plant level requirements include requirements for passive and active fulfillment of functions, plant cost, plant availability, plant investment protection requirements, construction schedule, load following versus base load, etc. This step includes the identification of systems and components and their functions, including energy production functions, maintenance functions, auxiliary functions, and safety functions. This is a purely deterministic step that produces a definition of the design in sufficient detail to begin the Probabilistic Risk Assessment (PRA).

---

1. See Section 3.3.1 for discussion on inherent and passive design features.

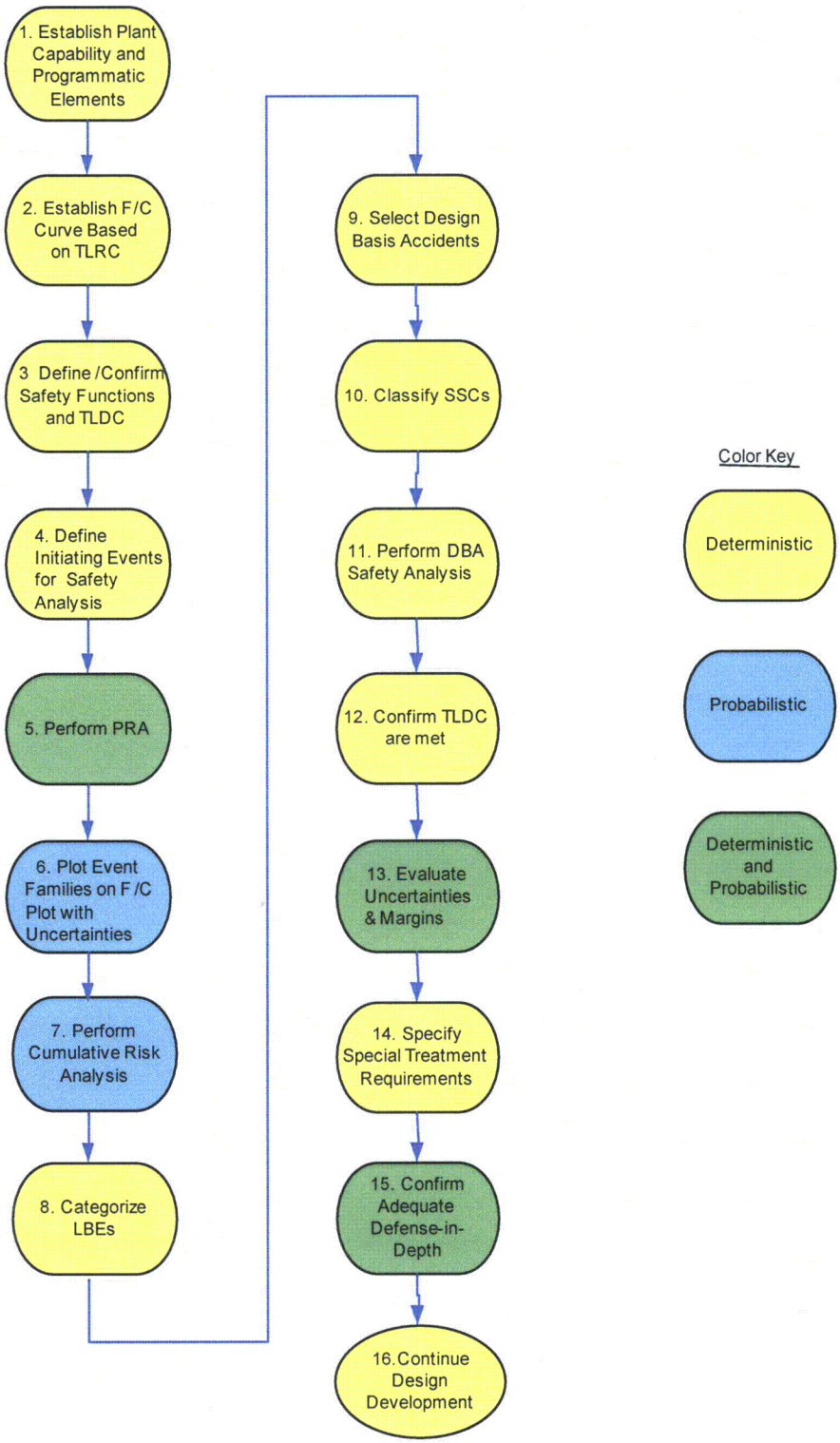


Figure D-1. Risk-informed performance-based design process.

D.1.3 Determination of Initial Modes and States (Box 1 in Figure D-1)

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

D.1.4 Incorporation of Defense-in-Depth Capabilities in Initial Design (Box 1 Figure D-1)

By the time the steps listed in the previous sections are performed, the design process will have defined the major elements of its plant capabilities for defense-in-depth as well as an initial selection of codes and standards that form part of the programmatic defense-in-depth. By addressing the fundamental top level requirements operability, availability, maintainability, and investment protection features for the design, using conventional practices and industry codes and standards, a great deal of the defense-in-depth capability is naturally established. It is noted that additional plant capabilities as well as programs and compensating measures may be added as a result of subsequent probabilistic and deterministic evaluations in subsequent steps.

D.1.5 Establish Baseline Special Treatment per Code (Box 1 in Figure D-1)

Initially, the designer makes decisions on both the design and selection of codes and standards that influence design and some baseline level of special treatment. For example, the designer may select certain parts of the American Society of Mechanical Engineers (ASME) design code for certain SSCs which may be linked to ASME requirements for in-service inspection. Provisions must then be made in the design and the definition of modes and states to perform the required inspections. Final decisions on the frequency and extent of inspections will be made later in Box 14 of Figure D-1. The full extent of special treatment is defined later following the evaluation of licensing basis events (LBEs) and the selection of SSC safety classes for each SSC. Hence, selection of codes and standards supports both the plant capabilities for defense-in-depth and the programs that contribute to the overall defense-in-depth.

D.1.6 Frequency-Consequence Curve (Box 2 in Figure D-1)

In Box 2, a set of frequency versus dose criteria are selected as a reference boundary for assessing the integrated design level of safety. The frequency consequence (F-C) Curve defines the limits to be used to evaluate the frequency and consequences of the LBEs. In this approach, the term top level regulatory criteria (TLRC) is used to refer to the set of criteria from the existing body of regulations and guidance that are used to derive the consequence limits on the F-C Curve. The following primary sources have been identified in selecting criteria for setting limits on the risk or consequences of potential radiological releases from nuclear power plants in the United States:

- Reactor Safety Goal Policy Statement [7]: This policy limits public safety risk resulting from nuclear power plant operation. Limits are stated in the form of the maximum allowable risk of immediate death and the risk of delayed mortality from exposure to radiological releases of all types from nuclear power plants.
- 10 CFR Part 20, "Standards for Protection against Radiation (Subpart D, Radiation Dose Limits for Individual Members of the Public)": These criteria limit the dose consequences of releases associated with relatively high frequency events that occur as part of normal plant operations.
- 40 CFR Part 190, "Environmental Radiation Protection Standards for Nuclear Power Operations": These standards provide the generally applicable exposure limits for members of the general public

from all operations, except transportation and disposal or storage of spent fuel associated with the generation of electrical power by nuclear power plants.

- 10 CFR Part 100, "Reactor Site Criteria (Subpart B, Evaluation Factors for Stationary Power Reactor Site Applications on or After January 10, 1997)": §100.20 defines the exclusion area boundary (EAB) and low population zones of a nuclear reactor site, and requires that the combination of the site and reactor located on that site be capable of meeting the dose and dose rate limitations set forth in 10 CFR §50.34(a).
- 10 CFR §50.34(a)(ii)(D), "Contents of Applications: Technical Information (Radiological Dose Consequences)": This section of the regulation specifies dose limits for evaluating the acceptance of the engineered safety features that are intended to mitigate the radiological consequences of accidents. These dose limits are consistent with those utilized in 10 CFR Part 100 for determining the extent of the EAB and Emergency Planning Zone (EPZ).

Frequency consequence criteria from these guidelines are used to represent the TLRC for judging the acceptability of the frequency and consequence of each LBE. Figure D-2 depicts the F-C Curve developed for the NGNP Project based on these guidelines. The white paper on LBE Selection (to be submitted, see Section 1.6) will describe the basis for the event frequency and consequence limits used.

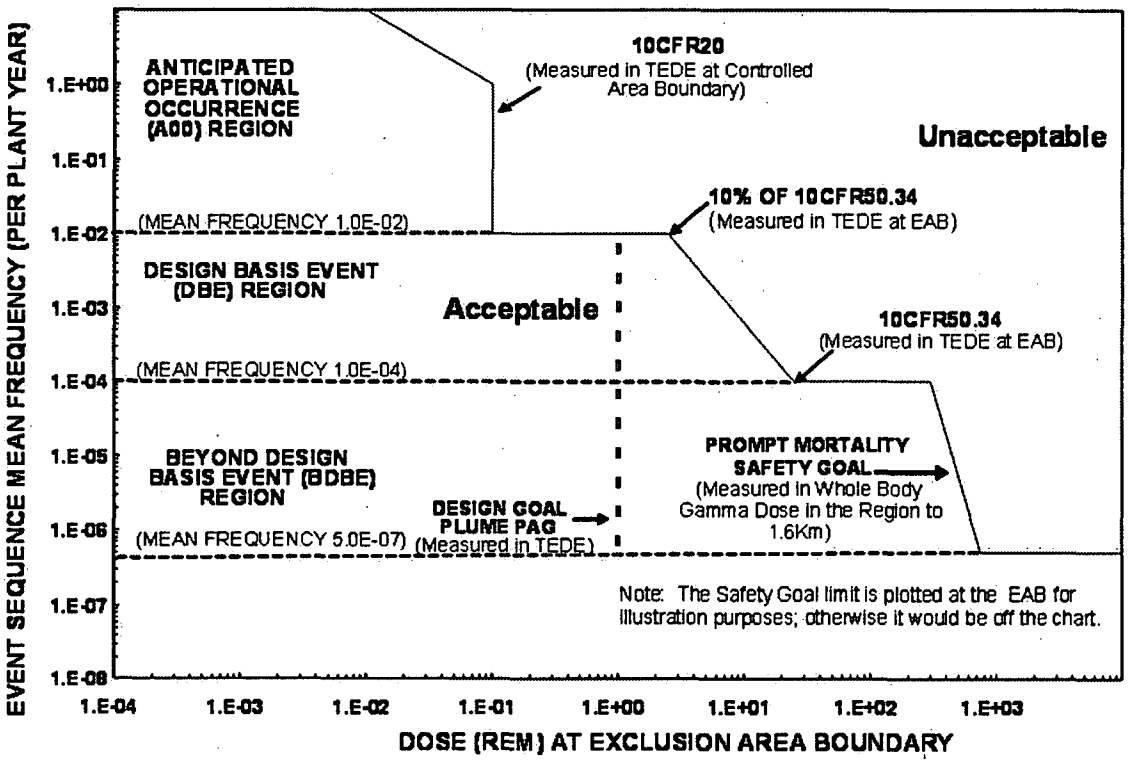


Figure D-2. NGNP frequency-consequence curve.

D.1.7 Definition of Safety Functions (Box 3 in Figure D-1)

The plant designer defines the reactor specific safety functions as represented in Box 3. All reactors are designed to meet certain fundamental safety functions such as containment of radioactive material, decay heat removal, and reactivity control. However, application of the reactor specific safety design approach leads to a set of reactor specific safety functions that achieve the fundamental safety functions.

During this process the designer confirms the allocation of these safety functions to both passive and active SSCs. In Box 3 the top level design criteria are also confirmed for all the SSCs selected to perform the reactor specific safety functions. By the time Box 3 is completed the plant capabilities that support defense-in-depth are largely determined. Adjustments may be made in later steps to address the results of subsequent evaluations that may expose weaknesses in design or operating assumptions, or expose margin uncertainties that are insufficient to demonstrate adequate levels of safety and sufficient defense-in-depth. All functions associated with the prevention and mitigation of accidents are referred to in the design approach as safety functions. SSCs that perform safety functions are not necessarily, but may become, classified as safety-related; however, that is determined in a later stage of design.

Figure D-3 illustrates the top-level safety functions for many HTGRs with emphasis on the safety functions for the reactor sources of radioactive material and includes functions needed for radiological protection of both the public and onsite personnel. These functions are considered HTGR examples, since the NGNP design is still evolving. Other functional diagrams may be required for issues such as security and safeguards or emergency planning.

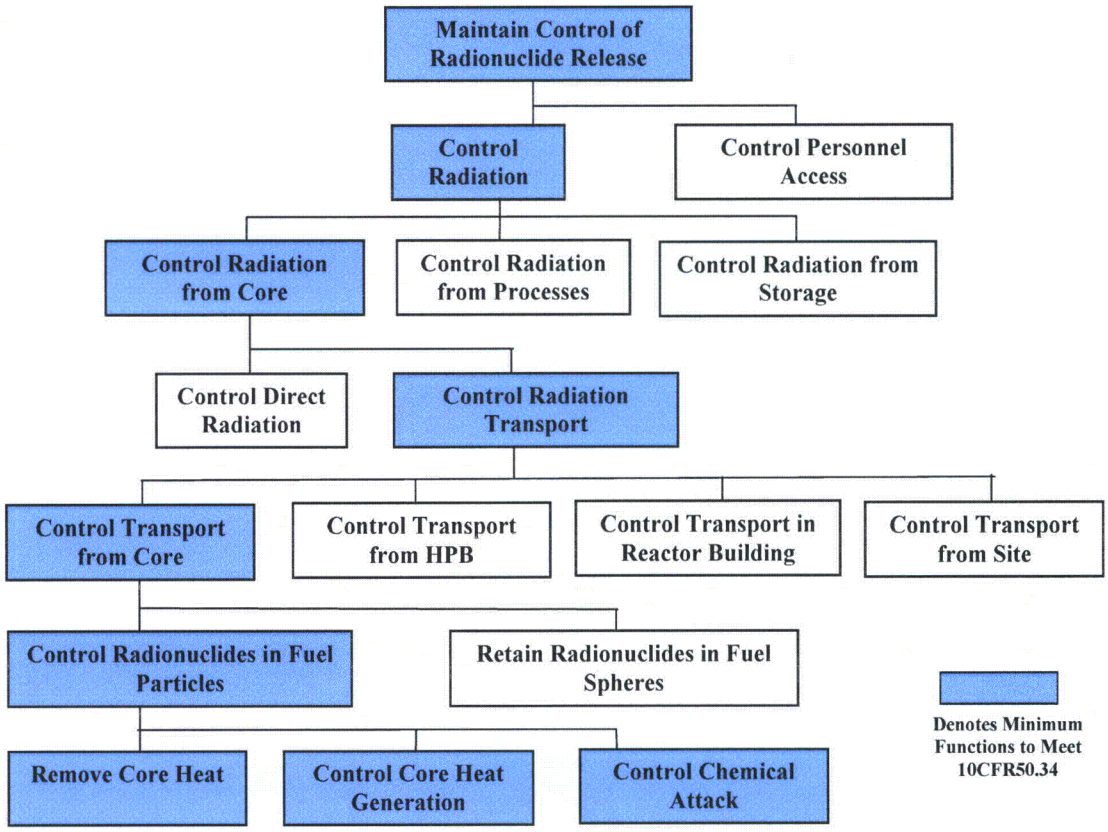


Figure D-3. Example safety functions for an HTGR.

As shown, the design includes functions for radionuclide retention within the fuel particles, fuel spheres, helium pressure boundary (HPB), reactor building, and site. Not all of the functions in Figure D-3 are required in order to meet the TLRC. Safety analyses are performed in Box 11 of Figure D-1 to determine which are the required safety functions for the reactor sources, as identified as the minimum subset that is shaded, to keep the consequences for the deterministically selected Design Basis Accidents (DBAs; defined in Box 9 of Figure D-1) within the offsite dose limits of 10 CFR §50.34. The functions shown without shading are not required, but are included in the design to contribute to the plant capabilities for defense-in-depth or to control smaller, nonlimiting sources of radionuclides, and to meet user requirements for plant availability and investment protection. The required safety functions for the NGNP design include those to:

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

D.1.8 Selection of SSCs to Perform Safety Functions (Box 3 of Figure D-1)

For the NGNP Project, safety functions are performed by combinations of inherent reactor characteristics (e.g., large core heat capacity so prevent rapid changes in core temperature), passive design features and SSCs (e.g., passive means of removing reactor decay heat), and active SSCs (e.g., use of circulators and water cooled heat exchangers to remove decay heat). This approach to performing safety functions is an example of the application of diversity in reactor safety design. In Section 3.3, a more detailed discussion of the specific inherent, passive, and active means to perform each safety function are described.

D.1.9 Top-Level Design Criteria Development (Box 3 in Figure 3-3)

The approach to development of the Top-Level Design Criteria (TLDC) is that TLDC define design requirements necessary to ensure that TLRC and defense-in-depth objectives are met.

D.1.10 Selection of Off-Normal Initiating Events and Event Sequences (Boxes 4 and 5 in Figure D-1)

Once the safety design approach is defined and safety functions confirmed through Box 3, the events that are considered for safety protection can be examined, as shown in Box 4. This includes the initial deterministic evaluation of the plant response to events as well as the systematic search for initiating events that challenge the radionuclide barriers and SSCs that perform the safety functions. The operating and shutdown modes, safe intermediate operating states, internal and external initiating events, event sequences, and end states that need to be considered in both the probabilistic and deterministic safety analyses are defined through this step. Recognizing the "chicken and egg" nature of this process, the expanded definition of event sequences for safety protection helps to refine the requirements for the design and confirmation or formulation of the TLDC for SSCs. Part of the iterative nature of this process is that certain special treatment requirements are defined or confirmed to support the validity of screening out initiating events or event sequences from the safety analyses (e.g., catastrophic vessel failures may be precluded by applying certain requirements, codes, and standards to reduce the likelihood of such events below a level of concern in the risk-informed performance-based [RIPB] process). It is important to note that all the decisions up through Box 4 represent fully deterministic elements of the RIPB design approach.

In the initial stages of the design, an evaluation is made to decide which initiating events and event sequences to consider within the design basis and for designing specific measures to prevent and to mitigate off normal events and accidents. This selection uses existing standards and guidance (including regulatory) supplemented by operating experience for similar equipment in different industries. It is later refined in the PRA on the basis of the more rigorous approach to SSC reliability and failure frequency determinations and more complete event sequence definition. The approaches to selecting initiating events and defining the possible event sequences that result from them are inherently deterministic and are initially made by the designer. Later, when the deterministic safety analyses and PRA are performed, the list of initiating events evolves, becoming more refined and achieving a greater level of completeness.

The primary methods used to accomplish the selection of initiating events include the deterministic tools such as Hazops, failure modes and effects analysis, and Master Logic Diagram methods. An example Master Logic Diagram is shown in Figure D-4.[m]

The boxes of Figure D-4 in Steps 2–5 represent a structured set of FMEAs to identify failure modes and causes of failure (challenges) focused on barriers and structures on the left hand side and systems and components that perform safety functions on the right hand side. These internal failure modes are supplemented by input from separate evaluations of internal and external plant hazards to compile an exhaustive list. While this diagram is a product of procedures developed for performing a PRA, it makes use of established deterministic system engineering methods for identification of events to consider in the design. This process is performed initially to support the design and is later refined in support of the PRA. As the level of design maturity advances, the level of detail in the resolution of the events and its completeness advances. The process includes identification of events that can be made deterministically, i.e., via a peer review process that can challenge the completeness of the events. Other events may be defined in regulatory reviews for analysis to explore sensitivities or other uncertainties including beyond design basis event (BDBE) sequences. Steps 7 and 8 are completed as part of the PRA. Prior to performance of the PRA, the compiled list of initiating events is used to select an initial set of prospective LBEs from which to make some of the basic design decisions. Examples of these basic decisions include decisions for the sizes and locations of HPB breaks to assume for an initial set of DBAs. This process leads to a list of initiating events that can be grouped into functional categories.

Examples of Initiating Event Functional Categories include:

- Transients with intact HPB examples:
  - +Heat transport system (HTS) and shutdown cooling system (SCS) still capable of forced cooling operation
  - HTS failed, SCS still capable of operation
  - HTS and SCS not capable of operation
- Transients with intact HPB and reactivity addition examples:
  - Control rod or group withdrawal
  - Overcooling transients
- HPB Leaks and Breaks (excl. HPB HX failures) examples:
  - Range of break sizes from small leaks up to complete breaks of HTS piping
  - Range of break locations with different potential for HTS retention, He-air gas-exchange, and pressure and temperature loads on reactor building

m. This diagram is depicted as Figure 2 in the US Design Certification PBMR white paper on PRA [Ref. 2].

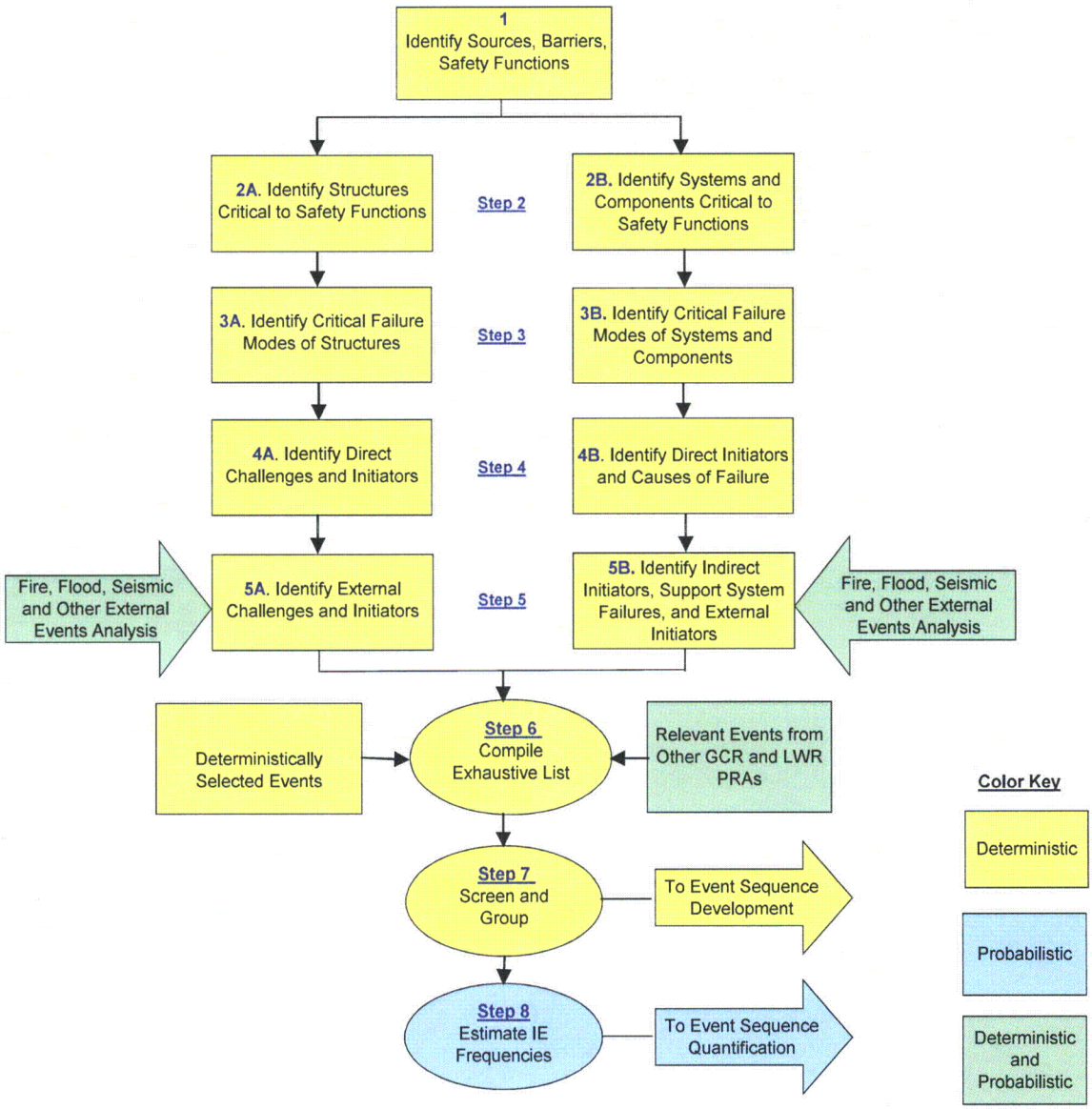


Figure D-4. Master logic diagram for selection of initiating events.

- HPB heat exchanger failures examples:
  - IHX failure
  - Steam generator failure
  - SCS heat exchanger failure.
- Initiating events specific to radionuclide sources outside the HTS boundary, including spent fuel, helium purification, gas waste, etc.
- Functional initiating events that may be caused by internal events, internal plant hazards, or external events including seismic events and process hazards.

D.1.11 Initial Development of PRA from Basic Design Information

In Box 5 of Figure D-1 above, probabilistic elements are introduced in the performance of the PRA. The PRA is not considered a purely probabilistic process because PRA models, particularly those used to systematically identify initiating events, evaluate the plant response to events, and construct event sequences are based on deterministic evaluations of the plant design performed in Box 4. Safety analysis done for the PRA is done on a "best estimate" basis with quantified uncertainties.

For the NGNP Project, the PRA is formally introduced in the conceptual design stage when enough system information becomes available. However the tools and methods of PRA have already been partially exercised in the initial selection of events in Box 4 of Figure D-1.[n] The PRA will address the guidance in the ASME PRA Standard for Advanced Non-LWRs when that standard is completed.[D-1] The PRA itself is classified as an element of the risk-informed and performance-based design approach that contains both deterministic and probabilistic elements. This is true because the PRA is not developed independently but rather is built on the deterministic foundations already completed in Boxes 1-4 in Figure D-1. A more complete depiction of the feed streams into the PRA is shown in Figure D-5.

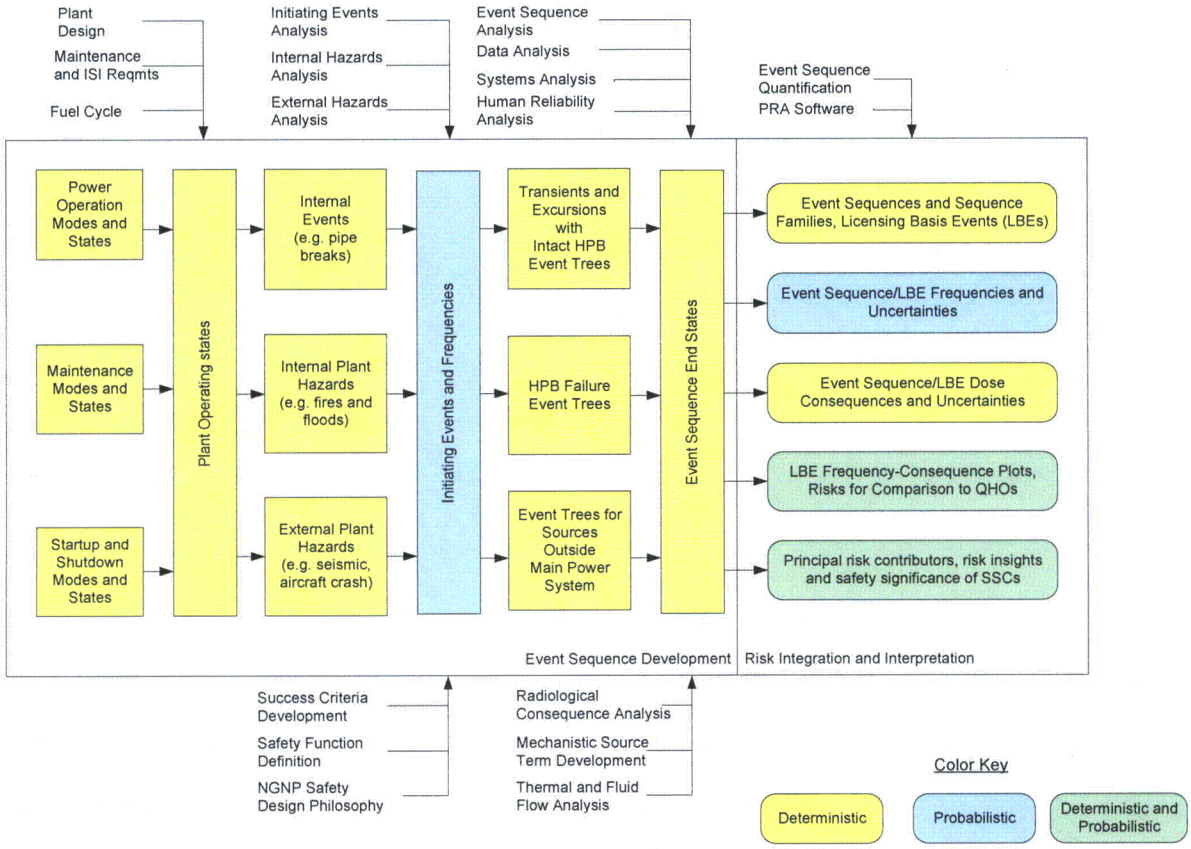


Figure D-5. Overview of PRA elements.

When the PRA is performed, many of the elements of the PRA itself require performance of analyses that are clearly deterministic in nature. This is seen upon examination of Figure D-5 and Table D-1 which breaks the PRA down into its constituent elements as defined in the referenced draft PRA standard.[D-1] It is

n. The PRA approach for the NGNP is the same as that described in the PBMR US Design Certification white paper on PRA.[2]

seen in this table that most of the elements of a PRA, especially those aspects associated with the definition of event sequences and evaluation of the consequences of the event sequences are applications of deterministic processes. It is only those aspects associated with the quantification of event frequencies and probabilities that are regarded as probabilistic.

Table D-1. Evaluation of the deterministic bases for the PRA.

PRA Element	Deterministic Basis
Definition of plant operating states	All of this element is deterministic
Initiating events analysis	Identification and grouping of events is deterministic; estimation of IE frequencies is probabilistic
Event sequence development	All of this element is deterministic
Success criteria development	All of this element is deterministic
Thermal and fluid flow analysis	This element is deterministic, except for the potential statistical treatment of input data
Systems analysis	All of this element is deterministic except for the quantification of failure mode probabilities
Data analysis	All of this element is probabilistic
Human reliability analysis	All of this element is deterministic except for human error rate estimation
Internal flooding analysis	All of this element is deterministic except for flood initiating event frequency estimation
Internal fire analysis	All of this element is deterministic except for fire initiating event frequency estimation
Seismic risk analysis	Contains a mixture of deterministic and probabilistic aspects that are difficult to separate
Other external events analysis	Contains a mixture of deterministic and probabilistic aspects that are difficult to separate
Event sequence frequency quantification	All of this element is probabilistic
Mechanistic source term analysis	The mechanistic source term models are deterministic; the evaluation of uncertainties is probabilistic
Radiological consequence analysis	Most of this element is probabilistic
Risk integration and interpretation of results	Contains a mixture of deterministic and probabilistic aspects that are difficult to separate
Peer review	Peer review covers both the probabilistic and deterministic aspects

The NGNP PRA has an extensive deterministic basis similar to PRAs on existing and advanced light water reactor (LWR) plants. The primary difference is that the vast majority of the plant and SSC performance data to provide the deterministic bases for the LWR PRAs predates the risk studies. By contrast, for new reactors, some of the deterministic and probabilistic bases are being developed in parallel.

For the NGNP Project, the scope of the PRA for radiological consequences includes site boundary doses as well as the capability to evaluate the risk metrics for demonstrating conformance to the safety

goal quantitative health objectives (QHOs) as well as to evaluate alternative approaches to establishing the EPZ and for meeting the emergency planning requirements.[o]

D.1.12 Integration of Risk Insights into the Design Process

The purpose of this section is to summarize the RIPB licensing approach, which includes those elements with an important role in NGNP licensing. An overview of that approach and the questions addressed in each step is provided in Table D-2.

Table D-2. Risk-informed performance-based licensing approach.

Elements of Approach	Purpose
F-C Curve derived from Top Level Regulatory Criteria	Establish what level of safety must be achieved in terms of the frequencies and radiological doses of event sequences
LBEs	Define when and under what conditions the F-C Curve must be met based on event sequences selected from the PRA
Reactor specific safety functions Safety classification of SSCs TLDC	Establish how it will be assured that the TLRC are met
Analysis of deterministic DBAs Special treatment requirements Plant capability defense-in-depth Programmatic defense-in-depth	Provide assurance that the TLRC (i.e., radiological dose criteria) are met. Provide assurance that performance and safety criteria will be met over the plant lifetime.

D.1.13 LBE Development (Boxes 6, 7, 8, and 9 in Figure D-1)

The approach to define LBEs includes the probabilistically defined events derived from information developed in the PRA as well as the deterministically defined DBAs. The approach, to be described in more detail in a future paper (see Section 1.6), is summarized below.

In Box 6 the results of the PRA are organized by forming event families with similar common characteristics, i.e., initiating event challenge type, safety system response, and plant end state, and plotting the frequencies, doses, and uncertainty ranges on the F-C Curve. These families are referred to as LBEs. 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. Note that for a multi-module plant, the end state includes the number of reactor modules involved in 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 a combination would mask the definition of unique challenges to the SSCs that perform safety functions.

---

o. In their review of the PBMR US Design Certification white paper on Defense-in-Depth[5] the NRC staff in RAI DID-2 questioned how emergency planning considerations would be addressed given the perception that the PRA would only include site boundary doses.

- 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.
- 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.

A common situation that yields accident 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.

In Box 7 the LBEs are categorized based on frequency of occurrence. Events are categorized based on their mean frequency of occurrence for further analysis under rules appropriate for their category. The categories are:

- Anticipated Operational Occurrences (AOOs)—Event Sequence Frequencies >10-2 per plant year
- Design Basis Events (DBEs)—Event Sequence Frequencies between 10-2 and 10-4 per plant year
- Beyond Design Basis Events (BDBEs)—Event Sequence Frequencies between 10-4 and 5×10-7 per plant year.

The deterministic DBAs are selected based on conservative rules that address uncertainties exposed by the PRA as well as events selected to evaluate the protection against physical security threats. The deterministic DBAs are subjected to deterministic safety analyses comparable to those performed on existing plants.

A confirmation that the cumulative risks from reactor events are in conformance with the NRC Safety Goal Quantitative Health Objectives is performed in Box 8.

In Box 9, deterministic judgment is applied to select the subset of the LBEs that will be further examined as DBAs. One of these deterministic rules is that only safety related SSCs are credited for prevention or mitigation in DBA analyses.

D.1.14 SSC Classification Validation (Box 10 in Figure D-1)

The approach to the classification of SSCs, to be described in more detail in a future paper (see Section 1.6) is summarized here. In Box 10, the designer then examines the options for which SSCs to select as safety-related and therefore be considered in the DBA analysis. These are deterministic judgments that consider the existing levels of redundancy and diversity in the design as well as economic and other issues.

This approach includes three categories of safety classification for SSCs[p]:

- Safety-Related (SR):
  - This category is for SSCs relied on to perform required safety functions to mitigate the public consequences of Design Basis Events (DBEs) to comply with the dose limits of 10 CFR §50.34.

---

p. The NGNP approach to SSC safety classification is based on the approach described in the PBMR US Design Certification white paper on safety classification of SSCs.[4]

- This category is also for SSCs relied on to perform required safety functions to prevent the frequency of Beyond Design Basis Accidents (BDBEs) with consequences greater than the 10 CFR §50.34 dose limits from increasing into the DBE region.

- Non-Safety-Related with Special Treatment (NSRST):
  - This category is for SSCs relied on to perform safety functions to mitigate the consequences of AOOs to comply with the offsite dose limits of 10 CFR Part 20.
  - This category is also for SSCs relied on to perform safety functions to prevent the frequency of DBEs with consequences greater than the 10 CFR Part 20 offsite dose limits from increasing into the AOO region.
- Non-Safety-Related with No Special Treatment:
  - This category is for all SSCs not included in either of the above two categories.

In implementing this approach for the NGNP Project it is noted that any SSC that is classified as SR or NSRST is subjected to special treatment[q,r,s] Only those SSCs whose reliability and capability do not

---

q. This issue was the subject of RAIs SSC-1, SSC-3, SSC-12 and SSC-13 in NRC's review of PBMR's white paper on safety classification of SSCs.[4] The NGNP approach is consistent with the suggestion by the NRC in this RAI to the extent that only the SR and NSRST SSCs are viewed as playing a significant defense-in-depth role. E.g., Any SSCs whose reliability and/or capability play a role in the prevention and mitigation of an accident play a defense-in-depth role and are within the scope of SSCs modeled in the PRA.

r. In RAI DID-13, the NRC staff questioned the role of the Single Failure Criterion (SFC) in the proposed defense-in-depth framework and whether the intent was to propose a risk-informed alternative. The SFC as historically understood is applied in the context of a purely deterministic approach to selection of LBEs in which quantitative estimates of event frequencies are not addressed and in which common cause failures are not considered. Since the proposed risk-informed design and analysis approach includes both deterministic and probabilistic elements that address these exclusions and the reliability intended to be obtained from application of the SFC, the NGNP approach does not include the application of a single failure criterion. The purpose of applying the historic SFC is the provision for redundancy in active systems that perform required safety functions. The NGNP project will address the need for redundancy on a case-by-case basis as needed to achieve the necessary and sufficient degree of reliability to perform the required safety functions. Some systems classified as safety-related will in fact satisfy the SFC. For example, NGNP will have redundant reactor shutdown systems and will have redundant active and passive core cooling systems. However, the decisions to implement redundancy will be made and justified on a case-by-case basis. As a matter of standard reactor design practice and as provided in Appendix A of 10 CFR §50, redundancy is not required for passive SSCs that perform safety functions. Defense-in-depth in passive SSCs is addressed by other means such as design margins and conservative analyses to demonstrate performance. The alternatives to the SFC considered by the staff in SECY-05-0138 have been reviewed relative to the NGNP project. It is difficult to make comparisons between the NGNP risk-informed and performance-based licensing approach and the alternatives to the SFC considered in SECY-05-0138. First the starting point for this SECY is the historical background of an LWR safety design approach that is based on the use of active safety functions to mitigate a deterministically derived set of design basis accidents to which the SFC has already been applied. Risk-informed alternatives to the SFC are then evaluated in the context of managing the beyond design basis risk metrics of CDF and LERF. SECY-05-0138 acknowledges the difficulties and inconsistencies in applying the SFC to passive systems which are emphasized in the NGNP safety design approach. The SECY also acknowledges that meeting the SFC may not be sufficient to meet certain reliability based targets and there may be advantages to extending the SFC to safety significant, non-safety related systems. Among the alternatives considered in SECY-05-0138, the NGNP approach probably is most comparable to Alternative No. 3, "Replace SFC with Risk and Safety Function Reliability Requirements". In the NGNP approach to SSC classification and special treatment, SSC reliability requirements are derived based on the need to maintain each category of LBE within their prescribed LBE frequency and dose limits, and in this sense may be compared to Alternative No. 3 in the SECY. However, in the case of the NGNP the need to maintain reliability and capability requirements is not an option to the SFC but rather a fundamental requirement. The application of redundancy in the NGNP approach, in which case a SFC would be met by default, is simply one of a wide set of design approaches that would be available to meet the required reliability targets. In addition, in the NGNP approach, the incorporation of redundancy or diversity is not necessarily limited to safety classification of SSCs, but also as means for assuring operational reliability and investment protection.

s. In a related question, the NRC staff asked in RAI DID-14 for each LBE in each event category, whether the SSCs that provide defense-in-depth have sufficient capability to meet the TLRC when the credited SSCs (e.g., the safety-related SSCs for DBAs) are assumed to fail? SSCs in each category provide a role in defense-in-depth, either prevention, mitigation, or

influence the capability to meet the TLRC are not subject to special treatment requirements. There are many SSCs in existing reactors that play a role in the prevention or mitigation of accidents that are not classified as safety related (e.g., main feed-water, condensate, and circulating water systems that offer a means of decay heat removal).

D.1.15 Performing DBA Analysis (Boxes 11 and 12 in Figure D-1)

In Boxes 11 and 12 the deterministic safety analyses of the DBAs are performed and a confirmation is made that the TLDC have been met. DBAs are reanalyzed using safety analyses methods and models that have undergone an extensive verification and validation process in accordance with Regulatory Guide 1.203, "Transient and Accident Analysis Methods,"[2] and analysis conducted with conservative rather than best-estimate assumptions consistent with the requirements of Chapter 15 of the NGNP Safety Analysis Report.

D.1.16 Uncertainty Assessment and Special Treatment Refinement (Boxes 13 and 14 in Figure D-1)

The margins in the best estimate PRA results and the conservative Chapter 15 results, along with uncertainties in the probabilistic and deterministic safety analyses, are assessed in Box 13. This includes uncertainties that have been explicitly identified and quantified in the PRA as well as other non-quantified sources of uncertainty. This evaluation together with the results of the previous steps provides sufficient information to confirm the special treatment requirements for two SSC safety classes: SR and NSRST in Box 14.[t]

SSCs classified as SR or NSRST are subjected to special treatment requirements. The guiding principle for setting these requirements is to ensure that plant capability and associated programmatic conditions provide a sufficient degree of capability and reliability to prevent and mitigate accidents as assumed in the probabilistic and deterministic safety analysis throughout the plant lifecycle.

---

both. This characteristic is not unique to the NGNP but is true for all reactors. When the frequencies and consequences of LBEs are plotted for comparison to the TLRC the evaluation does not apply credit or withdraw credit to any SSC but rather identifies whether the SSC helps to prevent the LBE (by lowering its frequency) or whether it provides a mitigative role by limiting the event consequence. In the NGNP approach, event sequence frequencies and consequences are compared against the TLRC without artificially removing or adding credit for any specific SSC. All the SSCs that can prevent or mitigate an accident are represented in the PRA and, depending on the event sequence, some SSCs are assumed to fail and others assumed to function and the probability of success vs. failure is reflected in the event sequence frequencies. The only time an SSC is "credited" or "not credited" is when the deterministic DBAs for Chapter 15 are defined and analyzed. In that case the criteria are dose based and the frequency of the event is not considered. In many cases the deterministic DBAs correspond to event sequences in the PRA with frequencies in the BDBE region and in some cases the frequencies are so low as to be below what is the general level of regulatory concern.

t. In their review of the PBMR US DC white paper on Defense-in-Depth, the NRC staff requested in RAI DID-11 a discussion of how the defense-in-depth approach addresses aspects of the plant design that have unknowingly been omitted from the risk analysis (i.e., the unknown unknowns). The NGNP defense-in-depth approach embraces the engineering and regulatory practices that have evolved over the last 50 years of reactor design and licensing. It combines deterministic and probabilistic methods into a robust fabric designed to expose simple as well as complex relationships in design and operation. It also provides for special treatment in design, manufacturing, construction, testing, operations and maintenance to provide reasonable assurance that there is a very low likelihood of unknown unknowns. In support of plant safety and defense-in-depth, reactor suppliers and operators have processes that assure that deviations from required performance – either during initial plant design and analysis or during the operating lifetime – are exposed and addressed. This is part of lifetime programmatic defense-in-depth. In the license application, the NGNP project will provide information to demonstrate that the NGNP PRA has an adequate degree of design completeness. The NGNP design will include a multiple-barrier design like all other reactors although different levels of public safety assurance will be derived from each barrier, reflecting a general shift from mitigation to prevention. The NGNP project will also evaluate the use of emergency planning as a defense-in-depth capability and identify the extent and value of that program. The NGNP PRA will include a rigorous process of identifying sources of uncertainty, quantifying their impacts on the PRA results for accident frequency and consequence, investigating modeling uncertainties via sensitivity studies, and implementing the risk-informed and performance-based approach to defense-in-depth.

D.1.17 Confirmation of Defense-in-Depth Adequacy (Boxes 15 and 16 in Figure D-1)

The final step in the RIPB design approach shown in Box 15 is a risk-informed evaluation to confirm that there are sufficient capabilities in the design and sufficient programs defined to assure an adequate level of defense-in-depth. Further discussion is provided in Section 3.2.4.3. In some cases, it may be necessary to revise the design if additional special treatments do not provide the requisite level of confidence in the design or if safety relies on a single feature or the design. If the design is satisfactory, as shown in Box 16, the design continues to be developed to completion. Periodically, as defined in the designer's processes, the risk informed evaluation of the design including the maintenance of adequate defense-in-depth is repeated until a final design and associated licensing process is completed.

D.2 References for Appendix D

D-1 American Society of Mechanical Engineers, "Draft PRA Standard for Advanced Non-LWRs", Issued for Public Review and Comment, October 2008.

D-2 Regulatory Guide 1.203, "Transient and Accident Analysis Methods," U.S. Nuclear Regulatory Commission, Revision 0, December 2005.