



P B M R

Pebble Bed Modular Reactor (Pty) Ltd.

Reg. No: 1999/17946/07

3rd Floor, Lake Buena Vista Building 1267 Gordon Hood Avenue Centurion Republic of South Africa
PO Box 9396 Centurion 0046 Tel (+27 12) 677-9400 Fax (+27 12) 663-3052/8797/ 677-9446

Date:
December 13, 2006

Your Ref.:

Our Ref.:
USDC20061213-1

Enquiries:
E.G. Wallace
TEL:US 423-344-6774

ATTN: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

NRC Project No. 732

Attention: Mr. N. Prasad Kadambi

Subject: PBMR White Paper: Defense-in-Depth Approach

Ref: PBMR (Pty) Ltd. Letter, Subject: Submittal of PBMR Preapplication White
Papers, May 1, 2006

Enclosed is the PBMR white paper entitled "Defense-in-Depth Approach for the Pebble Bed Modular Reactor", Revision 1. This paper describes the defense-in-depth approach that has been applied to the PBMR design and sets forth certain facts for review and discussion in order to facilitate an effective submittal leading to a PBMR design certification. This submittal also completes our action on the four papers that were agreed upon for review as outlined in the reference. Your review and feedback on next steps are appreciated.

If you have any questions about this submittal, please feel free to contact me.

Yours sincerely,

Edward G. Wallace
Senior General Manager- US Programs
PBMR (Pty) Ltd.

Enclosure

cc: Ms. Christiana Lui, RES
Ms. Margaret T Bennett, RES
Mr. James Danna, RES
Mr. Stuart J. Rubin, RES
Mr. Lawrence J. Burkhart, NRR

ABSTRACT

This paper identifies the regulatory issues related to the PBMR approach to defense-in-depth for which U.S. Nuclear Regulatory Commission feedback is desired during the pre-application review of the Pebble Bed Modular Reactor (PBMR). The regulatory foundation for review of the PBMR approach to defense-in-depth is summarized, compliance with the regulatory criteria is described, and specific issues for which feedback is requested are described. This paper describes the defense-in-depth approach that has been applied to the PBMR and is expected to be used to obtain a Design Certification for the PBMR under 10 CFR Part 52.

CONFIGURATION CONTROL

Document History

Rev.	Date	Preparer	ECPs	Changes
A	2006/07/26	K Fleming		New document.
B	2006/07/27	K Fleming		Document updated after Comments Review. Sent for Independent Review.
C	2006/12/08	K Fleming		Comments Review
1	2006/12/11	K Fleming		Document formatted and sent for approval.

Document Approval

Action	Function	Designate	Signature
Prepared	Author	K Fleming	See signatures on file
Reviewed	Independent Reviewer	E Burns	See signatures on file
Reviewer 2	Systems Engineer - Nuclear Safety	M Bredin	See signatures on file
Reviewer 3	PRA Supervisor	L Lusse	See signatures on file
Approved	Senior GM, US Programs	E G Wallace	See signatures on file

Document Retention Time

This document is a Quality Record and shall be retained in accordance with PRC0012.

CONTENTS

ABBREVIATIONS	6
1. INTRODUCTION.....	9
1.1 SCOPE AND PURPOSE	9
1.2 STATEMENT OF THE ISSUES.....	10
1.3 SUMMARY OF PREAPPLICATION OUTCOME OBJECTIVES	11
1.4 RELATIONSHIP TO OTHER PREAPPLICATION FOCUS TOPICS/PAPERS.....	12
2. REGULATORY FOUNDATION	13
2.1 NRC REGULATORY FOUNDATION FOR DEFENSE-IN-DEPTH.....	13
2.1.1 NRC Regulations	13
2.1.2 NRC Policy Statements.....	14
2.1.3 NRC Guidance	16
2.1.3.1 NUREG-0800, Standard Review Plan	16
2.1.3.2 SECY-06-0217, Improvement to and Update of the Risk-Informed Regulation Implementation Plan	19
2.1.3.3 SECY-05-0006, Second Status Paper on the Staff's Proposed Regulatory Structure for New Plant Licensing and Update on Policy Issues Related to New Plant Licensing	23
2.1.3.4 SECY-98-144, White Paper on Risk-Informed and Performance-Based Regulation.....	24
2.1.3.5 Regulatory Guide 1.174, an Approach to Using PRA in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis.....	24
2.1.3.6 SECY-00-0198, 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).....	24
2.1.4 NRC Precedents Involving Gas-Cooled Reactors	25
2.2 IAEA APPROACH TO DEFENSE-IN-DEPTH	26
2.3 REGULATORY BASIS SUMMARY	27
3. PBMR APPROACH	28
3.1 DEFINITION OF DEFENSE-IN-DEPTH FOR THE PBMR	28
3.1.1 Overview	28
3.1.2 Plant Capability Defense-in-Depth.....	31
3.1.3 Programmatic Defense-in-Depth	37
3.1.4 Risk-Informed Evaluation of Defense-in-Depth	39
3.1.4.1 Scope of Risk-Informed Evaluation.....	39
3.1.4.2 Demonstrating Adequacy of Defense-in-Depth	40
3.1.4.3 Consistency with IAEA Approach	46
3.1.4.4 Use of PRA to Evaluate Roles of SSCs in Accident Prevention and Mitigation	47
3.2 PBMR IMPLEMENTATION OF DEFENSE-IN-DEPTH	55
3.2.1 PBMR Implementation of <i>Plant Capability Defense-in-Depth</i>	55
3.2.1.1 Radioactive Sources and Barriers to Radionuclide Transport.....	55
3.2.1.2 PBMR Safety Functions.....	58
3.2.1.3 Selection of PBMR Inherent Features	59
3.2.1.4 PBMR Design Features Supporting Required Safety Functions	59
3.2.2 PBMR Implementation of <i>Programmatic Defense-in-Depth</i>	63
3.2.3 PBMR Implementation of <i>Risk-Informed Evaluation of Defense-in-Depth</i>	65
3.3 PBMR APPROACH TO APPLYING DEFENSE-IN-DEPTH PRINCIPLES	66
3.4 SUMMARY OF DEFENSE-IN-DEPTH INSIGHTS FOR THE PBMR	70

4. ISSUES FOR PREAPPLICATION RESOLUTION.....	72
5. PREAPPLICATION OUTCOME OBJECTIVES.....	77
6. APPENDICES.....	79
6.1 APPENDIX A: USE OF PRA TO EVALUATE ROLE OF SSCS IN ACCIDENT PREVENTION AND MITIGATION.....	79
6.1.1 Use of PRA in <i>Risk-Informed Evaluation of Defense-in-Depth</i>	79
6.1.2 Evaluation of Selected PWR Event Sequences.....	80
6.1.3 Evaluation of Selected MHTGR Sequences.....	83
Prevention and Mitigation Insights from PWR and MHTGR Examples.....	86
7. REFERENCES.....	88

FIGURES

Figure 1: Elements of PBMR Approach to Defense-in-Depth.....	29
Figure 2: Detailed Elements of PBMR Defense-in-Depth Approach.....	32
Figure 3: Barriers to Radionuclide Transport Included in <i>Plant Capability Defense-in-Depth</i>	34
Figure 4: Elements of Safety Design Approach Incorporated into <i>Plant Capability Defense-in-Depth</i>	35
Figure 5: Logic for Implementing <i>Risk-Informed Evaluation of Defense-in-Depth</i>	44
Figure 6: Scenario Framework for Defense-in-Depth Provided by IAEA.....	46
Figure 7: Design Features Contributing to Prevention and Mitigation of I-131 Releases from Selected MHTGR Sequences.....	53
Figure 8: Risk Reduction Factors Associated with MHTGR Design Features Responsible for Prevention and Mitigation of I-131 Releases.....	54
Figure 9: PBMR's Primary Barrier to Radionuclide Transport.....	57
Figure 10: Major Components of the Main Power System, Helium Pressure Boundary, and Containment System.....	57
Figure 11: PBMR Safety Functions.....	58
Figure 12: Design Features Contributing to Prevention and Mitigation of I-131 Releases from Selected PWR Sequences.....	82
Figure 13: Risk Reduction Factors Associated with PWR Design Features Responsible for Prevention and Mitigation of I-131 Releases.....	83
Figure 14: Design Features Contributing to Prevention and Mitigation of I-131 Releases from Selected MHTGR Sequences.....	86
Figure 15: Risk Reduction Factors Associated with MHTGR Design Features Responsible for Prevention and Mitigation of I-131 Releases.....	87

TABLES

Table 1: Levels of Defense-in-Depth According to IAEA INSAG-10.....	26
Table 2: Elements of <i>Plant Capability Defense-in-Depth</i>	36
Table 3: Elements of <i>Programmatic Defense-in-Depth</i>	38
Table 4: Derivation of Defense-in-Depth Principles from Standard Review Plan Chapter 19.....	41
Table 5: Principles for Establishing the Adequacy of Defense-in-Depth for the PBMR.....	43
Table 6: Elements of <i>Risk-Informed Evaluation of Defense-in-Depth</i>	45

Table 7: Event Sequence Model for Prevention and Mitigation.....	50
Table 8: PBMR Radioactive Sources and Barriers.....	56
Table 9: PBMR Design Features and SSCs Providing <i>Plant Capability Defense-in-Depth</i>	60
Table 10: PBMR Approach to Addressing Defense-in-Depth Principles of Table 5.....	67
Table 11: Data Assumed for LWR Sequence Evaluation (from NUREG-1150).....	81
Table 12: Data Assumed for MHTGR Sequence Evaluation (from Reference [24])	85

ABBREVIATIONS

This list contains the abbreviations used in this document.

Abbreviation or Acronym	Definition
ACS	Active Cooling System
ACNW	Advisory Committee on Nuclear Waste
ACRS	Advisory Committee on Reactor Safeguards
AEPS	Auxiliary Electrical Power System
ALARA	As Low As Reasonably Achievable
AOO	Anticipated Operational Occurrence
BDBE	Beyond Design Basis Event
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
COTS	Commercial Off-the-shelf
CBCS	Core Barrel Conditioning System
CCS	Core Conditioning System
DBA	Design Basis Accident
DBE	Design Basis Event
DCA	Design Certification Application
DPP	Demonstration Power Plant
ECP	Engineering Change Proposal
EE	External Event
EPCC	Equipment Protection Cooling Circuit
EPM	Engineering Performance Monitoring
EPS	Equipment Protection System
EPRI	Electric Power Research Institute
EPS	Equipment Protection System
EQ	Equipment Qualification
Eskom	Eskom Holdings Limited – RSA
FEM	Finite Element Modelling
FOAK	First of a Kind
GDC	General Design Criterion
HPB	Helium Pressure Boundary
HPS	Helium Purification System
HTF	Helium Test Facility
HTTF	Heat Transfer Test Facility
HX	Heat Exchanger
IEEE	Institute of Electrical and Electronics Engineers
IAEA	International Atomic Energy Agency

Abbreviation or Acronym	Definition
ISI	In-service Inspection
IST	In-service Surveillance Testing
KLI	Key Licensing Issue
LBE	Licensing Basis Event
LERF	Large Early Release Frequency
LOCA	Loss of Coolant Accident
MDSS	Manual Diverse Shutdown System
MHSS	Main Heat Sink System
MPS	Main Power System
NNR	National Nuclear Regulator (RSA)
NPP	Nuclear Power Plant
NUREG	NUclear REGulatory Commission Report
OBE	Operating Basis Earthquake
OCS	Operational Control System
OPM	Operational Performance Monitoring
PAG	Protective Action Guideline
PBMR	Pebble Bed Modular Reactor
PQ	Plant Qualification
PRA	Probabilistic Risk Assessment
PRS	Pressure Relief System
QA	Quality Assurance
QAPD	Quality Assurance Program Description
RAI	Request for Additional Information
RAL	Review Action List
RCS	Reactivity Control System
RCCS	Reactor Cavity Cooling System
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RSS	Reserve Shutdown System
RS	Reactor SCRAM
RSA	Republic of South Africa
SAR	Safety Analysis Report
SAS	Small Absorber Spheres
SC	Safety Case
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan
SSCs	Structures, Systems and Components
SSE	Safe Shutdown Earthquake

Abbreviation or Acronym	Definition
TEDE	Total Effective Dose Equivalent
TG	Turbine Generator
TLRC	Top Level Regulatory Criteria
TNF	Technology-Neutral Framework
TQC	Testing, Qualification and Commissioning
TQC	Total Quality Management
V&V	Verification and Validation

1. INTRODUCTION

1.1 SCOPE AND PURPOSE

This paper describes the approach to the treatment of defense-in-depth for the Pebble Bed Modular Reactor (PBMR). The 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, and an explanation of how this safety philosophy has been applied to the PBMR.

PBMR recognizes that defense-in-depth is a crucial element of the overall safety of nuclear power plants. The principles of defense-in-depth have been applied for the design, licensing, construction, operation and regulation of existing and advanced nuclear power plants and the PBMR is no exception. The PBMR approach to defense-in-depth is built upon a foundation of conservative design features to prevent transients and accidents, and inherent reactor characteristics and passive design features to ultimately perform the safety functions necessary to prevent the release of radioactive material and to mitigate the consequences of accidents. The principles of multiple, independent, and concentric barriers to radionuclide transport have been applied for each significant source of radioactive material. In addition, the principles of design margins, redundancy, and diversity have been applied in the design of the Structures, Systems, and Components (SSCs) that support each required safety function that serve to support and maintain the integrity and effectiveness of these barriers. The extent to which defense-in-depth strategies are applied is sufficient to ensure that the Top Level Regulatory Criteria (TLRC) are met, adequate safety margins are achieved, and that uncertainties in the reliabilities and capabilities of the SSCs providing these safety functions are adequately addressed.

The PBMR approach to defense-in-depth relies on inherent characteristics and passive SSCs to ultimately perform safety functions that are required in the prevention and mitigation of design basis accidents. In addition the PBMR safety design approach includes active SSCs to provide additional defense-in-depth in the performance of safety functions. This approach of providing combinations of inherent features and passive SSCs to form the required safety functions as well as additional redundant and diverse active SSCs to perform these same functions is strong evidence of a robust approach to defense-in-depth.

Defense-in-depth has also been applied in the risk-informed safety evaluation process for the PBMR. This is reflected in use of conservative assumptions and treatment of uncertainties in the selection of the Top Level Regulatory Criteria (TLRC), selection of the Licensing Basis Events (LBEs), performance of deterministic safety analyses of design basis accidents, safety classification of SSCs, and development of special treatment requirements. The PBMR approach to defense-in-depth has been 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 apply the principles of defense-in-depth.

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 PBMR definition of defense-in-depth recognizes three major elements:

- ***Plant Capability Defense-in-Depth*** which reflects the decisions made by the designer that incorporate the defense-in-depth into the physical plant.
- ***Programmatic Defense-in-Depth*** which reflects the decisions made associated with the processes of manufacturing, constructing, operating, maintaining, and inspecting the plant and in the processes that assure plant safety.
- ***Risk-Informed Evaluation of Defense-in-Depth*** which reflects the development and evaluation of strategies to 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 the 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.

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

1.2 STATEMENT OF THE ISSUES

The issues addressed in this paper are framed in terms of the following questions about the PBMR approach to defense-in-depth that will be implemented as part of the PBMR DCA:

1. What is an appropriate definition of defense-in-depth for the PBMR?
2. How should defense-in-depth be defined so that the PBMR approach to employing defense-in-depth strategies to design, construct, and operate the plant can be objectively evaluated?
3. What are the elements of defense-in-depth for the PBMR safety design philosophy, design approach and analyses, and the assurance programs to ensure that defense-in-depth is applied throughout the life of the plant?
4. How is the defense-in-depth philosophy reflected in the risk-informed licensing approach that is proposed for the PBMR?
5. How are the defense-in-depth strategies of accident prevention and mitigation defined and evaluated for the PBMR?
6. 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 PBMR DCA?

1.3 SUMMARY OF PREAPPLICATION OUTCOME OBJECTIVES

The objective of this paper and the follow-up workshops is to get NRC agreement on the treatment of defense-in-depth to support PBMR certification. Specifically, we would appreciate NRC agreement with the following statements, or that the NRC provide an alternative set of statements with which they agree.

1. The definition of defense-in-depth presented in Section 3 of this paper, which recognizes three elements of the defense-in-depth approach: **Plant Capability Defense-in-Depth**, **Programmatic Defense-in-Depth**, and **Risk-Informed Evaluation of Defense-in-Depth**, is appropriate for the PBMR DCA.
2. The PBMR approach to **Plant Capability Defense-in-Depth**, 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 DCA.
3. The PBMR approach to **Programmatic Defense-in-Depth** 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 will be maintained throughout the lifetime of the plant.
4. The PBMR approach to **Risk-Informed Evaluation of Defense-in-Depth** represents an acceptable event sequence framework for the definition of accident prevention and mitigation the evaluation of the roles of design features and SSCs responsible for prevention and mitigation for the DCA, and logical progress to establish the adequacy and sufficiency of defense-in-depth.
5. Sufficient information on the PBMR approach to defense-in-depth required to support certification of the PBMR design will be included in the DCA. This information will include:
 - a. An appropriate definition for defense-in-depth.
 - b. The roles of each barrier to fission product release in providing defense-in-depth.
 - c. The roles of inherent and passive design features and SSCs that are used as well as active engineered systems to provide defense-in-depth.
 - d. How the reliability, capability, and independence of each barrier are defined and evaluated in terms of their defense-in-depth role.
 - e. How the safety functions are defined and how they support the integrity of each barrier in providing 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 defense-in-depth.
 - g. How the principles of design margins, redundancy, diversity, and independence been applied in providing defense-in-depth.
 - h. An appropriate definition of prevention and mitigation and a means to evaluate the impact of these strategies on maintaining acceptable risk levels.

- i. The roles and effectiveness of specific barriers and SSCs in the prevention and mitigation of accidents.
- j. What is the role of design safety margins reflected in the applied codes and standards in providing a robust design with defense-in-depth?
- k. How defense-in-depth is applied to address uncertainties.
- l. A set of principles to determine the adequacy and sufficiency of defense-in-depth.

1.4 RELATIONSHIP TO OTHER PREAPPLICATION FOCUS TOPICS/PAPERS

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. 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. The treatment of defense-in-depth is best evaluated in an integrated fashion. Many of the papers that have been identified for the PBMR pre-application review provide additional insight into defense-in-depth in the PBMR design.

The paper on the PBMR approach to PRA [1] covers a crucial input to the selection of licensing basis events and the information needed to implement the PBMR approach to ***Risk-Informed Evaluation of Defense-in-Depth***. The defense-in-depth considerations that have been applied to the derivation of the Top Level Regulatory Criteria (TLRC) and the selection of Licensing Basis Events (LBEs) based on information from the PRA are discussed in the paper on LBE Selection [2]. The companion paper on SSC Safety Classification [3] describes how the principles of ***Programmatic Defense-in-Depth*** have been applied in the safety classification of SSCs and in the development of special treatment requirements for safety classified SSCs. ***Programmatic Defense-in-Depth*** is also germane to the selection of design codes and standards for the PBMR as discussed in separate papers planned for materials selection, codes, and standards.

Details on the design, performance, and operational controls for a crucial part of the PBMR approach to ***Plant Capability Defense-in-Depth***, the coated particle fuel barrier, are covered in a paper planned for the Fuel Performance and Test Program. Additional papers are planned to discuss the treatment of uncertainties in the development of the mechanistic source term and in the verification and validation of computer models for the safety and design analyses. Analysis of these uncertainties is an important element of ***Risk-Informed Evaluation of Defense-in-Depth*** and provides feedback to the development of requirements that manage uncertainties as part of the ***Programmatic Defense-in-Depth*** element.

2. REGULATORY FOUNDATION

This section reviews the regulatory foundation in order to identify NRC expectations for the application of defense-in-depth. Although most of this section is devoted to the NRC regulatory foundation for defense-in-depth, it also includes a description of the IAEA approach to defense-in-depth which offers additional perspectives.

2.1 NRC REGULATORY FOUNDATION FOR DEFENSE-IN-DEPTH

2.1.1 NRC Regulations

There are few provisions in 10 CFR that provide a clear definition of defense-in-depth. In 10 CFR Part 50, Appendix R, on the requirements for the fire protection program for older plants [4] the following requirement is included to implement the defense-in-depth approach to fire protection program:

'The fire protection program shall extend the concept of defense-in-depth to fire protection in fire areas important to safety, with the following objectives:

To prevent fires from starting;

To detect rapidly, control, and extinguish promptly those fires that do occur;

To provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent the safe shutdown of the plant.'

Similar provisions are in 10 CFR 50.48. These are the only references to the term 'defense-in-depth' in 10 CFR Part 50; however, other parts of 10 CFR include references to the term.

As discussed more fully in Section 3, this definition of defense-in-depth for fire protection is viewed to be consistent with the PBMR approach to defense-in-depth which has been broadly applied to all areas including the fire protection program.

2.1.2 NRC Policy Statements

The NRC does not have any policy statements specifically devoted to defense-in-depth. However, the NRC's *Policy Statement on Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities* [5] does state:

'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, as well as the philosophy of a multiple-barrier approach against fission product releases.'

The 'philosophy of a multiple barrier approach against fission product release' is applicable to the PBMR. The specific reference here to the application of 'redundancy for facilities with 'active' safety systems' needs to be interpreted for the PBMR, which emphasizes the use of inherent characteristics and passive SSCs to implement safety functions, while retaining the concept of active systems to provide an additional measure of defense-in-depth in the performance of safety functions.

Additionally, NRC's *Policy Statement on Regulation of Advanced Nuclear Power Plants* [6] includes the following statement:

'...the Commission expects that advanced reactors will provide enhanced margins of safety and/or utilize simplified, inherent, passive or other innovative means to accomplish their safety functions.'

This policy statement also lists attributes that should be considered in advanced reactor designs:

'Highly reliable and less complex shutdown and decay heat removal systems. The use of inherent or passive means to accomplish this objective is encouraged (negative temperature coefficient, natural circulation, etc.).'

'Longer time constants and sufficient instrumentation to allow for more diagnosis and management before reaching safety system challenge and/or exposure of vital equipment to adverse conditions.'

'Simplified safety systems that, where possible, reduce required operator actions, equipment subjected to severe environmental conditions, and components needed for maintaining safe shutdown conditions. Such simplified systems should facilitate operator comprehension, reliable system function, and more straightforward engineering analysis.'

'Designs that minimize the potential for severe accidents and their consequences by providing sufficient inherent safety, reliability, redundancy, diversity, and independence in safety systems.'

'Designs that provide reliable equipment in the balance of plant (BOP) (or safety system independence from BOP) to reduce the number of challenges to safety systems.'

'Designs that provide easily maintainable equipment and components.'

'Designs that reduce potential radiation exposures to plant personnel.'

'Designs that incorporate defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for and consequences of severe accidents.'

'Design features that can be proven by citation of existing technology or that can be satisfactorily established by commitment to a suitable technology development program.'

Although only one of these attributes explicitly mentions defense-in-depth, all are relevant to the PBMR safety design approach and its approach to defense-in-depth.

Finally, the Commission's *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.'

This concept of defense-in-depth is also applicable to the PBMR with the following clarifications. Core melt accidents have been precluded in the PBMR safety design approach by the application of inherent design features and passive SSCs which preclude the conditions needed for a 'core melt' accident consistent with NRC's advanced reactor policy statement. However, there are certain types of accidents that could occur in the PBMR that could result in the release of radioactive material. PBMR has a containment system¹ which provides one of the radionuclide transport barriers and hence has a defense-in-depth role. However, because of the PBMR inherent and passive capabilities to prevent large releases from the fuel and helium pressure boundary, the safety significance of the containment system is much different than that for an existing LWR. With these clarifications, the above definition of defense-in-depth is consistent with the PBMR approach to defense-in-depth as described more fully in Section 3. Moreover, the specific approach that PBMR has taken to address defense-in-depth is consistent with NRC's advanced reactor policy statement.

¹ As described in Reference [20] and in Section 3 of this paper, the PBMR containment system is a collection of passive structures, systems, and components, including the citadel, vented reactor building, and pressure relief system (PRS) blow-out panels, and active SSCs, including PRS relief shaft isolation dampers and reactor building Heating, Ventilation, and Air Conditioning (HVAC) filtration system, that perform PBMR specific safety functions.

2.1.3 NRC Guidance

2.1.3.1 NUREG-0800, Standard Review Plan

The NRC has several guidance documents that address defense-in-depth in general. For example, Chapter 19 of the Standard Review Plan (SRP) [8] provides the following broad 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....'

With one clarification, this definition of defense-in-depth is applicable to the PBMR. As discussed more fully in Section 3, the terms 'core damage prevention' and 'containment failure' as defined for LWRs do not apply in the conventional sense to the PBMR. Furthermore, as discussed more fully in Section 3, balancing prevention and mitigation of core damage events in LWRs has been defined by comparing such LWR risk metrics as Core Damage Frequency (CDF), Large Early Release Frequency (LERF), and the conditional containment failure probability. The direct application of this concept to the PBMR is not appropriate. However, the objective that a design should employ both prevention and mitigation strategies is applicable to the PBMR. What is to be prevented and mitigated needs to be defined in terms of PBMR specific plant damage states.

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

'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.'

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 fulfills 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 fulfills 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.'

Although this part of the SRP deals with risk-informed changes to an already licensed plant and not a design certification, it provides a good basis for reviewing the PBMR approach to defense-in-depth. Each element of the defense-in-depth safety philosophy reflected in this document is applicable to the PBMR with a few clarifications. As noted earlier, the prevention and mitigation strategies for the PBMR do not specifically refer to core damage but rather to PBMR specific damage states which are less severe than the LWR core damage threshold. The PBMR containment system, while different than LWR containment, provides one of the barriers in the PBMR approach to defense-in-depth but its safety functions are defined somewhat differently than those for an LWR containment system. With these clarifications, the concept of defense-in-depth reflected in SRP Chapter 19 is reflected in the approach for the PBMR.

SRP Chapter 19 also includes the following criteria for reviewing the results of a PRA to examine the extent of redundancy and diversity available in the plant design to prevent an accident involving core damage or release of radioactivity:

'In addition to the usual quantitative risk indices, PRAs provide important qualitative results, namely, the contributors to accident sequences. For PRAs that use the fault tree linking approach, these contributors are described by the accident sequence minimal cut-sets. Each accident sequence minimal cut-set is a combination of passive and active SSC failures and human errors that would cause core damage or a release of radioactivity. The cut-sets therefore directly show one particular aspect of defense in depth, in that they reveal how many failures must occur in order for core damage or radiological release to occur. Thus, the minimal cut-sets show the effective redundancy and diversity of the plant design...

In most cases, events that appear in each minimal cut-set are targeted by programmatic activities to ensure the reliability of the associated SSC. Specific activities that are important to maintain the reliability of a component include IST, ISI, periodic surveillance required by Technical Specifications, quality assurance, and maintenance.

Therefore, when a review of the minimal cut-sets reveals areas where redundancy or diversity are already marginal, it would arguably be inappropriate to reduce the level of activities aimed at ensuring SSC performance. (The exception would arise if the licensee can show that the activities have little or no effect on SSC performance, or if it can be shown that uncertainties in the performance of the elements in this cut-set are well understood and quantified. It is also possible that the licensee could propose compensating or alternative activities to provide assurance of SSC performance.) The objective of this review is to avoid completely relaxing the defense-in-depth posture at points at which the plant design has the least overall functional independence, redundancy, and/or diversity. On the other hand, in areas where a plant has substantial redundancy and diversity, defense-in-depth arguments used to justify relaxations should be given appropriate weight.

As part of the defense-in-depth evaluation, reviewers should consider the effects of multiple component failures and common cause failures that could result from the proposed change. For example, if the licensee proposes to reduce the requirements for all events in a cut set, reviewers should ensure that the effect of the change is properly modelled and that the change does not have an adverse effect on defense in depth.

Finally, in assessing the accident sequence cutsets, reviewers should devote attention to potential over-reliance on programmatic activities or operator actions that compensate for weaknesses in the plant design. For example, proposed maintenance and surveillance activities should complement and not replace proper plant design'

As recommended in the SRP, the PBMR approach to defense-in-depth includes a structured examination of the PRA results. However, as noted in the paper on the PBMR PRA Approach, there are differences in the PRA structure due to different safety design approaches between the PBMR and LWRs. When these differences are taken into account, the SRP criteria for using the PRA results to examine the roles of SSCs in preventing and mitigating accidents are applicable to the PBMR. As discussed more fully in Section 3, PBMR has structured the results

of the PRA so that the roles of SSCs in the prevention and mitigation of accidents are more visible compared with the standard event sequence cut-set format.

2.1.3.2 SECY-06-0217, Improvement to and Update of the Implementation Plan Risk-Informed Regulation

SECY-06-0217 [9] provides some of the most recently published definitions of NRC's approach to defense-in-depth in the following statements:

'Defense-in-depth is the use of successive measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. Defense-in-depth is a philosophy used by the NRC to provide redundancy for facilities with 'active' safety systems. This multiple-barrier approach is also used to protect against fission product releases. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.'

The principle of defense-in-depth has always been and will continue to be fundamental to regulatory practice in the nuclear field. It is expected that defense-in-depth for reactors and nuclear materials (which includes disposal, transportation and storage, processing and fabrication, and industrial and medical applications) may need to be considered differently due to the greater diversity in licensed materials activities and to the differences in safety issues.'

As discussed in more detail in Section 3, the PBMR approach to **Plant Capability Defense-in-Depth** is consistent with this statement in that it provides multiple barriers and has redundant, independent, and diverse methods for performing key safety functions.

SECY-06-0217 continues by quoting an Advisory Committee on Reactor Safeguards (ACRS) letter [10], [11]:

'In its May 25, 2000, letter to Chairman Meserve, the Advisory Committee on Reactor Safeguards (ACRS) and the Advisory Committee on Nuclear Waste (ACNW) provided a perspective on the role of defense-in-depth in risk-informed regulation.'

'The primary need for improving the implementation of defense-in-depth in a risk-informed regulatory system is guidance to determine how many compensatory measures are appropriate and how good these should be. To address this need, we believe that the following guiding principles are important:

- *Defense-in-depth is invoked primarily as a strategy to ensure public safety given the unquantified uncertainty in risk assessments. The nature and extent of compensatory measures should be related, in part, to the degree of uncertainty.*
- *The nature and extent of compensatory measures should depend on the degree of risk posed by the licensed activity.*
- *How good each compensatory measure should be is, to a large extent, a value judgement and, thus, a matter of policy.*

The ACRS/ACNW letter further stated that defense-in-depth entails 'placing compensatory measures on important safety cornerstones to satisfy acceptance criteria for defined design-basis reactor accidents that represent the range of important accident sequences.'

ACRS has expressed concerns about the role of defense-in-depth in a risk-informed regulatory scheme. The Committee cites instances in which 'seemingly arbitrary appeals to defense-in-depth have been used to avoid making changes in regulations or regulatory practices that seemed appropriate in the light of results of quantitative risk analyses.' The letter's attachment describes the scope and nature of defense-in-depth in two models. 'In the structuralist model, defense-in-depth is primary, with PRA available to measure how well it has been achieved.' (This is the model implicit in the agency's PRA policy statement and in RG 1.174 concerning risk-informed changes to reactor licensing bases.) In the rationalist model, 'the purpose of defense-in-depth is to increase the degree of confidence in the results of the PRA or other analyses supporting the conclusion that adequate safety has been achieved. What distinguishes the rationalist model from the structural model is the degree to which it depends on establishing quantitative acceptance criteria, and then carrying formal analyses, including analysis of uncertainties, as far as the analytical methodology permits.'

To define the role of defense-in-depth in risk-informed regulation and to establish a consistent and reasoned approach, the following considerations should be addressed:

- *What elements of defense-in-depth should be independent of risk information?*
 - *measures to provide prevention and mitigation protection?*
 - *use of good engineering practices (e.g. codes and standards)?*
 - *number and nature of barriers to radiation release?*
 - *emergency plans and procedures?*
- *What elements of defense-in-depth should be dependent upon risk information?*
 - *the balance between prevention and mitigation?*
 - *the number of barriers?*
 - *the need for redundancy, diversity, and independence of systems?*
 - *the events that need to be considered in the design?*
- *Do the defense-in-depth considerations in RG 1.174 apply?*

Risk insights can make the elements of defense-in-depth clearer by quantifying them to the extent practicable. Although the uncertainties associated with the importance of some elements of defense may be substantial, the fact that these elements and uncertainties have been quantified can aid in determining how much defense makes regulatory sense. Decisions on the adequacy of or the necessity for elements of defense should reflect risk insights gained through identification of the individual performance of each defense system in relation to overall performance.

In implementing risk-informed changes to requirements or practices, the staff should ask:

- *Is defense-in-depth commensurate with the risk and uncertainty associated with the estimate of risk?*
- *Is a reasonable balance preserved among accident prevention, radiation exposure prevention, and consequence mitigation?*
- *Are programmatic activities overly relied on to compensate for design weaknesses?*
- *Are redundancy, independence, and diversity of the system commensurate with the expected frequency and consequences of challenges to the system and with the uncertainties?*
- *Are defenses against potential common-cause failures preserved and have potential new common-cause failure mechanisms been assessed?*
- *Is the independence of barriers preserved?*
- *Are defenses against human errors preserved?*

The attachment to the ACNW/ACRS letter [10] provides some insights on the evolution of thinking about defense-in-depth from the perspective of the ACRS. This attachment defines and contrasts two schools of thought on how to define defense-in-depth, including a 'structuralist' school, which holds that defense-in-depth is implicit in the regulations and a 'rationalist' school which argues that defense-in-depth is embodied in the results of a PRA.

In this attachment it is stated:

'In the structuralist model, defense-in-depth is primary, with PRA available to measure how well it has been achieved' while to the rationalist 'the purpose of defense-in-depth' (deterministic methods) 'is to increase the degree of confidence in the results of the PRA or other analyses supporting the conclusion that adequate safety has been achieved. What distinguishes the rationalist model from the structural model is the degree to which it depends on establishing quantitative acceptance criteria, and then carrying formal analyses, including analysis of uncertainties, as far as the analytical methodology permits.'

The PBMR approach to defense-in-depth incorporates both the 'rationalist' and 'structuralist' concepts outlined in the ACNW/ACRS letter and its attachment. An important difference for the PBMR is that the PRA is done at the beginning to support the design and to provide input to the selection of licensing basis events and the formulation of the regulatory requirements, rather than after the plant has been designed against a set of deterministic requirements. However, PBMR agrees that there is a role for the formulation of deterministic requirements to address and minimize uncertainties in the PRA results and to increase the level of confidence that SSCs will serve their appointed roles in the prevention and mitigation of accidents.

These ACRS references highlight the principles of prevention and mitigation and refer to the need to balance these strategies in the context of core damage accidents. In order to apply these concepts to the PBMR, it is necessary to clearly define what is to be prevented and what is to be mitigated, because the core damage state, as it has been defined for an LWR, does not apply to the PBMR. An approach for assessing the role of SSCs in the prevention and mitigation for different classes of accidents for the PBMR is described in this paper.

SECY-06-0217 also makes the point that the concept of safety margins is an element of defense-in-depth with the following statement:

'Existing regulations were developed to ensure adequate safety margins to account for uncertainties in analyses and data and to ensure that adequate time is available to prevent the consequences of events. Safety margins are part of defense-in-depth; they assure safety in spite of uncertainties.'

Regulatory Guide 1.174 states that acceptable risk-informed changes to a nuclear power reactor's licensing basis will be consistent with the principle that sufficient safety margins are maintained. Improved information from data analysis, research experiments, and the like suggest that some safety margins are excessive, given the current state of knowledge and current uncertainties. As regulations are evaluated to improve the focus on safety, regulations that require excessive safety margins will be candidates for change. To define the role that safety margins play in risk-informed regulation and to establish a consistent and reasoned approach, the following considerations should be addressed:

- *How should safety margins be employed to account for uncertainties in engineering analysis?*
 - *best estimate analysis with conservative acceptance criteria?*
 - *specified confidence level?*
 - *role of codes and standards (i.e., do they inherently address safety margins)?*
- *How should safety margins be employed to account for uncertainty in risk?*
 - *parameter uncertainty; defense-in-depth (i.e., redundancy, diversity, independence)?*
 - *incompleteness in risk analysis (e.g., engineering judgement)?*
 - *model uncertainty (e.g., conservative acceptance criteria)?*

In making risk-informed changes to requirements or practices, the staff should ask:

- *What safety margins are acceptable given the risk significance of the regulated activity and uncertainties?*
- *Is the proposed change consistent with the principle that sufficient and realistic safety margins be maintained?*
- *Is there a method for evaluating whether safety margins will be adequately maintained?*

As discussed in Section 3, the PBMR approach to **Programmatic Defense-in-Depth** is consistent with these statements, in that it accounts for uncertainties and includes safety margins.

2.1.3.3 SECY-05-0006, Second Status Paper on the Staff's Proposed Regulatory Structure for New Plant Licensing and Update on Policy Issues Related to New Plant Licensing

The NRC staff has proposed a revised framework for defense-in-depth as part of its Technology Neutral Framework (TNF) for licensing new reactor designs. In Attachment 3 to SECY-05-0006 [12] the NRC staff provides the following model of defense-in-depth and criteria for reviewing new reactor designs:

'Defense-in-Depth Model

The model of defense-in-depth which the staff is recommending for application to new reactors incorporates both deterministic and probabilistic elements. The deterministic part of the model mainly addresses completeness uncertainties by asking the question, 'What if this barrier or safety feature fails?' without relying on a quantitative estimate of the likelihood of such a failure. As a result, the deterministic element is defined by protective strategies that are successive measures designed to protect public health and safety even if some of the strategies fail. The protective strategies of the technology-neutral framework are to ensure Physical Protection, maintain Barrier Integrity, limit Initiating Event Frequencies, assure adequate reliability of Protective Systems, and provide Accident Management. In addition, the deterministic element imposes specific qualitative requirements to be included in the regulations to ensure that the accomplishment of key safety functions are not dependent upon a single element of plant design construction, maintenance or operation.

The probabilistic part of the model seeks to evaluate the uncertainties in the analysis and to determine what steps should be taken to compensate for those uncertainties. The probabilistic elements address primarily modelling and parameter uncertainties, and establish specific quantitative performance goals, such as equipment reliability goals, that compensate for the calculated uncertainty.

The staff's defense-in-depth model uses a deterministic approach at a high level by requiring that all the protective strategies are included. Within each protective strategy a probabilistic approach is used to determine how much defense-in-depth is needed to achieve the desired quantitative goals on initiating event frequency and safety system reliability, including uncertainty.

Implementation of the Defense-in-Depth

The staff's approach for implementation of the above model relies on the application of the defense-in-depth principles as qualitative criteria to be adhered to, and the use of a PRA for achieving quantitative risk goals. Inclusion of all the protective strategies assures some protection against completeness uncertainty. Within each strategy, a probabilistic defense-in-depth element is applied to ensure adequate performance in meeting the objective of the strategy. The systems, barriers and actions used in the performance of the safety functions associated with the protective strategy are examined in terms of deterministic and probabilistic elements of defense-in-depth. Quantitative risk information is used, where possible, to assess the degree of conformance and the need for additional defense-in-depth measures (e.g., redundancy, diversity, safety margins).

Monitoring and feedback are essential aspects of this process, since the validity of initial design assumptions, and of design changes made as part of the outlined steps, will be established by the actual operation of the reactor. Additional hardware or procedural changes may result from this feedback. This is especially important for the new and innovative designs for which there is no operating experience.

The staff envisions whole process of applying defense-in-depth as an iterative process, a series of steps, that is expected to be used initially by the designer and ultimately by the designer and regulator to develop the emerging design. As the design evolves the PRA will also be able to be developed to greater detail.'

As described in more detail in Section 3, the PBMR approach provides for both deterministic and probabilistic evaluations of defense-in-depth. As with the TNF approach, the PBMR approach is applied in an iterative fashion and addresses a set of defense-in-depth principles that includes the consideration of uncertainties.

2.1.3.4 SECY-98-144, White Paper on Risk-Informed and Performance-Based Regulation

The NRC's white paper on risk-informed and performance-based regulation, SECY-98-144 [13], defines defense-in-depth as the element of NRC's safety philosophy that:

'...employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.'

This concept of defense-in-depth is reflected in the PBMR approach to defense-in-depth. As discussed more fully in Section 3, the PBMR employs multiple independent barriers, and has redundant, independent, and diverse methods for performing key safety functions.

2.1.3.5 Regulatory Guide 1.174, an Approach to Using PRA in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis

Regulatory Guide 1.174 [14] on risk-informed decision making identifies several factors for ensuring that defense-in-depth is maintained in risk-informed changes to LWRs. These factors are essentially the same as those currently included as guidelines in Chapter 19 of the SRP and have been considered in developing the PBMR approach to defense-in-depth.

2.1.3.6 SECY-00-0198, 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)

SECY-00-0198 [15] contains the following statements regarding defense-in-depth that are consistent with those made in the previously discussed documents, but add further insights regarding NRC expectations for achieving and maintaining defense-in-depth.

'The defense-in-depth approach includes elements that are dependent upon risk insights and elements that are employed independent of risk insights. Risk insights are used to set guidelines that:

- *limit the frequency of accident-initiating events;*
- *limit the probability of core damage, given accident initiation;*
- *limit radionuclide releases during core damage accidents; and*
- *limit public health effects caused by core damage accidents.*

Safety function success probabilities (commensurate with accident frequencies, consequences, and uncertainties) are achieved via appropriate:

- *redundancy, independence, and diversity;*
- *defenses against common-cause failure mechanisms;*
- *defenses against human errors; and*
- *safety margins.*

The following defense-in-depth elements are employed independent of risk insights:

- *prevention and mitigation are maintained;*
- *reasonable balance is provided among prevention, containment, and consequence mitigation;*
- *over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided;*
- *independence of barriers is not degraded; and*
- *the defense-in-depth objectives of the current GDC in Appendix A to 10 CFR Part 50 are maintained.'*

This concept of defense-in-depth is consistent with those discussed previously and includes some additional thoughts. A specific goal of limiting the initiating event frequency is listed as a specific strategy to address accident prevention.

The PBMR approach to defense-in-depth is consistent with the strategies identified in this SECY paper, with the clarifications noted earlier about the need to use PBMR specific risk metrics and definitions of prevention that are meaningful for the PBMR. In addition to the items listed above under safety function success probabilities, the PBMR emphasizes the use of inherent and passive means to fulfil the required safety functions and to ensure their reliability and capability.

2.1.4 NRC Precedents Involving Gas-Cooled Reactors

In 2001-2002, the NRC staff conducted a pre-application review of the PBMR at the request of Exelon. In a letter to Exelon dated March 26, 2002 [16], the NRC staff provided its assessment of the licensing approach proposed by Exelon, including the top level regulatory criteria (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] see ms to i mply that the function ca n be met without controlling radi onuclide transport fr om the rea ctor buildin g and from the site, which appe ars to contradict the defense-in-depth philo sophy. The role of a containment in the PB MR design will be specifically addressed and is expected to be presented to the Commission as a policy issue. (Enclosure, pg. 17)'

PBMR agrees with the staff conclusion that simply meeting the TLRC does not necessarily mean that a reactor has provided a sufficient degree of defense-in-depth. As discussed more fully in Section 3, the PBMR approach to defense-in-depth goes well beyond the meeting the TLRC in demonstrating that the approach to defense-in-depth is adequate.

As discussed in SECY-04-0103 on policy issues related to new plant licensing [17] the NRC staff is still in the process of developing a position on the defense-in-depth role to be played by the containment or confinement systems in non-LWRs. Attachment 4 to SECY-05-0006 provides some additional discussion on the assessment of containment options for modular HTGRs.

2.2 IAEA APPROACH TO DEFENSE-IN-DEPTH

The International Atomic Energy Agency (IAEA) published INSAG-10 [18] with a definition of the defense-in-depth safety philosophy, the key elements of which are summarized in Table 1. This IAEA concept of defense-in-depth has been incorporated into the PBMR approach to defense-in-depth.

Table 1: Levels of Defense-in-Depth According to IAEA INSAG-10

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

As discussed in Section 3, the PBMR has these means and accomplishes these objectives, with the clarifications that severe accidents in the PBMR do not entail core melt, and that off-site emergency planning is a licensing consideration that is outside the scope of a design certification.

2.3 REGULATORY BASIS SUMMARY

The scope and concepts of the definitions of the defense-in-depth safety philosophy reviewed in this section cover broad areas of design, regulatory requirements, and scenario based models of how a good application of defense-in-depth will be reflected in the prevention and mitigation of accidents.

Defense-in-depth involves the application of multiple lines of defense and conservative design and safety analysis approaches to assure the safe design and operation of nuclear reactors. With one exception in Appendix R to 10 CFR Part 50 dealing with fire protection programs, defense-in-depth is not a requirement per se but rather a philosophy that has been used to develop the requirements for currently licensed plants. Chapter 19 of the SRP provides a good summary of the defense-in-depth objectives for risk-Informed changes to currently licensed LWRs. NRC's Policy on the Regulation of Advanced Nuclear Power Plants provides useful guidance on defense-in-depth principles that should be considered for advanced reactor designs and a good perspective from which to evaluate the PBMR approach to defense-in-depth.

By and large the definitions and concepts of risk-informed defense-in-depth reflected in NRC regulations, policies and guidance documents are applicable to the PBMR. In the following section the PBMR approach to incorporating these defense-in-depth principles is described.

3. PBMR APPROACH

3.1 DEFINITION OF DEFENSE-IN-DEPTH FOR THE PBMR

3.1.1 Overview

Defense-in-depth is an established safety 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. Many different definitions of defense-in-depth have been published by the NRC and international regulatory authorities in regulations, regulatory guides, commission papers, and ACRS reports. Each of these definitions brings out a different facet of this important safety philosophy. A comprehensive set of definitions was reviewed in Section 2 in order to establish the depth and breadth of NRC expectations for applying the principles of defense-in-depth for a DCA for advanced reactors. The definitions that were reviewed are regarded as applicable to the PBMR when viewed at a high level. However, some interpretation of the details in these definitions is necessary because they have been couched in terms that are specific to LWRs. For example, the strategy of balancing of prevention and mitigation of core damage, has to be generalized somewhat before it can be meaningfully applied to the PBMR.

PBMR has embraced defense-in-depth in the development of its safety design approach and in the formulation of the regulatory process that is being proposed for the PBMR DCA. In order to clearly communicate how defense-in-depth has been applied to the PBMR and to identify potential issues in demonstrating the adequacy of defense-in-depth for the PBMR DCA, a definition of defense-in-depth for the PBMR is presented in this section.

PBMR has adopted a risk-informed and performance-based approach to defense-in-depth as outlined in Figure 1. This approach recognizes three major elements: **Plant Capability Defense-in-Depth**, **Programmatic Defense-in-Depth**, and a **Risk-Informed Evaluation of Defense-in-Depth**. This approach 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 PBMR. These three elements enable 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 plant as-designed will be built and will operate safely throughout the lifetime of the plant 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.

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 light water reactor plants and have been modified in recent years to reflect the changes in philosophy brought about by risk-informed and performance-based regulation. As noted previously, some of these definitions and concepts have been defined in terms that are specific to LWRs. The reason for having three major elements of defense-in-depth is to organize our thinking as we apply the underlying principles to the PBMR whose safety design philosophy differs in fundamental ways from that of an LWR. These elements are defined while recognizing that defense-in-depth principles are applied in many areas of plant design, assurance, and regulation.

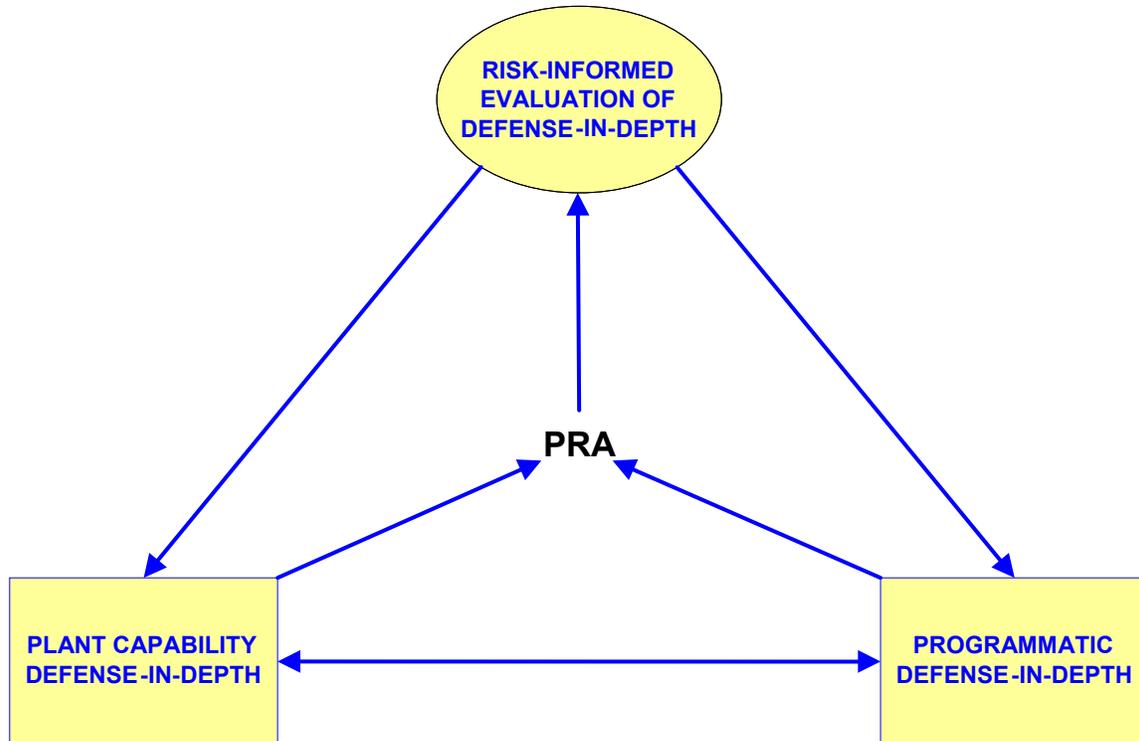


Figure 1: Elements of PBMR Approach to Defense-in-Depth

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** 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.

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, 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. 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 1 that represents the incorporation of risk insights into the development and enhancement of the plant capabilities and programs as the design and program development evolve.

In support of each of these elements of defense-in-depth is a comprehensive PRA which helps ensure that all decision making in these processes are systematically evaluated in a comprehensive risk-informed manner. The PRA is based on a plant design 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 modelled in the PRA. The reliability of the SSCs responsible for the **Plant Capability Defense-in-Depth** is adequately assured by the elements of **Programmatic Defense-in-Depth**. The PRA is called out separate from the defense-in-depth elements in Figure 1 because information from the PRA is used to support the design, provide input to the formulation of process requirements, and provide information to evaluate the adequacy and sufficiency of these defense-in-depth strategies. Conversely, the PRA itself provides a model of the plant capabilities and how the plant is operated and maintained under the programmatic controls, as part of the modelling 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 is utilized in all the elements of the defense-in-depth approach.

The PBMR approach to defense-in-depth is regarded as performance-based for several reasons. First, an objective perspective on the adequacy and sufficiency of defense-in-depth is provided by comparing the frequencies and consequences of the Licensing Basis Events (LBEs) and their uncertainties against the Top Level Regulatory Criteria (TLRC). 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 a basis for monitoring the reliability and availability performance 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. Hence, the approach is both performance-based and risk-informed.

The elements of the PBMR defense-in-depth approach are applied in an iterative process. Key elements of the safety design approach are fixed early in the design process. These elements include:

- Conservative design approach that minimizes challenges to safety systems and implements a passive SSC safety design approach
- Barrier design and configuration
- Inherent characteristics
- Definition of safety functions including those required to meet requirements and those that provide a supportive² role and contribute to defense-in-depth.
- Selection of passive and active SSCs to support required and supportive safety functions

The PRA is initially performed during the conceptual design and is then updated as design matures providing information that is factored into each design stage including:

- Events and event sequences challenging safety functions and SSCs
- Reliability and capability requirements for SSCs performing safety functions
- Definition of LBEs and margins between their frequencies, consequences, and uncertainties vs. the TLRC
- Risk and reliability insights to evaluate design options for each design stage
- Plant capability and engineering assurance program requirements updated at each stage of design

PRA models and ***Risk-Informed Evaluation of Defense-in-Depth*** are updated concurrently as the design and engineering assurance programs mature with feedback loops to enhance the ***Plant Capability Defense-in-Depth*** and ***Programmatic Defense-in-Depth*** elements as needed to demonstrate the adequacy and sufficiency of defense-in-depth. As the design matures there is greater emphasis placed on the development and enhancements to ***Programmatic Defense-in-Depth***, as the details of these programs cannot be defined without a mature design.

A more detailed definition of the elements of the PBMR approach to defense-in-depth is provided in Figure 2 and is explained more fully in the following sections.

3.1.2 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 physical lines of defense include multiple barriers, inherent reactor characteristics, and engineered features and SSCs whose safety functions serve to protect the integrity of these barriers. Barriers have two roles including 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 physical barriers and associated safety systems that

² The term 'supportive' is used here to note that an SSC may be capable of providing a safety function even though it might not be required and may not receive special treatment.

prevent or block the movement of radionuclides, as well as time delays in the transport that allow for the radioactive decay and deposition of radionuclides prior to their release, time for implementation of emergency protective actions, and 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 use of inherent features and passive SSCs as a first line of defense in the performance of safety functions and conservative design margins to improve the capability of SSCs to withstand challenges that may exhibit uncertainties.

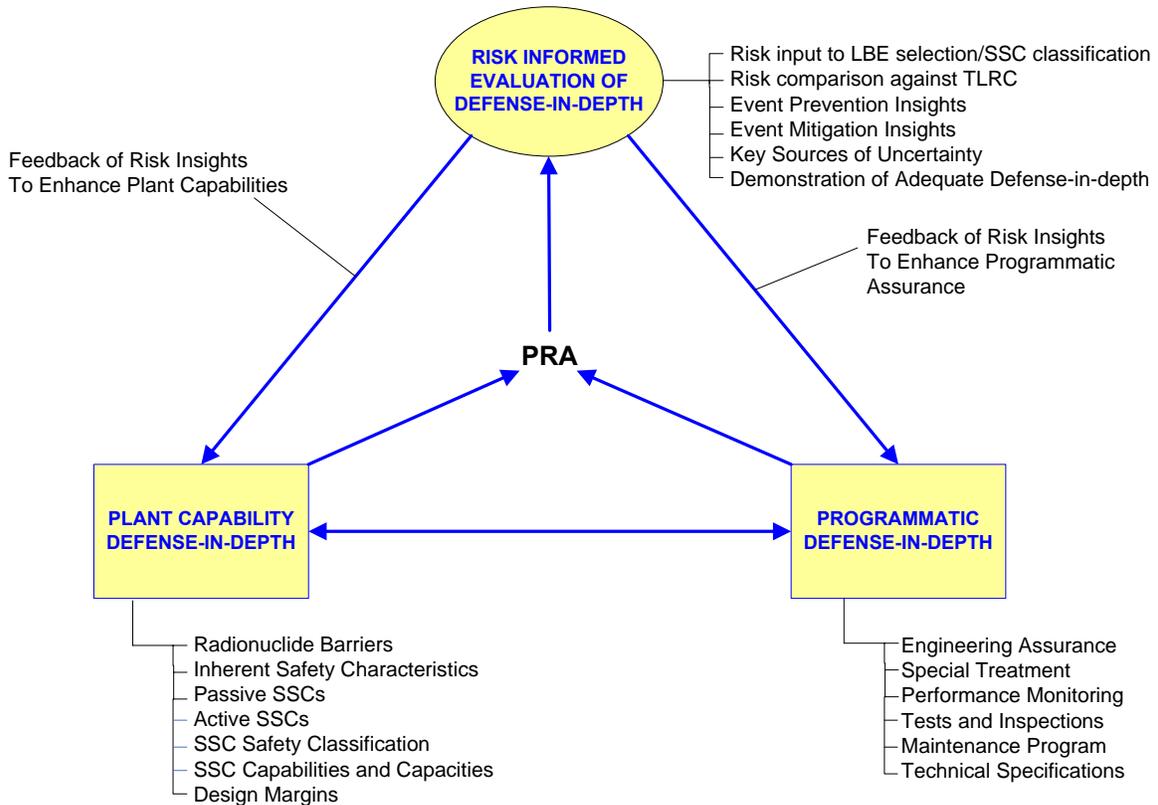


Figure 2: Detailed Elements of PBMR Defense-in-Depth Approach

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 (Brayton) 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 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
 - 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 as conceptualized in Figure 3. In this concept, a set of multiple physical barriers is introduced between the hazard, i.e. the inventory of radioactive material in the reactor, and the environment. A model for these barriers that applies to all existing and advanced reactors consists of the fuel element and its cladding, 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 reactor siting 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.

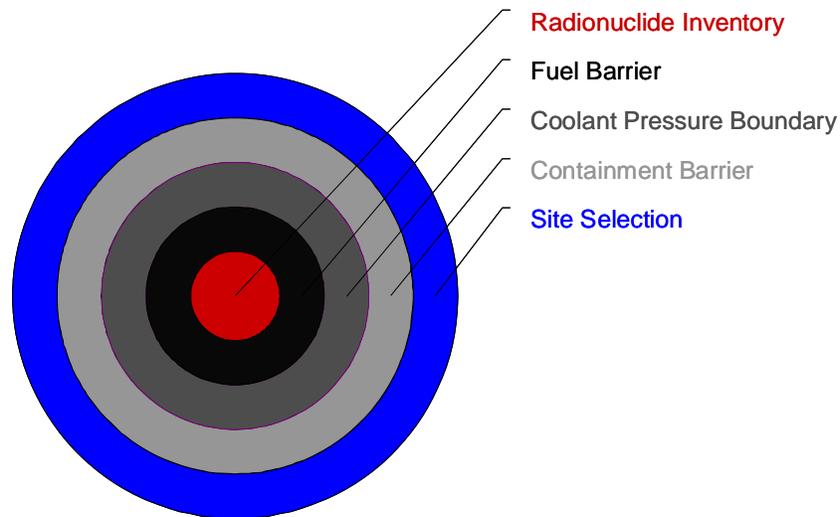


Figure 3: Barriers to Radionuclide Transport Included in *Plant Capability Defense-in-Depth*

Important attributes of the use of barriers in ***Plant Capability Defense-in-Depth*** are to ensure that the barriers are concentric and independent so that 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 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 the barrier. Full independence among barriers may not be feasible for any reactor concept, however the extent of independence is an important attribute to consider in evaluating the adequacy of defense-in-depth. As illustrated in Figure 4 the elements of the safety design approach for the reactor provide a starting point for developing the ***Plant Capability Defense-in-Depth***.

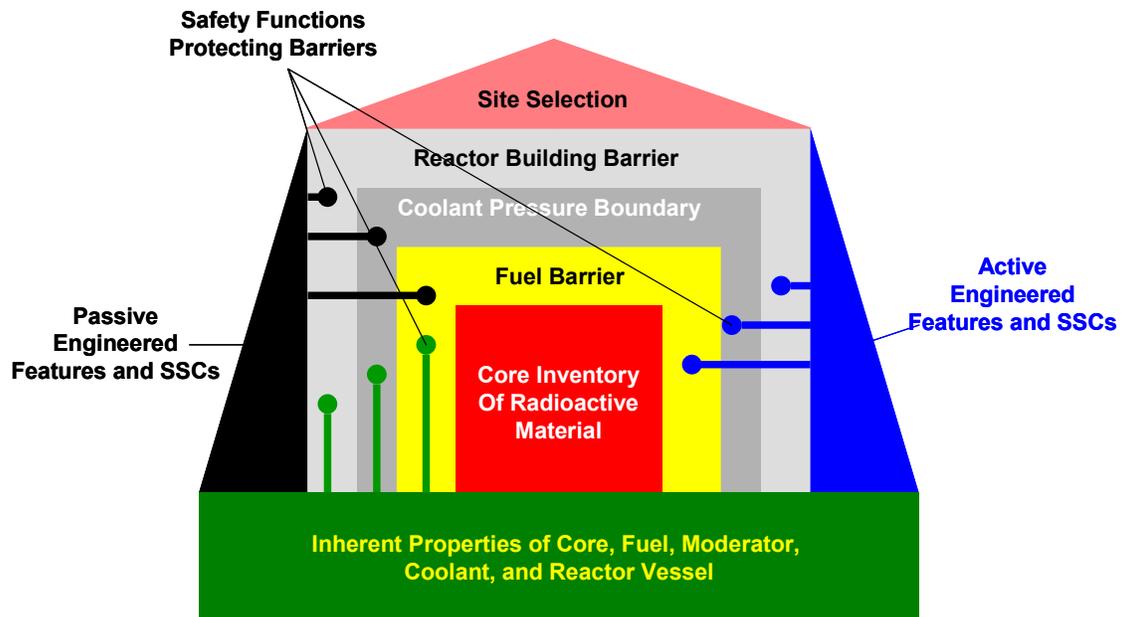


Figure 4: Elements of Safety Design Approach Incorporated into *Plant Capability Defense-in-Depth*

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 either directly by contributing to the integrity of the radionuclide barriers or by dictating the requirements for engineered features that are provided to support barrier integrity, or 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 different minimum sets of safety functions that need to be supported to protect the barriers to achieve 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 gas-cooled reactors such as the PBMR, coolant inventory control, while necessary to produce electric power, is not required to protect the integrity of the fuel. In the PBMR, the safety significance of the helium pressure boundary is not to control the helium inventory but rather to provide a barrier to fission product release and to protect against chemical attack. 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.

Table 2: 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

In the design of the engineered features to support each safety function there are both passive and active strategies to consider. 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*** for the PBMR 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 to mitigate accidents. As explained previously, this is an iterative process which 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 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 including 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 for those features that 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 2. In contrast with the definitions of defense-in-depth reviewed in Section 2, this definition includes explicit consideration of inherent features that play important roles in the performance of safety functions and the delineation of engineered safety functions into those 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 an adequate reliability and capability to perform these functions.

3.1.3 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, and to provide protection against uncertainties for the life of the plant after the plant has been designed. These programs include the special treatment requirements for safety classified SSCs, tests and inspections, monitoring of plant and SSC performance, and oversight.

The PBMR approach focuses on the DCA 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 Top Level Regulatory Criteria (TLRC), 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 Licensing Basis Events (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: 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
-	Operator training programs
-	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
-	Root cause analysis
-	Event trending
-	Closure effectiveness

When the frequencies and consequences and associated uncertainties for each LBE are compared against the TLRC, the classification of each LBE as an Anticipated Operational

Occurrence (AOO), Design Basis Event (DBE), or Beyond Design Basis Event (BDBE) conservatively accounts for the uncertainties. The frequency-dose criteria embodied in the TLRC are set with significant margins against the NRC Safety Goal Quantitative Health Objectives (QHOs). Adherence to the TLRC assures that the QHOs for the individual risk of latent cancer fatality are met by several orders of magnitude [19]. There is additional conservatism introduced by the requirement to demonstrate that each Deterministic Design Basis Accident can be sufficiently mitigated with only the safety classified 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, 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. The bases for the specific requirements are derived from **Risk-Informed Evaluation of Defense-in-Depth**, as described below. In the view of PBMR this definition of **Programmatic Defense-in-Depth** is consistent with the engineering assurance program elements of the defense-in-depth definitions reviewed in Section 2. A major goal of the pre-application review is to work out the specific expectations for establishing the proper level of **Programmatic Defense-in-Depth** for the PBMR. These expectations will need to be developed in the context of the PBMR approach for the PRA, the selection of Licensing Basis Events (LBEs), the safety classification of SSCs, and the derivation of special treatment requirements for SSCs.

3.1.4 Risk-Informed Evaluation of Defense-in-Depth

3.1.4.1 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 PBMR DCA. The structure of these scenarios, in a manner that permits the identification of prevention and mitigation, assures that the strategies of **Plant Capability Defense-in-Depth** and **Programmatic Defense-in-Depth** have been adequately implemented. The strategies of accident prevention and mitigation 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 the prevention and mitigation of accidents. For the PBMR, the strategies of prevention and mitigation are defined somewhat more broadly than for currently licensed reactors, which focus on the prevention and mitigation of core damage. In the case of the PBMR 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 in the PBMR.

Prevention strategies are 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. Hence prevention and mitigation are directly correlated to the reliability and capability of the SSCs responsible for providing the **Plant Capability Defense-in-Depth**. The evaluation of 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 PBMR approach to defense-in-depth provides the best estimate plant performance evaluation framework 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 that are to be included in the plant design basis and the scope of all deterministic and probabilistic safety evaluations. This framework is useful for the incorporation of information and insights from the PRA and to the formulation of strategies that can be implemented in both the **Plant Capability** and **Programmatic Defense-in-Depth** elements.

3.1.4.2 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 design certification. The PBMR approach to addressing this challenge is defined by a set of defense-in-depth principles that were derived from the regulatory foundation that was 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 [11] and the advanced reactor design attributes from the NRC policy on Regulation of Advanced Nuclear Power Plants [9]. 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 4 together with an evaluation of how these objectives could be used to evaluate the PBMR design. 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 which relies on active engineered systems to perform the required safety functions for the design basis events.

Table 4: 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 PBMR DCA
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 Regulatory 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 advanced reactor policy statement and organizing the principles according to the PBMR approach to defense-in-depth that is outlined in the previous section, the defense-in-depth principles of Table 5 were developed. Table 5 combines the strengths of the two source documents, and is restructured to better align with our (PBMR's) approach to defense-in-depth.

One significant change in this table 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 PBMR. 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 the defense-in-depth. This is the set of defense-in-depth criteria that PBMR proposes to use in its design certification.

A logical approach for evaluating the adequacy and sufficiency of defense-in-depth as part of the risk-informed evaluation is shown in Figure 5. The intent of this approach is to systematically ensure that the defense-in-depth principles of Table 5 have been adequately applied. A primary step towards meeting these principles is to meet the frequency-dose requirements within the TLRC. This implies that the reliabilities and capabilities of the SSCs that are modelled in the Licensing Basis Events (LBEs) are adequate to prevent the Design Basis Events (DBEs) and Beyond Design Basis Events (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 principle of achieving an appropriate level of prevention and mitigation is accomplished by examining the PRA results in a structured way in order to provide an objective definition of what is meant by prevention and mitigation for the PBMR and to identify the specific SSCs responsible for the prevention and mitigation of each LBE. This structured approach is summarized in the next section and explained in some detail with examples in the Appendix.

In the course of performing and reviewing the PRA and the deterministic safety analysis, key uncertainties will be identified 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 the risk-Informed evaluation of the adequacy of defense-in-depth is to ensure that all the principles of Table 5 have been adequately applied. The main elements of the ***Risk-Informed Evaluation of Defense-in-Depth*** are summarized in Table 6.

Table 5: Principles for Establishing the Adequacy of Defense-in-Depth for the PBMR**1. 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 4)
- ✚ 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 4) These strategies include:
 - 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.
 - use of appropriate combinations of inherent reactor characteristics, passive SSCs, and active SSCs in the performance of safety functions
 - use of redundant, diverse, and independent means of fulfilling each safety function (SRP Principles 3, 7 and 9 in Table 4)
 - use of adequate safety margins and conservative design approaches to address uncertainties in barrier and SSC performance (Use of SRP Principle 7 in Table 4)
 - use of 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 4)
 - use of 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 4)

2. Programmatic Defense-in-Depth Principles:

- ✚ 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:
 - avoid over-reliance on programmatic approaches to compensate for design weaknesses (SRP Principle 6 in Table 4)
 - address significant uncertainties identified in the performance and review of the PRA (SRP Principle 7 in Table 4), and
 - 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 4)

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 4)
 - 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 4)
 - 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 4)
 - 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 4)
 - deterministic requirements are met (SRP Principle 11 in Table 4)

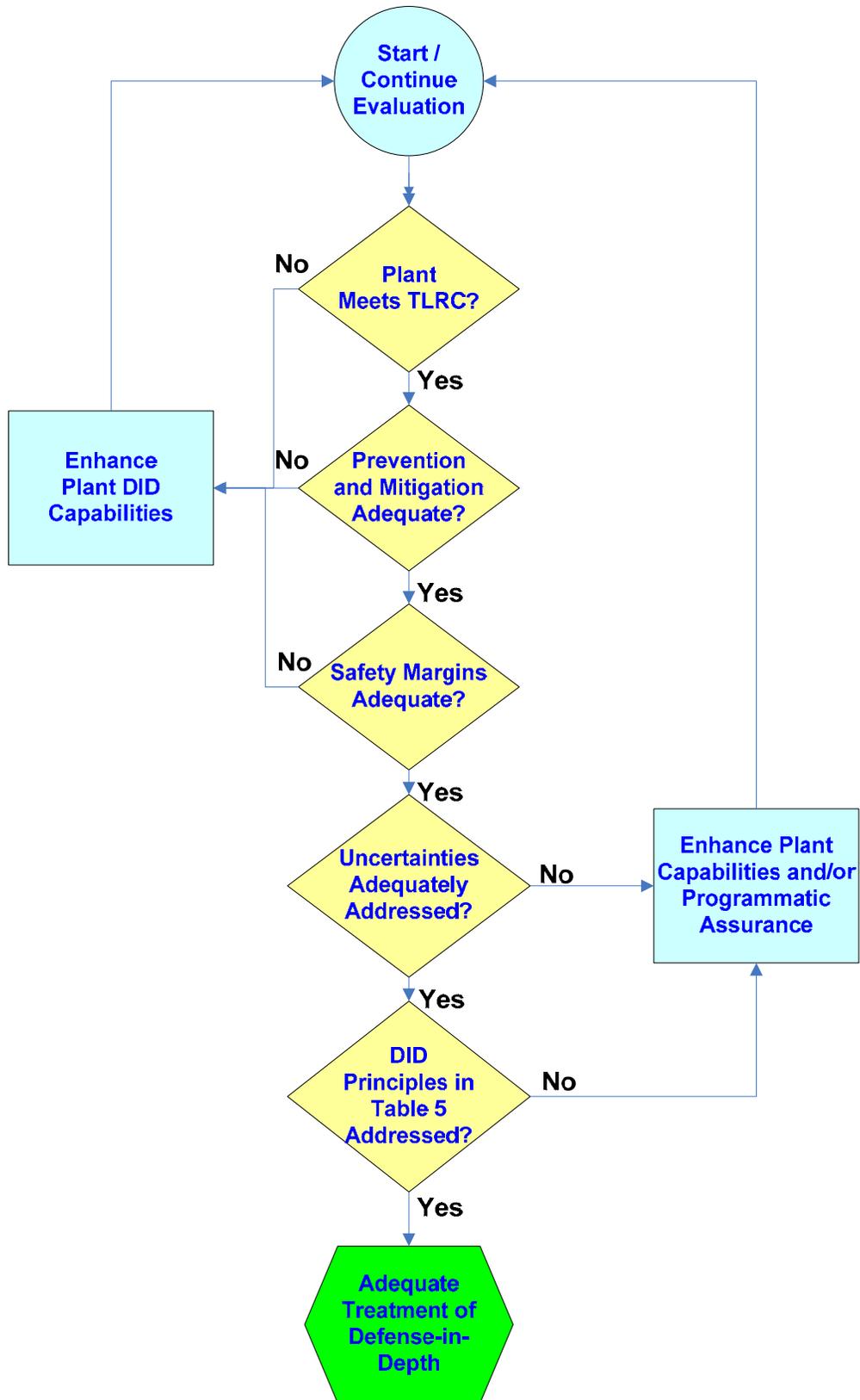


Figure 5: Logic for Implementing *Risk-Informed Evaluation of Defense-in-Depth*

Table 6: Elements of Risk-Informed Evaluation of Defense-in-Depth

<ul style="list-style-type: none"> ✚ Definition of a comprehensive set of challenges to barrier integrity <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - Strategies to limit impact of challenges and loads to barriers and SSCs - Strategies to retain and delay transport of radionuclides from barriers during accidents <ul style="list-style-type: none"> ▪ 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 <ul style="list-style-type: none"> - 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
--

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. Those proposed programs that cannot be attributed to reducing uncertainties and enhancing the plant capabilities with respect to the TLRC will be deemed of no significant added value and will not be implemented, unless required by NRC regulations or for other purposes. It is important that such programs be held accountable to their effectiveness as risk management tools.

3.1.4.3 Consistency with IAEA Approach

The prevention and mitigation strategies that are evaluated in the ***Risk-Informed Evaluation of Defense-in-Depth*** are consistent with the definition of defense-in-depth developed by the IAEA [18]. This is illustrated in Figure 6. 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 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. As explained more fully in the next section, the IAEA scenario framework for defining defense-in-depth is useful in the evaluation of prevention and mitigation strategies that contribute to defense-in-depth.

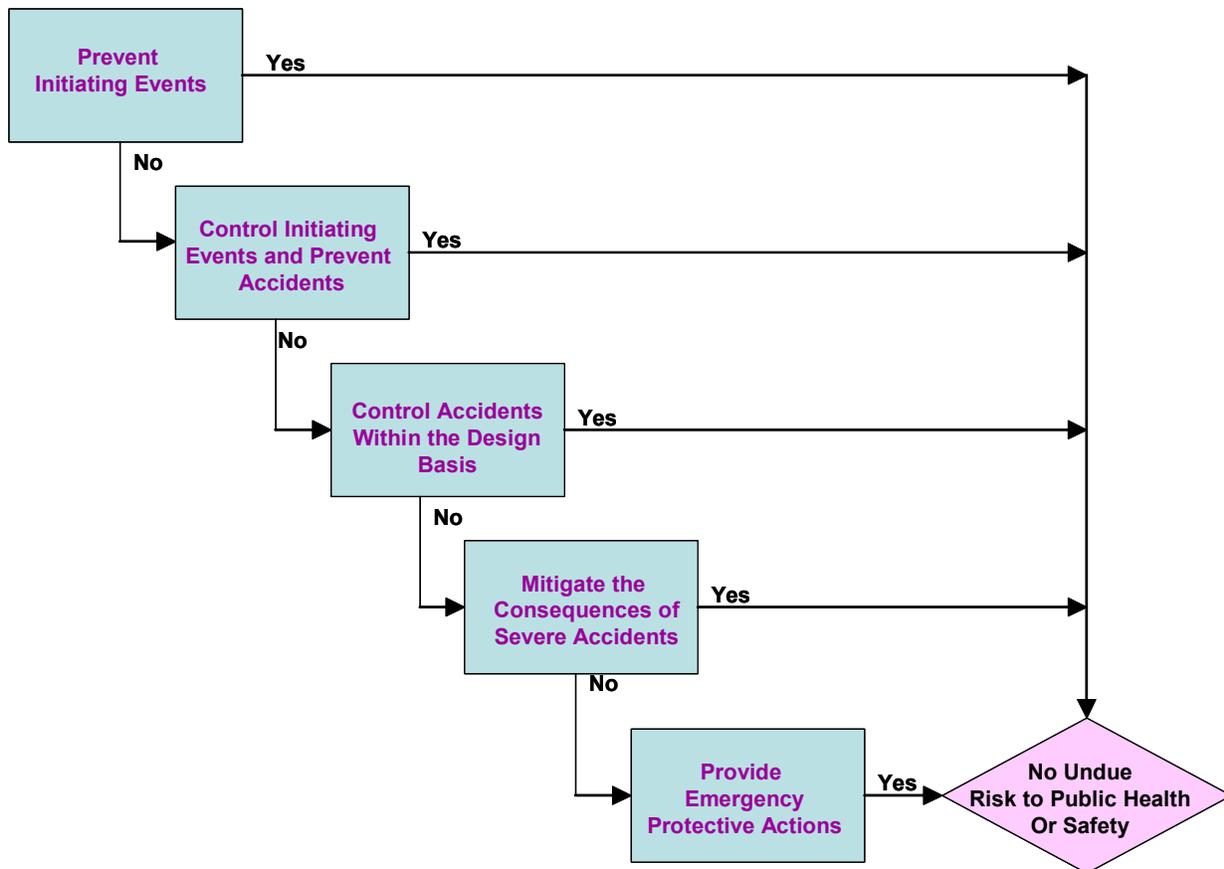


Figure 6: Scenario Framework for Defense-in-Depth Provided by IAEA

3.1.4.4 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 Licensing Basis Events (LBEs) and the results of the PRA help establish that Top Level Regulatory Criteria (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 PBMR 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 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. This approach is outlined below.

The PRA has an important role to play in ***Risk-Informed Evaluation of Defense-in-Depth*** as it provides an objective way to identify the roles that each plant safety feature plays in the prevention and mitigation of accidents and to examine how these risk management strategies are balanced. The PRA is used to provide some clarity of the meaning of prevention and mitigation for a reactor such as the PBMR that does not utilize risk metrics such as core damage frequency. Using this approach, information from the PRA is used to answer the questions: *What are we trying to prevent?* and *What are we trying to mitigate?*

An accident sequence can be described in terms of the following elements. This form of sequence definition lends itself to defining what is meant by prevention and mitigation, and to identifying which SSCs are responsible for different degrees of prevention and mitigation.

1. **Initiating Event** An initiating event that constitutes a challenge to the plant systems and structures responsible for control of transients and protection of the plant SSCs including the radionuclide transport barriers.
2. **Active SSC Response** The response (successes and failures) of active systems that support key safety functions responsible for protection of barriers, retention of radioactive material, and protection of the public health and safety, as defined by the accident sequence.
3. **Passive SSC Response** The response of passive design features responsible for supporting key safety functions, including the structures that form the radionuclide barriers themselves and the passive systems that support them.
4. **Barrier Retention Factors** The response of each barrier to radionuclide transport from the radioactivity sources to the environment to the initiating events and safety system responses. This response is expressed as the degree of retention of radioactive material for each barrier expected for the sequence; these barriers include the fuel elements, the coolant pressure boundary, and the reactor building barrier. Depending on the reactor design, the reactor building barrier may be described as a leak tight or vented containment, confinement, reactor building or containment system barrier.

5. **Emergency Plan Response** The implementation of emergency plan protective actions to mitigate the radiological consequences of a given release from the plant.

In this definition, all the SSCs performing or supporting a safety function are included, irrespective of the SSC safety classification, as opposed to restricting the definition to those functions that prevent core damage or those SSCs that are classified as safety related. It is noted here, however, that the point along an accident sequence that one chooses to talk about prevention vs. mitigation can be varied producing different perspectives from which to define what is to be prevented and what is to be mitigated. For example, if the point of accident initiation is chosen, then actions to reduce the frequency of an initiating event may be regarded as prevention, while any feature that reduces the probability of failure of systems and structures or magnitude of release at steps 2 through 5 would constitute mitigation of the consequences of the initiating event. Moreover, the use of passive design features that limit the release from the fuel when active systems are postulated to fail could be equally regarded as preventing large releases as mitigating the consequences of active system failures. Hence, while there is a precedent for using core damage as a pivot point for defining prevention and mitigation for LWRs, the more generalized accident sequence framework presented above is technology neutral and lends itself to a more complete definition of the strategies of accident prevention and mitigation, which can be applied at any point along the event sequence.

The development of this framework for discussing accident prevention and mitigation makes use of the following key PRA insights:

- Absolute prevention of an accident would imply that the frequency of the accident is zero, i.e. impossible. However, the PRA approach is not to prove impossibility but to assume possibility and to estimate the frequency. Hence, design features and characteristics that reduce the frequency of a given accident are viewed from the PRA perspective as contributing to prevention. Those that prevent or reduce the level of consequences as viewed from a particular point along an accident sequence are viewed as contributing to mitigation.
- A given design feature that contributes to prevention, mitigation, or both exhibits varying degrees of importance on different accident sequences. Hence it is necessary to examine a spectrum of sequences some of which may include successful operation of the design feature and others that postulate its failure to understand the safety significance of the design feature. This insight is consistent with the way in which safety significance has been defined in risk-informed regulation of LWRs.
- A design feature may be postulated to fail along one sequence, but operate successfully on another so it may prevent an accident in some cases and mitigate an accident in others. Hence the extent to which risk is managed by prevention or mitigation by a given design feature varies across the accident sequence spectrum.

A generalized model for describing an accident sequence in terms of the design features that support prevention and mitigation reflecting the above insights is provided in Table 7. This table provides an important feedback mechanism between **Risk-Informed Evaluation of Defense-in-Depth** and **Plant Capability Defense-in-Depth**. The event sequence framework is part of the **Risk-Informed Evaluation of Defense-in-Depth** and the roles of SSCs in the prevention and mitigation of accidents are the result of **the Plant Capability Defense-in-Depth**. The reliabilities and capabilities of the SSCs that prevent and mitigate events are influenced by both

the **Plant Capability** and **Programmatic Defense -in-Depth** elements. **Programmatic Defense-in-Depth** reduces the uncertainty in the reliability and capability performance of the SSCs responsible for prevention and mitigation.

The accident sequence framework for evaluating accident prevention and mitigation in Table 7 is used to define a simple model for estimating the risk of a release of radionuclides associated with a specific accident sequence, or Licensing Basis Event (LBE):

$$R_j = Q * F_{IE,j} * P_{ASSC,j} * P_{PSSC,j} * r_{fuel,j} * r_{PB,j} * r_{cont,j} \quad (1)$$

Where:

- R_j = Expected quantity of radioactive material released per year from sequence j
- Q = Quantity of radionuclides (for a given isotope) in the reactor core inventory
- $F_{IE,j}$ = Frequency of the initiating event associated with sequence j
- $P_{ASSC,j}$ = Probability of the successful and failed active SSCs along sequence j
- $P_{PSSC,j}$ = Probability of the passive structure successes and failures along sequence j
- $r_{fuel,j}$ = Release fraction from the fuel, given system and structure response for sequence j
- $r_{PB,j}$ = Release fraction from the HPB, given system and structure response for sequence j
- $r_{cont,j}$ = Release fraction from the reactor building barrier, given system and structure response for sequence j

Table 7: Event Sequence Model for Prevention and Mitigation

Standard Elements of Accident Sequence	Design Features Contributing to Prevention	Design Features Contributing to Mitigation
Initiating event occurrence	Reliability of SSCs supporting power generation reduces the initiating event frequencies; successful operation of the SSCs prevents the sequence	Capabilities of normally operating systems to continue operating to prevent initiating events serve to mitigate events and faults that may challenge these functions
Response of active SSCs supporting safety functions: successful and failed SSCs	Reliability and availability of active SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence	Capabilities of active successful SSCs reduce the impacts of the initiating events and reduce the challenges to barrier integrity.
Response of passive features supporting safety functions: successful and failed SSCs.	Reliability and availability of passive SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence	Capabilities of passive successful SSCs reduce the impacts of the initiating events and reduce the challenges to barrier integrity.
Fraction of source term released from fuel	None	Inherent and passive capabilities of the fuel given successful active or passive SSCs limit the release from the fuel.
Fraction of source term released from the coolant pressure boundary	None	Inherent and passive capabilities of the pressure boundary given successful active or passive SSCs and the capabilities of the fuel limit the release from the pressure boundary.
Fraction of source term released from reactor building barrier	None	Inherent and passive capabilities of the reactor building barrier conditioned on the successful response of any active or passive SSCs along the sequence and the capabilities of the fuel and coolant pressure boundary limit the release from the reactor building barrier.
Time to implement emergency plan protective actions.	None	Inherent and passive features and capabilities of the fuel, coolant pressure boundary, and reactor building barrier conditioned on the successful response of any active or passive SSC along the sequence dictate the time available for emergency response.

In view of the large uncertainties inherent in quantifying the risk of low frequency accidents, the quantification of Equation (1) cannot be calculated with high precision. However, the application of the equation to explore the roles of SSCs in the prevention and mitigation of accidents only requires approximate, order of magnitude estimates as only the relative magnitudes are significant for this application. Such rough estimates are all that is needed because the accident spectrum encountered in a PRA spans many orders of magnitude of accident frequency and release fractions.

Due to functional, physical, and human dependencies, each probability term in the right hand side of this equation is dependent on the events that precede it along the sequence as would be included in a competent PRA model. The partitioning of the risk into these specific terms is designed to support an evaluation of specific strategies for preventing and mitigating the risks of accidents.

Note that each term on the right hand side of Equation (1) whose values is less than 1 can be regarded as a 'risk reduction factor'. If we start with the certainty of the inventory Q and consider that the upper bound frequency of releases from this inventory is once per year³, then each factor less than 1 contributes to reducing the risk of a release as calculated in this equation in relation to the certainty of the radionuclide inventory. By noting the SSCs that correspond to each factor, this equation can be used to quantify the importance of each design feature in managing the risk for the associated sequence.

In the above formulation, highly reliable SSCs responsible for power production and keeping the plant in stable conditions reduce the frequency of initiating events and thereby prevent accidents from initiating. Highly reliable and available active and passive SSCs that are postulated to fail along the accident sequence manage the risk by reducing the values of $P_{ASSC,j}$ and $P_{PSSC,j}$. Hence the reliability characteristics of these systems prevent accidents. SSCs that are postulated to be successful along the sequence in the PRA model help reduce the loads on the barriers and together with the inherent features of the barriers help to prevent releases or reduce the magnitudes of the release fractions. The capabilities of these systems and structures when successful help to mitigate the consequences of the accidents. When a necessary and sufficient combination of successful SSCs meets the success criteria for the protection of each barrier, releases from that barrier are prevented. By examining the values of the response probabilities and the release fractions along each accident sequence that determines the risk profile, the role of design features in contributing to prevention and mitigation of accidents can be objectively quantified. When this process is applied to a representative set of accident sequence families that characterize the overall risk profile, a comprehensive assessment of the importance of each design feature in preventing and mitigating accidents is achieved. While the uncertainties that are inherent in estimating each of the factors in the equation are large, the objective is not an accurate allocation, but rather a rough order of magnitude feel for the relative importance of each design feature in contributing to the prevention and mitigation of accidents. Such estimates are indeed available from the results of a quality PRA of the type that will be developed to support the PBMR DCA.

³ While there is no theoretical upper bound for an event frequency, this is a practical upper bound for an accident with a significant release because the first such accident in any year will certainly be the last for that year and for the plant lifetime if any appreciable fraction of the core inventory is released.

To demonstrate the application of this concept an evaluation has been performed of selected event sequences from the MHTGR PRA [20]. The MHTGR has a package of inherent characteristics and engineered features that are representative of various modular gas cooled reactor designs using particle fuel, graphite moderator, helium working fluid, and passive decay heat removal capabilities similar to that included in the PBMR.

MHTGR-1: Moderate size leak in the Helium Pressure Boundary (HPB) of less than 13 in²; successful reactor trip and continued operation of one of the forced convection cooling systems; releases limited to circulating activity and some lift off of plated out radionuclides. This sequence is a representative Design Basis Event for the MHTGR.

MHTGR-2: Small leak in the HPB of less than 1 in²; successful reactor trip, failure of the active forced convection cooling systems; conduction cool down of the core using the active Reactor Cavity Cooling System (RCCS); releases limited to circulating activity and delayed release from small fraction of initially failed fuel particles that is minimized due to the successful HPB pump down along this sequence. This sequence is also a Design Basis Event but with a lower frequency and higher potential for release than MHTGR-1.

MHTGR-3: Small leak in the HPB of less than 1 in²; successful reactor trip; failure of the active forced convection cooling systems; failure of the active RCCS; conduction cool-down to the passive reactor cavity heat sinks; releases limited to circulating activity and delayed release from small fraction of initially failed fuel particles (somewhat larger fraction than in Sequence 2). This sequence is representative of a Beyond Design Basis Event for the MHTGR.

The risk plot in Figure 7 shows the frequencies and consequences of these three event sequences in which the consequences are expressed in terms of curie releases of the nuclide I-131, which has been shown to be a highly risk significant radionuclide for HTGR event sequences. By tracing through the terms of Equation (1) for these sequences the roles of SSCs responsible for accident prevention and mitigation can be easily identified using the logic of Table 7. By comparing the risks of these sequences to the certainty of the radionuclide inventory the risk reduction factors for each prevention and mitigation element can be identified. A bar chart that depicts these risk reduction factors is shown in Figure 8.

As seen in these figures the roles of prevention and mitigation for MHTGR-1 include 2 orders of magnitude of prevention by the reliability of the Helium Pressure Boundary, and 9 orders of magnitude of mitigation by the barriers. For this sequence there is a low level of importance of the reactor building barrier due to the roles of the fuel and HPB in retaining the vast proportion of the inventory.

MHTGR-2 involves a small breach in the pressure boundary followed by failure of the active SSCs supporting core cooling functions. The mitigation level for this sequence is aided by a passive core cooling capability that prevents significant releases from the fuel, although the releases are somewhat higher than in Sequence MHTGR-1. In MHTGR-3 there is failure of both active and passive core cooling systems following the pressure boundary breach, but the passive capability of the reactor to retain its fuel inventory is still significant as the core is still cooled by conduction and radiation to the reactor building heat sinks. What is striking about the prevention and mitigation analysis for these MHTGR sequences is that the mitigation importance of the fuel retention is significant for all envisioned sequences. This is to be

expected because the safety design approach for the MHTGR design includes a capability to maintain fuel integrity for each of these selected sequences. The roles of the barriers and the SSCs supporting each barrier are seen to be significantly different than those for the LWR example due to the differences in the safety design approach.

While one can use this process to attribute SSC roles and to quantify the SSC importance in preventing and mitigating accidents, it is important to note that the assessment of risk for any sequence for any reactor type is a function of how the inherent features and engineered features respond to the initiating event and interact with each other to produce the definition, frequency, accident progression and consequence of the scenario. In particular the role and importance of leak tight reactor building barriers in implementing the defense-in-depth concept should be evaluated in the context of the inherent features, particularly those that determine the fuel performance under accident conditions. This integrated perspective of risk factors is an important principle of **Risk-Informed Evaluation of Defense-in-Depth** that is essential to defining and evaluating prevention and mitigation strategies.

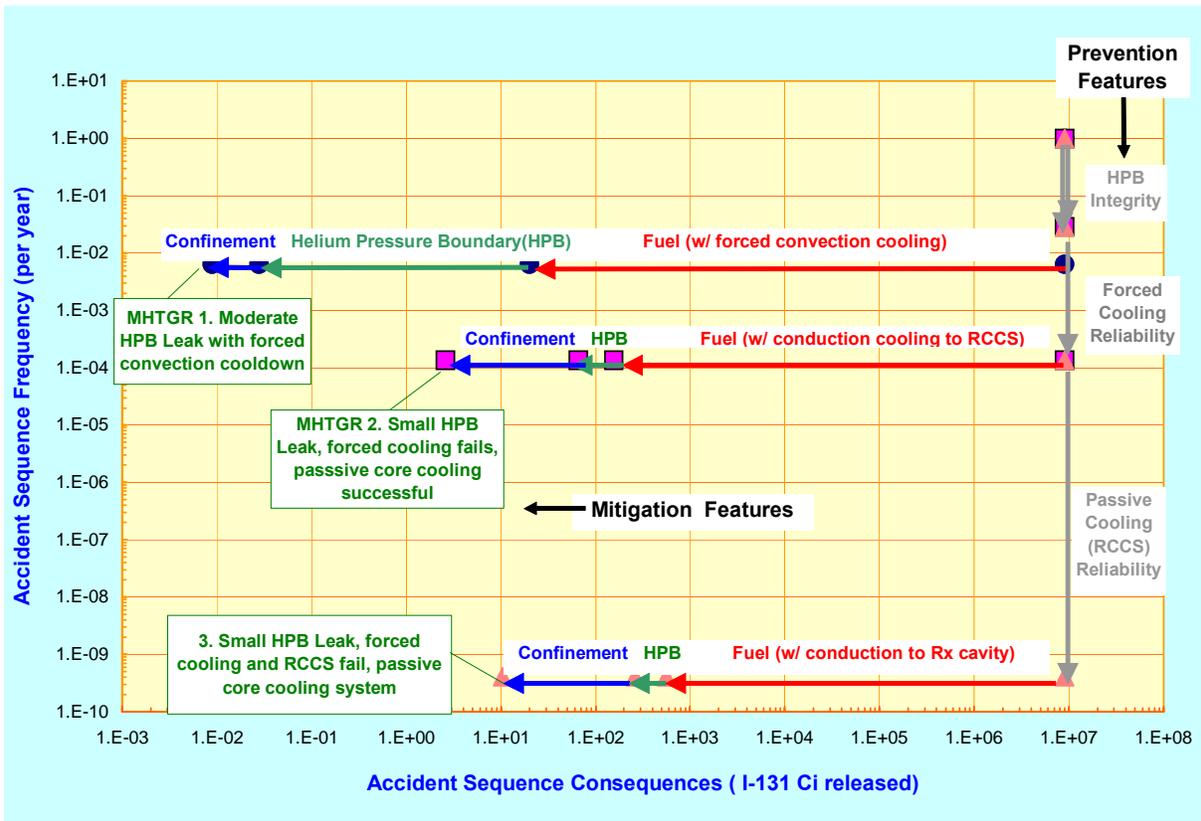


Figure 7: Design Features Contributing to Prevention and Mitigation of I-131 Releases from Selected MHTGR Sequences

Upon review of these sequences, it is instructive to review some of the elements of the earlier definitions of defense-in-depth. Several conclusions are supported by these examples:

- These examples support the conclusion that there exists no single ‘balance’ between prevention and mitigation. The roles of SSCs in the prevention and mitigation of accidents are inherently different for different sequences. High frequency/low consequence accidents appear to be addressed with more emphasis on mitigation than prevention, whereas low frequency/high consequence accidents rely more on prevention and progressively less on mitigation. Hence, the degree of ‘balance’ between prevention and mitigation should be assessed over a spectrum of event sequences ranging from high frequency-low consequence events to low frequency-high consequence events.
- There is no such thing as fully independent barriers to radioactivity release, as all the barriers are mutually dependent on the inherent features of the reactor and how these features interact with the respective barriers, which is different on different sequences. An important role of the PRA is to identify and evaluate the dependencies among the barriers. Barrier independence is a goal to strive for but in practice is only achieved in a manner of degrees.
- Differences in the safety design approach between different reactor designs are reflected in differences in the roles that each barrier and SSC play in the prevention and mitigation of accidents. In these examples, as well as additional LWR examples developed in the Appendix, it is seen that different reactors may apply prevention and mitigation using different combinations of inherent features, and passive and active SSCs.

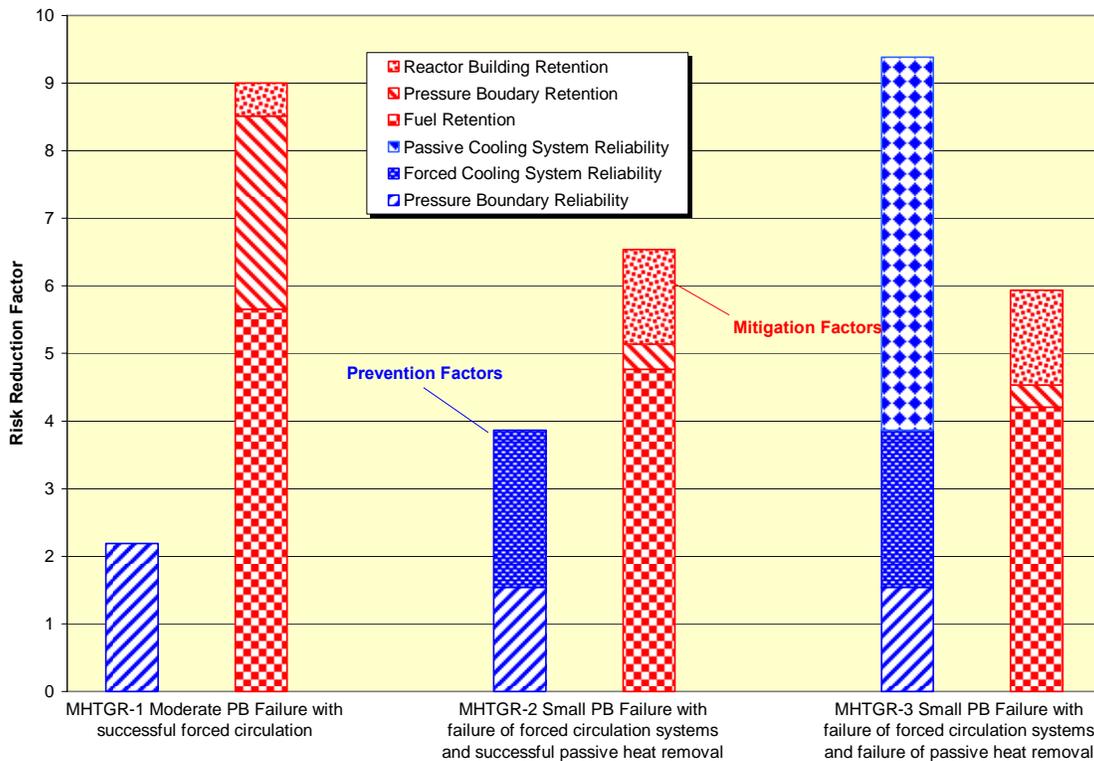


Figure 8: Risk Reduction Factors Associated with MHTGR Design Features Responsible for Prevention and Mitigation of I-131 Releases

It is acknowledged that there are uncertainties inherent in the PRA results that were used to support such examples. Hence, if one varies the PRA inputs selected for these examples, different results and conclusions could be obtained. A systematic review of the PRA uncertainties is an important element of ***Risk-Informed Evaluation of Defense-in-Depth*** and is expected to reveal performance issues that are most efficiently addressed by the addition of specific deterministic requirements.

These examples serve to demonstrate how PRA results can be used to examine and quantify the importance of specific design features in preventing and mitigating severe accidents. These order of magnitude estimates of risk reduction factors using PRA techniques are only intended to provide rough order of magnitude estimates of importance. Nonetheless, such estimates provide insights into the adequacy of defense-in-depth. In the PBMR DCA, an evaluation similar to that shown in these examples will be performed to assist the NRC in their review of the adequacy of ***Risk-Informed Evaluation of Defense-in-Depth*** for the PBMR.

3.2 PBMR IMPLEMENTATION OF DEFENSE-IN-DEPTH

3.2.1 PBMR Implementation of *Plant Capability Defense-in-Depth*

For the PBMR 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 actions such as pumps, blowers, HVAC, sprays; b) depending on availability 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. PBMR passive design features utilize inherent characteristics and properties associated with the fuel, moderator, and helium coolant as discussed previously.

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. The specific design features and SSCs that form the PBMR approach to ***Plant Capability Defense-in-Depth*** were described in the NRC in PBMR Pre-application Safety and Design Familiarization Workshops conducted in February and March, 2006 [21], [22].

3.2.1.1 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 PBMR are listed in Table 8. The most significant radionuclide inventories in the PBMR plant are those associated with the fuel inside the reactor vessel and that which is normally circulating between the core and the Fuel Handling and Storage System (FHSS). There are additional significant radionuclide inventories in the Spent Fuel Tanks which inventory accumulates during 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 moved to the Used Fuel Tank.

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 (Figure 9).

Table 8: PBMR Radioactive Sources and Barriers

Radioactive Material Source	Barriers to Radionuclide Transport
Fuel spheres in the core	Coated particles, graphite matrix, Helium Pressure Boundary, Citadel, reactor building
Fuel spheres outside the core	Coated particles, graphite matrix, Fuel Handling and Storage System (FHSS) piping, Spent Fuel Tanks (SFTs), Used Fuel Tank (UFT), or new fuel tanks, reactor building
Non-core sources within the MPS	Helium Pressure Boundary, reactor building
Other sources	Various tanks, piping systems and containers, reactor building or ancillary buildings housing waste management equipment

For the fuel spheres in the core and the other sources of radioactive material within the Main Power System (MPS) as well as the circulating fuel spheres in the FHSS, there are three additional physical and passive barriers to protect the integrity of the fuel and restrict the transport of radioactive material, including the Helium Pressure Boundary, the Citadel, and the reactor building confinement. As shown in Figure 10, the HPB consists of pressure vessels, piping, and heat exchangers that envelop the helium reactor heat transport fluid within the MPS, the Helium Inventory Control System (HICS), and the FHSS. The citadel and the vented reactor building confinement function are part of the PBMR containment system which also includes the Reactor Building Specialized Doorways Subsystem, Pressure Relief System (PRS) and HVAC system for maintaining pressure differentials to prevent an outward release path and for filtration of radionuclide released from the HPB and citadel. A more complete description of the passive and active SSCs that support the integrity and effectiveness of the passive barriers is provided in the next sections.

For fuel spheres that are not contained within the citadel and HPB there are tanks and piping systems that maintain a helium environment for the fuel and provide a secondary barrier to radionuclide transport. The SSCs supporting the containment system except for the citadel are also available as tertiary barriers to these sources. Hence, for the radionuclide sources within the reactor, there are four passive barriers to radionuclide transport and for all other fuel sources, there are three barriers as part of the **Plant Capability Defense-in-Depth**. These barriers are concentric to eliminate bypass pathways and are designed to operate independently consistent with the principles of defense-in-depth.

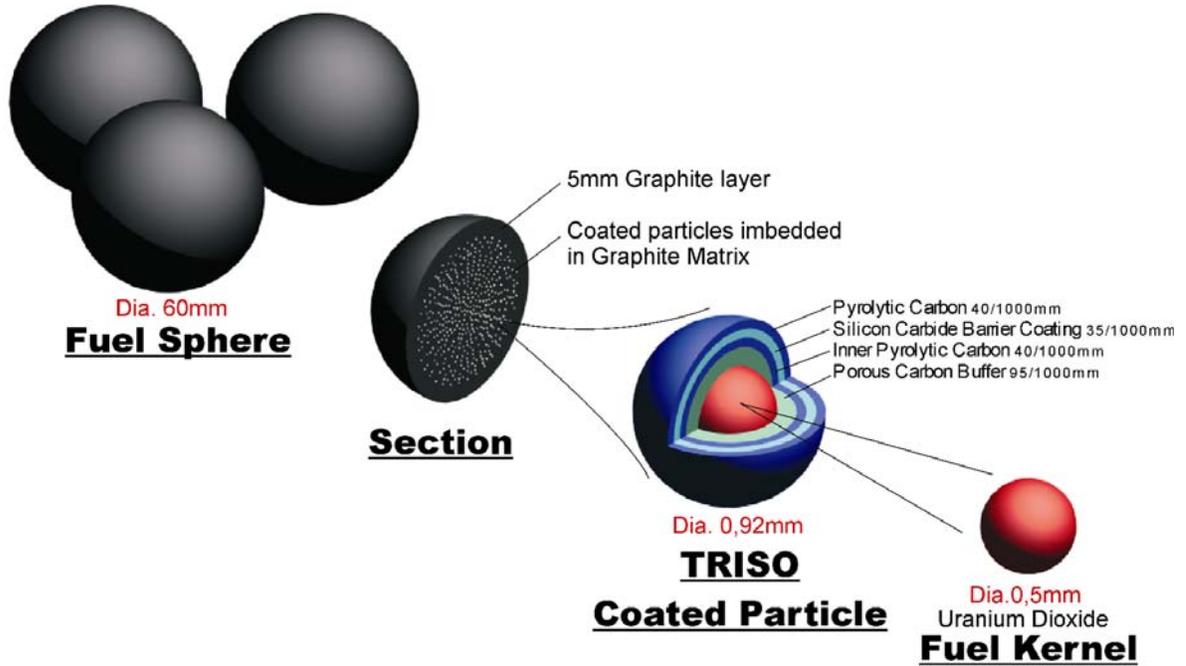


Figure 9: PBMR's Primary Barrier to Radionuclide Transport

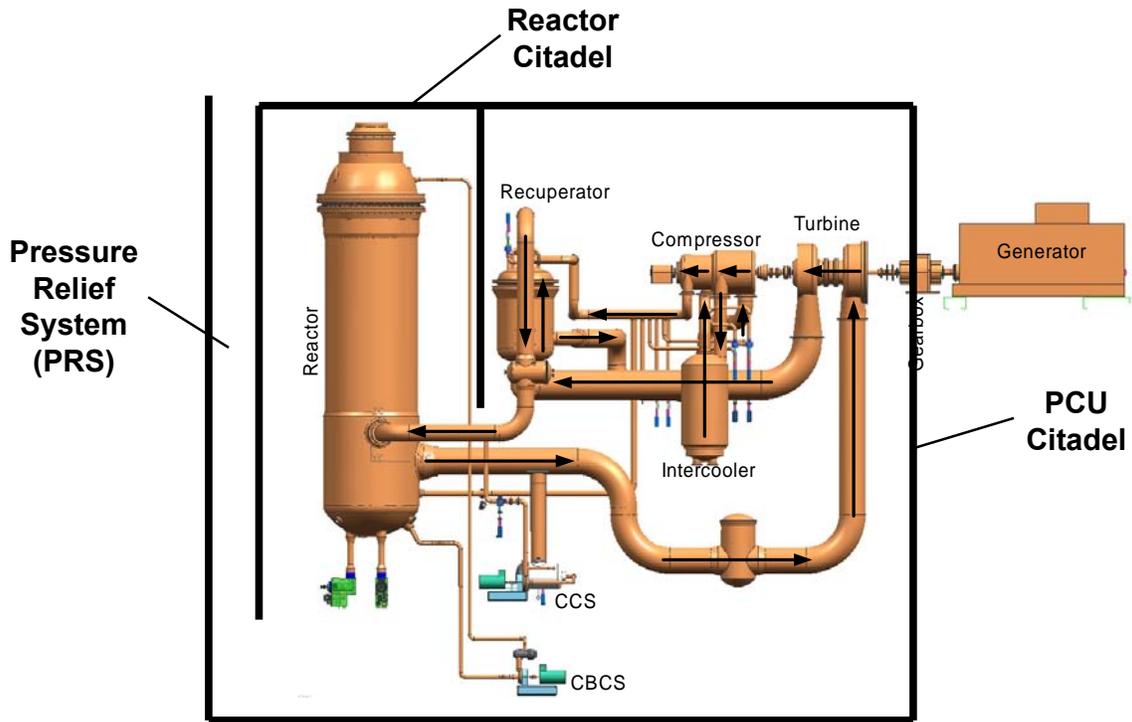


Figure 10: Major Components of the Main Power System, Helium Pressure Boundary, and Containment System

3.2.1.2 PBMR Safety Functions

The PBMR 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 11. 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 Design Basis Events. 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

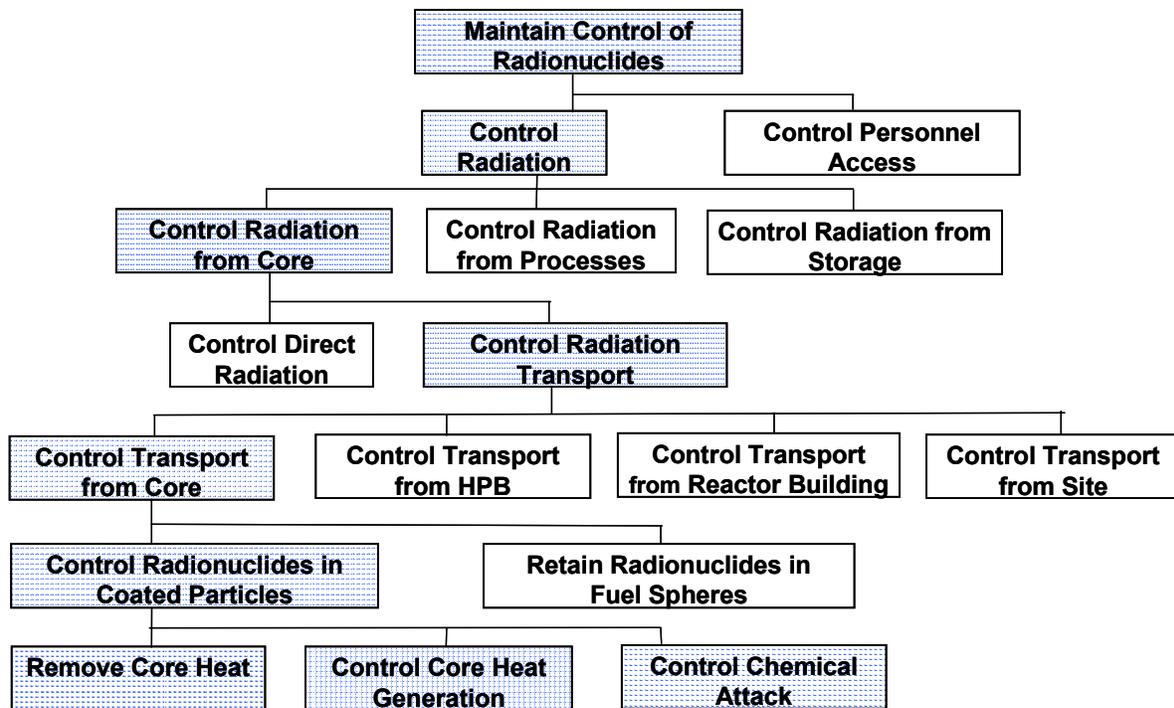


Figure 11: PBMR Safety Functions

3.2.1.3 Selection of PBMR Inherent Features

The PBMR design is based on meeting the following objectives that specifically incorporate the PBMR 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 characteristics of the PBMR the following are viewed as especially important in providing this component of the PBMR 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 thermal 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 neutronicallly inert
 - Low stored thermal energy

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

3.2.1.4 PBMR Design Features Supporting Required Safety Functions

As noted above, the PBMR safety design approach is to provide inherent characteristics and passive SSCs that are sufficient to protect the public and to meet the Top Level Regulatory Criteria and to 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 that are available to support each required safety function, as well as the additional active SSCs that support these functions, is provided in Table 9.

Table 9: PBMR Design Features and SSCs Providing *Plant Capability Defense-in-Depth*

Safety Function	Inherent Features and Passive SSCs	Active SSCs ⁴
Control of Radionuclides	<ul style="list-style-type: none"> ✚ Fuel barrier <ul style="list-style-type: none"> - Coated particle barrier - Graphite matrix - Graphite reflectors and other reactor internal surfaces ✚ Helium Pressure Boundary (HPB) barrier ✚ Reactor building barrier <ul style="list-style-type: none"> - Citadel - Confinement functions of reactor building - Reactor building Pressure Relief System (PRS) blow-out panels 	<ul style="list-style-type: none"> ✚ PRS dampers ✚ Reactor building Heating, Ventilation and Air-Conditioning (HVAC) filtration system
Control of Heat Generation	<ul style="list-style-type: none"> ✚ Strong negative temperature coefficient of reactivity ✚ Reduced excess reactivity due to online refuelling ✚ Gravity fall of control rods and Small Absorber Spheres (SAS) 	<ul style="list-style-type: none"> ✚ Control and protection systems <ul style="list-style-type: none"> - Operational Control System (OCS) - Equipment Protection System (EPS) - Reactor Protection System (RPS) ✚ Reactivity control systems <ul style="list-style-type: none"> - Reactivity Control System (RCS) trip release of control rod drives - Reserve Shutdown System (RSS) release of SAS

⁴ 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.

Safety Function	Inherent Features and Passive SSCs	Active SSCs ⁴
Control of Heat Removal	<ul style="list-style-type: none"> ✚ 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) <ul style="list-style-type: none"> - RCCS Tank inventory - Demineralized Water System (DWS) or Fire Protection System (FPS) makeup to RCCS tanks (two places) - RCCS Tank inventory + External tank truck makeup to RCCS tanks (two places) - RCCS dry ✚ PRS blow-out panels 	<ul style="list-style-type: none"> ✚ Active Reactor Cavity Cooling System (RCCS) <ul style="list-style-type: none"> - Equipment Protection Cooling Circuit (EPCC) → Main Heat Sink System (MHSS) - EPCC → Cooling Tower ✚ Power Conversion Unit (PCU) <ul style="list-style-type: none"> - Brayton Cycle → Active Cooling System (ACS) → MHSS - Motored Turbine Generator (TG) → ACS → MHSS ✚ Core Conditioning System (CCS) <ul style="list-style-type: none"> - EPCC → MHSS - EPCC → Cooling Tower ✚ Core Barrel Conditioning System (CBCS) <ul style="list-style-type: none"> - EPCC → MHSS - EPCC → Cooling Tower
Control of Chemical Attack	<ul style="list-style-type: none"> ✚ HPB high reliability piping and pressure vessels ✚ HPB design minimize penetrations in top of reactor vessel ✚ High purity specifications for inert helium coolant ✚ All interfacing systems at lower pressure than Main Power System (MPS) ✚ Lack of HPB pressurization mechanisms to open PRS valves ✚ ACS rupture discs protect against MPS Heat Exchanger (HX) leaks ✚ PRS relief blow-out panels 	<ul style="list-style-type: none"> ✚ PRS exhaust duct dampers and redundant closure mechanisms limit air ingress ✚ Isolation valves in MPS interfacing systems ✚ Helium Purification System (HPS) maintains high purity levels of Helium coolant
Maintain Core and Reactor Vessel Geometry	<ul style="list-style-type: none"> ✚ Reactor core and structures ✚ Reactor pressure vessel and structures ✚ Reactor cavity citadel ✚ Reactor building structure 	<ul style="list-style-type: none"> ✚ Active RCCS maintains acceptable reactor vessel support temperatures

In summary, there are inherent and passive design features available to support each of the PBMR 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 PBMR. In addition there are redundant and diverse active systems available to support PBMR safety functions and to prevent the challenges to the inherent and passive design features. As shown in Table 9, satisfaction of these safety functions is not dependent on a single element of the design but rather is provided through abundant and diverse means. The application of defense-in-depth principles in the PBMR safety design approach has produced the following characteristics that comprise strong points of the safety case:

- The PBMR has at least 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 TRISO coated particles within the spherical graphite fuel spheres. 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 containment system provides additional independent and concentric passive barriers including the citadel, vented reactor building confinement function, and PRS blowout panels as well as active and passive SSCs to minimize air ingress and provide filtration 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 in normal and accident conditions.
- The performance of PBMR 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 due to the on-line refuelling capability for the PBMR.
- There is passive reactor shutdown capability due to a negative temperature coefficient under any transient involving under-cooling conditions.
- The PBMR has two independent and diverse systems for reactivity control in addition to passive control via negative temperature coefficient of reactivity
- The PBMR has three independent and diverse systems for core heat removal, one of which operates using passive design principles.

3.2.2 PBMR Implementation of *Programmatic Defense-in-Depth*

The PBMR approach to *Programmatic Defense-in-Depth* includes the application of conservative safety margins and deterministic elements in the definition of the Top Level Regulatory Criteria (TLRC), 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 involve the application of conservative assumptions and are responsible for safety margins are considered part of the PBMR approach to programmatic defense-in-depth.

Selection of the TLRC

The frequency-dose criteria embodied in the TLRC are set with significant margins against the NRC safety goal Quantitative Health Objectives (QHOs). Adherence to the TLRC assures that the QHOs for the individual risk of latent cancer fatality are met by several orders of magnitude, [17]. When the PBMR LBE frequencies and consequences and associated uncertainties are compared against the TLRC, there are additional margins before the TLRC are reached. The PBMR has also imposed its own user requirement that the consequences of the LBEs are to be met at the site boundary, e.g. not require credit for emergency planning beyond the site boundary to meet the frequency vs. dose thresholds embodied in the TLRC. Hence, a significant part of *Programmatic Defense-in-Depth* is simply demonstrating that the TLRC are met.

Definition of Licensing Basis Events

In general, the sequences in the PRA lay out sets of event sequences which are organized into event sequence families for the definition of Licensing Basis Events (LBEs) as explained more fully in the companion paper on LBE selection. 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. When the frequencies and consequences and associated uncertainties for each LBE is compared against the TLRC, the classification of each LBE as an Anticipated Operational Occurrence (AOO), Design Basis Event (DBE), or Beyond Design Basis Event (BDBE) conservatively accounts for the uncertainties. If the 95%tile frequency of the LBE is above the breakpoint for separating the AOOs from the DBEs, or that for separating the DBEs from the BDBEs, the LBE is assigned to the higher frequency category where more stringent dose criteria are applied. The 95%percentile from the consequence uncertainty distribution is required to be within the associated TLRC frequency vs. dose curve.

The PRA that is performed to provide a basis for selecting the LBEs will address uncertainties in both the event sequence frequencies and the radiological consequences, including the uncertainties in the mechanistic source term. A goal is to quantify the impacts of uncertainties consistent with the current state of the art of PRA technology and to address additional sources of uncertainty identified in the performance of the PRA and in peer reviews of the PRA using sensitivity studies. The evaluation of uncertainties is expected to result in the formulation of deterministic regulatory design criteria that are applied as part of the *Programmatic Defense-in-Depth*.

Selection of Safety Related SSCs

An important element of ***Programmatic Defense-in-Depth*** is applied in the safety classification of SSCs. As explained more fully in the companion paper on SSC Safety Classification, SSCs are classified based on criteria that are 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. This approach adds an element of defense-in-depth that goes beyond that of the traditional approach to safety classification. The PBMR 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. The use of the PRA to quantify the frequencies of event sequences and to identify the sources of uncertainty in these quantifications are viewed as an advancement over the approach of using qualitative judgments as to which events are deemed credible. Importantly, all risk significant events as well as the deterministically analyzed design basis events are considered in this safety classification process. Hence, the risk-informed process of selecting safety related SSCs is expected to augment the defense-in-depth for the PBMR 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.

Deterministic Design Basis Event Requirements

There is additional conservatism introduced by the requirement to demonstrate that each Deterministic Design Basis Event can be sufficiently mitigated with only the safety classified SSCs being 'credited' for event mitigation. This is explained more fully in the companion paper on LBE selection. 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, as explained more fully below.

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 safety classified SSCs. The PBMR will apply ***Programmatic Defense-in-Depth*** in the same manner in order to ensure that the safety related SSCs have adequate reliability and capability to perform their safety functions. While specific special treatment requirements for the PBMR 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 SSC will perform their functions with an appropriate level of reliability and capability. Additionally, as explained in the paper on SSC Classification, 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.

3.2.3 PBMR Implementation of *Risk-Informed Evaluation of Defense-in-Depth*

The PBMR DCA will use the logic diagram shown in Figure 5 and the defense-in-depth criteria in Table 5 to document the *Risk-Informed Evaluation of Defense-in-Depth* and to justify that the plant capabilities and programs described in the DCA provide an adequate application of defense-in-depth principles for the PBMR. A cross reference table will be provided to show where in the DCA the NRC will find objective evidence that each of the defense-in-depth criteria in Table 5 have been adequately addressed.

The PBMR DCA will include an evaluation of the SSCs responsible for prevention and mitigation of accidents using the methodology outlined in Section 3.1.4.4. This will consist of the following steps.

1. The documentation of the process for safety classification of SSCs will identify all the inherent characteristics, passive SSCs and active SSCs that are available to support each safety function for each Design Basis Event (DBE). This is part of the redundancy and diversity of barriers and SSCs that included in the PBMR safety design approach.
2. Information from the PBMR PRA will be used to develop estimates of each parameter in Equation (1) for each of the PBMR LBEs
3. Information from the PRA will be used to attribute each term in Equation (1) to specific PBMR barriers, design features and SSCs responsible for the prevention of accidents and for the mitigation of the offsite radiological consequences.
4. The above information will be plotted in graphs such as those in Figure 7 and Figure 8 in order to examine the roles of specific SSCs in the prevention and mitigation of accidents.
5. The uncertainties in the estimation of the frequencies and consequences of all the LBEs and all parameters in Equation (1) will be reviewed including those that are accounted for in the uncertainty quantification as well as those epistemic uncertainties that are identified in the PRA and the PRA peer review. Insights from this review are expected to be useful in the formulation of regulatory design criteria for the PBMR DCA and COL.
6. The above results will be used to demonstrate that defense-in-depth criteria of Table 5 have been met. This includes an evaluation of the roles of barrier and SSC independence, redundancy, and diversity in ensuring that the capability to meet the top level regulatory for accident frequency and dose are not unduly dependent on a single element of the design.

3.3 PBMR APPROACH TO APPLYING DEFENSE-IN-DEPTH PRINCIPLES

In Section 2 of this paper, the regulatory foundation for defense-in-depth was reviewed. Among the various regulations and guidance documents that were reviewed, the defense-in-depth objectives in Chapter 19 of the Standard Review Plan [11] and the design attributes for advanced reactors from the NRC Policy on Advanced Reactor Regulation were selected as the basis for defense-in-depth criteria to be used for the PBMR DCA as documented in Section 3 and Table 5. These criteria will be used in the ***Risk-Informed Evaluation of Defense-in-Depth*** as illustrated in Figure 5 to demonstrate that the PBMR approach to defense-in-depth is adequate for the DCA. As shown in Table 10, the PBMR DCA will include sufficient information to judge the sufficiency of its approach to defense-in-depth in accordance with these criteria.

Table 10: PBMR Approach to Addressing Defense-in-Depth Principles of Table 5

Defense-in-Depth Principles	PBMR Approach
1. Plant Capability Defense-in-Depth Principles	
<p>✚ The safety design approach shall provide multiple, robust barriers to radioactive material release.</p>	<p>The PBMR includes multiple robust barriers to radioactive material release. The DCA 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 that is submitted to support the DCA.</p>
<p>✚ 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. These Strategies include:</p> <ul style="list-style-type: none"> - use of active SSCs that work in concert with the 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. - use of appropriate combinations of inherent reactor characteristics, passive SSCs, and active SSCs in the performance of safety functions - use of redundant, diverse, and independent means of fulfilling each safety function - use of adequate safety margins and conservative design approaches to address uncertainties in barrier and SSC performance - use of strategies to identify and defend against significant human errors and common cause failures that could challenge barriers to significant radioactive material release - use of 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. 	<p>The PBMR safety design approach is consistent with these criteria. Objective evidence will be included in the DCA to demonstrate that each criterion is met.</p>

Defense-in-Depth Principles	PBMR Approach
2. Programmatic Defense-in-Depth Principles	
<p>✚ 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:</p>	<p>The specific elements of programmatic defense-in-depth to be applied to the PBMR will be documented in the DCA.</p>
<ul style="list-style-type: none"> - avoid over-reliance on programmatic approaches to compensate for design weaknesses 	<p>Sufficient information will be provided in the DCA to demonstrate there are no weaknesses in the design that rely on programmatic approaches to compensate.</p>
<ul style="list-style-type: none"> - address significant uncertainties identified in the performance and review of the PRA 	<p>The PRA will include a comprehensive treatment of uncertainties. These as well as any additional uncertainties that may arise from PRA reviews will be addressed with appropriate programmatic requirements.</p>
<ul style="list-style-type: none"> - be sufficient to provide confidence that SSCs will have sufficient reliabilities and capabilities to perform safety functions for the licensing basis events 	<p>The safety classification approach and special treatment requirements to applied to SSCs will be described in the DCA. Sufficient information will be provided to enable NRC to judge the sufficiency.</p>
3. Risk-Informed Evaluation of Defense-in-Depth Principles	
<p>✚ 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:</p>	
<ul style="list-style-type: none"> - barrier and SSC reliability and independence are sufficient commensurate with the expected frequency of the challenge and the consequences of failure 	<p>The design information to be presented in the DCA 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.</p> <p>The systematic search for initiating events in the PBMR PRA will identify credible barrier failure modes including HPB failure modes and challenges to the fuel barrier, HPB, and reactor building 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 as described in Section 3.1.4.4 will reveal any significant dependencies and provide a framework for the NRC to review to determine sufficient independence.</p>

Defense-in-Depth Principles	PBMR Approach
<ul style="list-style-type: none"> - there is a reasonable balance between the prevention and mitigation of accidents involving release of significant quantities of radioactive material 	<p>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 as described in Section 3.1.4.4 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.</p>
<ul style="list-style-type: none"> - 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. 	<p>This will be demonstrated in the presentation of the PRA results.</p>
<ul style="list-style-type: none"> - 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 	<p>The PRA will include a comprehensive treatment of human errors and common cause failures that contribute to the frequency of each modelled event sequence and LBE. The contributions of human errors and common cause failures to LBE frequencies will be clearly documented.</p>
<ul style="list-style-type: none"> - deterministic requirements are met 	<p>The DCA will include objective evidence that this principle is met.</p>

3.4 SUMMARY OF DEFENSE-IN-DEPTH INSIGHTS FOR THE PBMR

In summary, the PBMR approach to defining and implementing the defense-in-depth safety philosophy has been described in this section. PBMR 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 PBMR

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.
- PBMR has embraced defense-in-depth in the formulation of the safety design approach it expects to follow for certification of the PBMR design.
- The PBMR 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 design certification of the PBMR.
- The definition of **Plant Capability Defense-in-Depth** proposed by PBMR 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, independent and concentric radionuclide barriers, and passive as well as active SSCs to protect the integrity of the barriers.
- The PBMR has at least three concentric and independent radionuclide barriers⁵.
 - The primary barrier to radionuclide transport for all the sources associated with the reactor, spent, used and new fuel is the TRISO coated particles within the spherical graphite fuel spheres. 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 PBMR design provides concentric passive barriers including the citadel, reactor building structure, and the PRS blow-out panels as well as active and passive SSCs to minimize air ingress and provide filtration of airborne radionuclides.

⁵ All fuel sources have the coated particle fuel elements, a helium pressure boundary, and the reactor building confinement to make 3 concentric barriers. The fuel inside the reactor vessel also has the citadel within the reactor building as a fourth concentric barrier. For the fuel inside the reactor vessel, the helium pressure boundary includes the reactor vessel and the vessels and piping that comprise the Main Power System, Helium Purification System, and Fuel Handling and Storage System (FHSS) helium pressure boundary. For the fuel in the spent and used fuel tanks, the tanks and piping within the fuel storage parts of FHSS comprise the helium pressure boundary. All fuel sources and their respective helium pressure boundaries are contained within the reactor building structure.

- The inherent and passive design features of the PBMR 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 through the use of a full scope PRA. The roles of the secondary (HPB) and tertiary (containment system) barriers are not to compensate for conditions in which failure of the fuel barrier is expected, but rather to help ensure that fuel integrity is not compromised.
- The PBMR has also included 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 PBMR DCA 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 PBMR.
- The components of **Programmatic Defense-in-Depth** will be applied during design certification 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 PBMR DCA.

4. ISSUES FOR PREAPPLICATION RESOLUTION

The issues addressed in this paper are framed in terms of the following questions about the PBMR approach to defense-in-depth that will be implemented in support of the PBMR DCA. The PBMR position on the appropriate response to these questions is discussed in detail in Chapter 3 and summarized following the listing of each question.

1. What is an appropriate definition of defense-in-depth for the PBMR?

PBMR Response:

Defense-in-depth is a well established safety philosophy in which multiple lines of defense are applied to the design, construction, and operation of nuclear plants to provide greater assurance that the public health and safety are adequately protected. Many different definitions of defense-in-depth have been published by the NRC and international regulatory authorities in regulations, regulatory guides, commission papers, and ACRS reports. Each of these definitions brings out a different facet of this important safety philosophy. A representative set of definitions selected to capture a reasonably complete set of the underlying principles of defense-in-depth was reviewed in Section 2. The various defense-in-depth principles and strategies referred to in these definitions are viewed as being applicable to, and have been applied to the PBMR. Some defense-in-depth strategies, such as the balancing of prevention and mitigation of core damage, have to be generalized somewhat before application to the PBMR. The defense-in-depth principles for the PBMR are identified in Table 5 of this paper.

2. How should defense-in-depth be defined so that the PBMR approach to employing defense-in-depth strategies to design, construct, and operate the plant can be objectively evaluated?

PBMR Response:

PBMR recognizes three major elements in its approach to defense-in-depth: **Plant Capability Defense-in-Depth**, **Programmatic Defense-in-Depth**, and **Risk-Informed Evaluation of Defense-in-Depth**.

Plant Capability Defense-in-Depth refers to the use of multiple lines of defense in the design of structures, systems, and components (SSCs) in a nuclear power plant that provide multiple and physical lines of defense between the hazard and the public. The hazard is an inventory of radioactive material and its potential for release to the environment in a manner that could harm the health or safety of the public. These physical lines of defense include multiple radionuclide transport barriers and inherent characteristics and engineered features whose safety functions preserve the integrity of these barriers. The transport barriers include physical barriers and associated safety systems that prevent or block the movement of radionuclides, as well as time delays in the transport that allow for the radioactive decay and deposition of radionuclides prior to their release, time for implementation of emergency protective actions, and siting considerations. For the PBMR the strategies to employ **Plant Capability Defense-in-Depth** begin with the use of conservative design conditions that exploit the inherent and passive safety features that anchor the safety case. The **Plant Capability Defense-in-Depth** strategies also include the application of redundancy, diversity and independence to achieve the necessary reliability and capability of the barriers and the SSCs that perform the safety functions. Conservative design approaches to ensure the reliability and capability of each SSC that performs a safety function are also part of the process of providing **Plant Capability Defense-in-Depth**.

Programmatic Defense-in-Depth refers to the use of multiple lines of defense in the processes and programs that are put into place to ensure that SSCs responsible for performing safety functions maintain adequate margin, reliability and capability, and to provide a means to address uncertainties in the design performance. These processes include the conservative elements of the PBMR risk-informed and performance-based licensing approach, special treatment requirements, tests and inspections, monitoring of performance, operational controls, and oversight.

Risk-Informed Evaluation of Defense-in-Depth provides a robust means to evaluate the multiple lines of defense reflected in the definition of scenarios that are analyzed in the deterministic and probabilistic safety evaluations. The structure of these scenarios assures that the strategies of **Plant Capability Defense-in-Depth** and **Programmatic Defense-in-Depth** have been adequately implemented. The strategies of accident prevention and mitigation 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 the prevention and mitigation of accidents. For the PBMR, the strategies of prevention and mitigation are defined somewhat more broadly than for currently licensed reactors that focus on the prevention and mitigation of core damage. Prevention strategies are those that are employed to reduce the frequency of accidents by improving the reliability of SSCs whose failure could cause an initiating event or prevent its successful mitigation. 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. Hence prevention and mitigation are directly correlated to the reliability and capability of the SSCs responsible for providing the **Plant Capability Defense-in-Depth**. The evaluation of prevention and mitigation effectiveness of SSCs in the probabilistic and deterministic safety analysis is the domain of **Risk-Informed Evaluation of Defense-in-Depth**.

The ultimate objective of the **Risk-Informed Evaluation of Defense-in-Depth** is to establish the adequacy and sufficiency of the plant capabilities and programs that are responsible for the defense-in-depth. For this purpose, the PBMR approach to completing this element includes a set of defense-in-depth principles that were derived from defense-in-depth objectives Chapter 19 of the Standard Review Plan and reactor attributes from the NRC's advanced reactor policy statement. A decision logic was derived to evaluate the plant capabilities and programs responsible for defense-in-depth in light of these criteria.

3. What are the elements of defense-in-depth for the PBMR's safety design philosophy, design approach and analyses, and the assurance programs to ensure that defense-in-depth is applied throughout the life of the plant?

PBMR Response:

As explained in Section 3, the PBMR approach to **Plant Capability Defense-in-Depth** includes multiple independent and diverse barriers to radionuclide transport including the coated particle fuel, helium pressure boundary, and reactor building and associated SSCs that comprise the PBMR Containment System. Independence of these barriers is strengthened through the inherent characteristics of the PBMR and a concentric configuration that minimizes the potential for bypass pathways. Inherent design features and passive SSCs are provided to perform the PBMR safety functions of control heat generation, control heat removal, control chemical attack and maintain barrier structural integrity which collectively assures adequate containment of radioactive material. Active engineered features are also provided to provide defense-in-depth in the performance of the safety functions and to meet user requirements for plant availability and investment protection. The reliability and capability of the barriers and SSCs providing safety functions are assured with the use of inherent and passive safety features, as well as active SSCs. The reliability and

capability of SSCs supporting safety functions are assured through appropriate application of the defense-in-depth principles of redundancy, diversity, and independence. The use of conservative assumptions in analyses performed in support of the design and the safety margins inherent in the design codes applied to the design of the SSCs also contribute the **Plant Capability Defense-in-Depth** for the PBMR in the sense that these conservatisms and margins lead to more robust SSCs. Defense-in-depth is applied during construction, commissioning, and plant operation by application of appropriate tests, inspections, maintenance, and monitoring of plant and SSC performance as part of **Programmatic Defense-in-Depth**.

4. How is the defense-in-depth philosophy reflected in the risk-informed licensing approach that is proposed for the PBMR?

PBMR Response:

PBMR has applied the strategies of **Programmatic Defense-in-Depth** that are reflected in the application of conservative safety margins and deterministic elements in each step of the PBMR risk-informed and performance-based licensing approach including the definition of the Top Level Regulatory Criteria (TLRC), selection of LBEs, safety classification of SSCs, and formulation of special treatment requirements. The TLRC have been selected so that meeting these criteria will ensure that NRC Safety Goal Quantitative Health Objectives are met by several orders of magnitude. Licensing Basis Event selection will be supported by a comprehensive all modes and all hazards PRA and will include a full treatment of dependent and common cause failures in setting the design basis envelope. Classification of safety related SSCs will be made in light of a rigorous requirement that all risk significant licensing basis events must be adequately addressed through both prevention and mitigation.

Deterministic Design Basis events will be selected and analyzed using conservative assumptions that will demonstrate the adequacy of defense-in-depth in the selection of LBEs, the safety classification of SSCs, and the application of special treatment requirements to assure that the safety classified SSC have adequate reliability and capability.

The PRA will include a detailed treatment of uncertainties including an identification of the sources of uncertainty, a quantification of the impact of uncertainties on the event sequence frequencies, mechanistic source terms and off-site doses, and sensitivity analyses to investigate the impact of modelling uncertainties and assumptions. The results of this uncertainty analysis will be factored into the selection of LBEs, safety classification of SSCs, the formulation of special treatment requirements, and other engineering assurance programs that comprise **Programmatic Defense-in-Depth**. More details on these points are found in the companion papers on PRA, LBE Selection, and Safety Classification of SSCs.

An important element of this approach 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. Those proposed programs that cannot be attributed to reducing uncertainties and enhancing the plant capabilities with respect to the TLRC will be deemed of no significant added value and will not be implemented. It is important that such programs be held accountable to their effectiveness as risk management tools.

5. How is the defense-in-depth strategies of accident prevention and mitigation defined and evaluated for the PBMR?

PBMR Response:

For the PBMR, the strategies of prevention and mitigation are defined somewhat more broadly than for currently licensed reactors with focus on the prevention and mitigation of core damage. Prevention strategies are those that are employed to reduce the frequency of accidents by improving the reliability of SSCs that contribute to initiating events and SSC failures along the event sequences. 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. Hence prevention and mitigation are directly correlated to the reliability and capability of the SSCs responsible for providing **Plant Capability Defense-in-Depth**. The evaluation of prevention and mitigation effectiveness of SSCs in the probabilistic and deterministic safety analysis is the domain of **Risk-Informed Evaluation of Defense-in-Depth**.

PBMR has provided a definition of prevention and mitigation so that the roles of SSCs in the prevention and mitigation of accidents can be clearly discussed and evaluated. The reliability and capability of SSCs that preclude accidents and reduce their frequency of occurrence and probability of failure are responsible for preventing accidents. The reliability and capability of SSCs that perform safety functions in response to an initiating event or accident sequence that challenges the SSC serve to mitigate the consequences or impact of the challenge. A given SSC may serve both prevention and mitigation roles on different event sequences.

PBMR has developed an approach that provides the capability of quantifying the degree that accidents are prevented and consequences are mitigated and which SSCs are responsible based on information from the PRA. The approach organizes information from the PRA on the capability of SSCs to prevent and mitigate event sequences to support this evaluation. This approach quantifies the impact of SSCs roles in the prevention and mitigation of accidents based on a risk model. Information provided by this approach can be used to examine the relative impacts of specific prevention and inspection strategies.

The structured process described is used to identify and evaluate the roles of SSCs in the prevention and mitigation of all licensing basis events. This process includes an examination of the degree of protection against human errors and a demonstration that the PBMR does not over rely on programmatic means to compensate for design inadequacies. This process will address uncertainties and identify the need for any deterministic defense-in-depth requirements.

6. 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 PBMR DCA?

PBMR Response:

The DCA will include sufficient information on the PBMR approach to defense-in-depth to support the design certification. This information will include:

- a. An appropriate definition for defense-in-depth.
- b. The roles of each barrier to fission product release in providing defense-in-depth.
- c. The roles of inherent and passive design features and SSCs that are used as well as active engineered systems to provide defense-in-depth.
- d. How the reliability, capability, and independence of each barrier are defined and evaluated in terms of their defense-in-depth role.

- e. How the safety functions are defined and how they support the integrity of each barrier in providing 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 defense-in-depth.
- g. How the principles of design margins, redundancy, diversity, and independence been applied in providing defense-in-depth.
- h. An appropriate definition of prevention and mitigation and a means to evaluate the impact of these strategies on maintaining acceptable risk levels.
- i. The roles and effectiveness of specific barriers and SSCs in the prevention and mitigation of accidents.
- j. What is the role of design safety margins reflected in the applied codes and standards in providing a robust design with defense-in-depth.
- k. How defense-in-depth is applied to address uncertainties.
- l. Principles that should be used in determining the adequacy and sufficiency of defense-in-depth for a DCA.

As a result of providing the above information, the NRC should have adequate information to evaluate the PBMR approach to defense-in-depth for the DCA.

5. PREAPPLICATION OUTCOME OBJECTIVES

The objective of this paper and the follow-up workshops and paper revisions that are planned is to get NRC agreement on the list of issues for the treatment of defense-in-depth to support PBMR design certification. Specifically, we appreciate it if the NRC would agree with the following statements, or provide an alternative set of statements with which they agree.

1. The definition of defense-in-depth presented in Section 3 of this paper, which recognizes three elements of the defense-in-depth approach: ***Plant Capability Defense-in-Depth***, ***Programmatic Defense-in-Depth***, and ***Risk-Informed Evaluation of Defense-in-Depth***, is appropriate for the PBMR DCA.
2. The PBMR approach to ***Plant Capability Defense-in-Depth***, which includes multiple independent and diverse barriers to radionuclide transport, the use of inherent characteristics and passive and active SSCs to perform the required safety functions, and conservative design strategies as described in this paper, is appropriate for the DCA.
3. The PBMR approach to ***Programmatic Defense-in-Depth*** 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 support defense-in-depth will have sufficient reliability and will be maintained throughout the lifetime of the plant.
4. The PBMR approach to ***Risk-Informed Evaluation of Defense-in-Depth*** represents an acceptable approach to the definition of accident prevention and mitigation and the evaluation of the roles of design features and SSCs responsible for prevention and mitigation, and a logical process to establish the adequacy and sufficiency of defense-in-depth for the PBMR.
5. Sufficient information on the PBMR approach to defense-in-depth required to support certification of the PBMR design will be included in the DCA. This information will include:
 - a. An appropriate definition for defense-in-depth.
 - b. The roles of each barrier to fission product release in providing defense-in-depth.
 - c. The roles of inherent and passive design features and SSCs that are used as well as active engineered systems to provide defense-in-depth.
 - d. How the reliability, capability, and independence of each barrier are defined and evaluated in terms of their defense-in-depth role.
 - e. How the safety functions are defined and how they support the integrity of each barrier in providing 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 defense-in-depth.
 - g. How the principles of design margins, redundancy, diversity, and independence been applied in providing defense-in-depth.
 - h. An appropriate definition of prevention and mitigation and a means to evaluate the impact of these strategies on maintaining acceptable risk levels.
 - i. The roles and effectiveness of specific barriers and SSCs in the prevention and mitigation of accidents.
 - j. What is the role of design safety margins reflected in the applied codes and standards in providing a robust design with defense-in-depth.
 - k. How defense-in-depth is applied to address uncertainties.

- I. Principles that should be used in determining the adequacy and sufficiency of defense-in-depth.

It is requested that the NRC take the following steps:

- Step 1 NRC review the paper for agreement on the list of issues and the PBMR approach to defense-in-depth proposed in this paper.
- Step 2 The holding of a workshop on the issues identified in the paper and a discussion of the approach that is proposed for resolution.
- Step 3 NRC issuance of preliminary comments and requests for additional information to clarify points not understood or adequately developed in the paper.
- Step 4 PBMR preparation of a revised paper which identifies any Request for Additional Information (RAI) that can be addressed in the near term as well as requested information that will be included with the DCA submittal on the PBMR approach to defense-in-depth. This will include a plan for preapplication activities that are agreed upon in the workshops as being necessary for a successful DCA review.
- Step 5 NRC issuance of an evaluation report on its findings related to the treatment of defense-in-depth with inputs to the DCA format and content guide that PBMR will use for the DCA.

6. APPENDICES

6.1 APPENDIX A: USE OF PRA TO EVALUATE ROLE OF SSCS IN ACCIDENT PREVENTION AND MITIGATION

6.1.1 Use of PRA in *Risk-Informed Evaluation of Defense-in-Depth*

Section 3.1.4.4 discusses the use of the PRA to evaluate the roles of SSCs in accident prevention and mitigation. The purpose of this appendix is to provide additional information and examples to show how this application of the PRA will be performed.

As discussed in Section 3.1.4.4, an accident sequence can be described in terms of the following elements for any reactor concept:

1. **Initiating Event** An initiating event that constitutes a challenge to the plant systems and structures responsible for control of transients and protection of the plant SSCs including the radionuclide transport barriers.
2. **Active SSC Response** The response (successes and failures) of active systems that support key safety functions responsible for protection of barriers, retention of radioactive material, and protection of the public health and safety, as defined by the accident sequence.
3. **Passive SSC Response** The response of passive design features responsible for supporting key safety functions, including the structures that form the radionuclide barriers themselves and the passive systems that support them.
4. **Barrier Retention Factors** The response of each barrier to radionuclide transport from the radioactivity sources to the environment to the initiating events and safety system responses. This response is expressed as the degree of retention of radioactive material for each barrier expected for the sequence; these barriers include the fuel elements, the coolant pressure boundary, and the reactor building barrier. Depending on the reactor design, the reactor building barrier may be described as a leak tight or vented containment, confinement, reactor building or containment system barrier.
5. **Emergency Plan Response** The implementation of emergency plan protective actions to mitigate the radiological consequences of a given release from the plant.

A generalized model for describing an accident sequence in terms of the design features that support prevention and mitigation reflecting the above insights was provided in Table 7. This table provides an important feedback mechanism between *Risk-Informed Evaluation of Defense-in-Depth* and *Plant Capability Defense-in-Depth*. The event sequence framework is part of the *Risk-Informed Evaluation of Defense-in-Depth* and the roles of SSCs in the prevention and mitigation of accidents are the result of *the Plant Capability Defense-in-Depth*. The reliabilities and capabilities of the SSCs that prevent and mitigate events are influenced by both the *Plant Capability* and *Programmatic Defense-in-Depth* elements.

The accident sequence framework for evaluating accident prevention and mitigation in Table 7 can be used to define a simple model for estimating the risk of a release of radionuclides associated with a specific accident sequence. This model is defined in Section 3.1.4.4 by Equation (1).

In the following sections this approach of defining and evaluating design features that support prevention and mitigation strategies is applied to sets of sequences for two different

reactor types, current generation (Generation II) PWR and the MHTGR. These examples were selected for several reasons:

1. The examples include one existing LWR concept which reflects the traditional approaches to defense-in-depth and one advanced reactor concept that has inherent characteristics fundamentally different than those of the existing LWRs;
2. The former example uses a conventional leak tight containment concept for the reactor building barrier whereas the latter uses a non-leak tight confinement building concept;
3. The PWR design uses conventional active safety systems to perform critical safety functions such as decay heat removal, whereas the MHTGR uses a combination of active and passive safety systems including a decay heat removal capability that is independent of any active components; and
4. Each has publicly available and peer reviewed PRAs to provide the necessary information including a quantification of uncertainties, from which mean values of the parameters in Equation (1) can be obtained.

These examples are used to demonstrate the capability of this approach to define and evaluate the roles of SSCs and barriers in the prevention and mitigation of accidents. The ultimate goal is to develop a better understanding of the ways in which each reactor has implemented defense-in-depth concepts to prevent and mitigate selected accident sequences that are representative of the respective PRA results.

6.1.2 Evaluation of Selected PWR Event Sequences

To demonstrate the concept used in this paper for evaluating prevention and mitigation strategies to existing LWRs, three sequences were selected as representative sequences from some of the PWR results in NUREG-1150 [23]. These selected sequences are representative of the results of the supporting PRA and include those that dominate the risk of I-131 releases. These sequences are briefly described as follows:

- **PWR-1:** This is a small LOCA initiated sequence with successful response of the ECCS and hence core damage is assumed to be prevented. As with PWR-2 the containment remains intact during this sequence. The major part of the I-131 inventory remains in the fuel during this sequence as core damage does not occur. The circulating activity in the reactor coolant is released to the containment which retains a large fraction of that in mitigating the releases to environment.
- **PWR-2:** This is a small LOCA initiated sequence with an independent failure of the ECCS in the recirculation mode which requires operator action. The ECCS failure is assumed to result in core damage, but in this sequence the containment remains intact during the sequence retaining a large fraction of the radionuclides that are released from the fuel.
- **PWR-3:** This is an interfacing systems LOCA sequence caused by failure of two check valves at the interface of the reactor coolant system and the low pressure injection system, which is assessed in the PRA to result in a loss of coolant accident bypassing the containment. There is an inability to establish emergency coolant recirculation functions as the coolant inventory is lost outside the containment. The PRA models this sequence as a core melt with a containment bypass because the release pathway is direct from the coolant pressure boundary to the environment bypassing the containment building. PWR-3 has long been recognized as a significant contributor to Large Early Release Frequency (LERF) for PWRs.

The PRA frequency and release data developed for the evaluation of these sequences was developed from NUREG-1150 for the radionuclide species I-131. A more complete

evaluation would need to consider a full set of risk significant sequences and a larger set of radionuclide species. However, for the purpose of evaluating SSCs responsible for accident prevention and mitigation, these three sequences and their I-131 releases are sufficient.

A summary of the salient data for these sequences is provided in Table 11. Each of these terms has associated with it an uncertainty distribution, from which the mean values have been selected. These uncertainties can be more than an order of magnitude, especially for the low frequencies and probabilities and the release fractions. In interpreting the results, only the logarithms of these numbers are considered significant in developing insights on the relative importance of plant features in managing risk via prevention and mitigation strategies. Absolute safety margin determinations are outside the scope of this example.

Table 11: Data Assumed for LWR Sequence Evaluation (from NUREG-1150)

Sequence	PWR-1	PWR-2	PWR-3
Initiating event	Small LOCA	Small LOCA	Interfacing systems LOCA
Active SSC response	Successful ECCS preventing core damage	Failure of ECCS in recirculation mode and core damage	Consequential failure of ECCS and core damage
Passive SSC response	Containment intact	Containment intact	Containment bypass
Initiating event frequency per yr.	$\sim 1 \times 10^{-2}$	$\sim 1 \times 10^{-2}$	$\sim 1 \times 10^{-6}$
Active SSC response probability	~ 1	8×10^{-4}	~ 1
Passive SSC response probability	~ 1	~ 1	~ 1
Fractional release of I-131 from fuel	$\sim 2 \times 10^{-6}$	~ 1	~ 1
Fractional release of I-131 from PB	~ 1	~ 1	~ 1
Fractional release of I-131 from containment	$\sim 2 \times 10^{-4}$	$\sim 2 \times 10^{-4}$	$\sim 2 \times 10^{-1}$

The sequences selected for the PWR examples are representative in that they contain examples of successful and unsuccessful SSC response to protect the fuel barrier and the containment barrier, and all three cases represented examples where the coolant pressure boundary barrier is violated at the initiating event. In PWR-1 the primary role of defense-in-depth is the mitigation effects of retaining the radionuclides in the fuel and in the containment when the fuel barrier and containment barrier are successfully protected. Sequence PWR-2 is a small LOCA with independent failure of the ECCS resulting in core damage and large releases into the containment, but the containment barrier is intact and is not bypassed in this sequence such that containment retention of this fission product is very effective. In PWR-3 the primary role of defense-in-depth is the prevention of the failure of the pressure boundary where interfacing systems LOCA can take place. This sequence which was originally identified in the Reactor Safety Study results in part from the lack of concentricity of the barriers in the PWR design. As it requires failure of two normally closed check valves in this example, its frequency is very low. However, the resulting core damage and containment bypass results in a large fraction of the I-131 inventory being released.

As shown in Figure 12, the frequencies and releases of I-131 for these three selected sequences can be plotted in a frequency consequence plot in a manner that permits the identification of different factors that contribute to accident prevention and mitigation. Also

plotted is a point corresponding to the inventory of I-131 for an assumed 300 MWt reactor (coinciding with the size of a typical modular reactor) at a frequency of one per year, which is selected to represent the upper bound on the frequency of any accident that involves the release of radioactive material. For each of the three PWR sequences, additional points are defined in which successive mitigation and prevention factors in Equation (1) that participate in the sequence are assumed to be removed in a progressive sequence to permit the characterization of importance of each prevention and mitigation strategy that participates in the sequence.

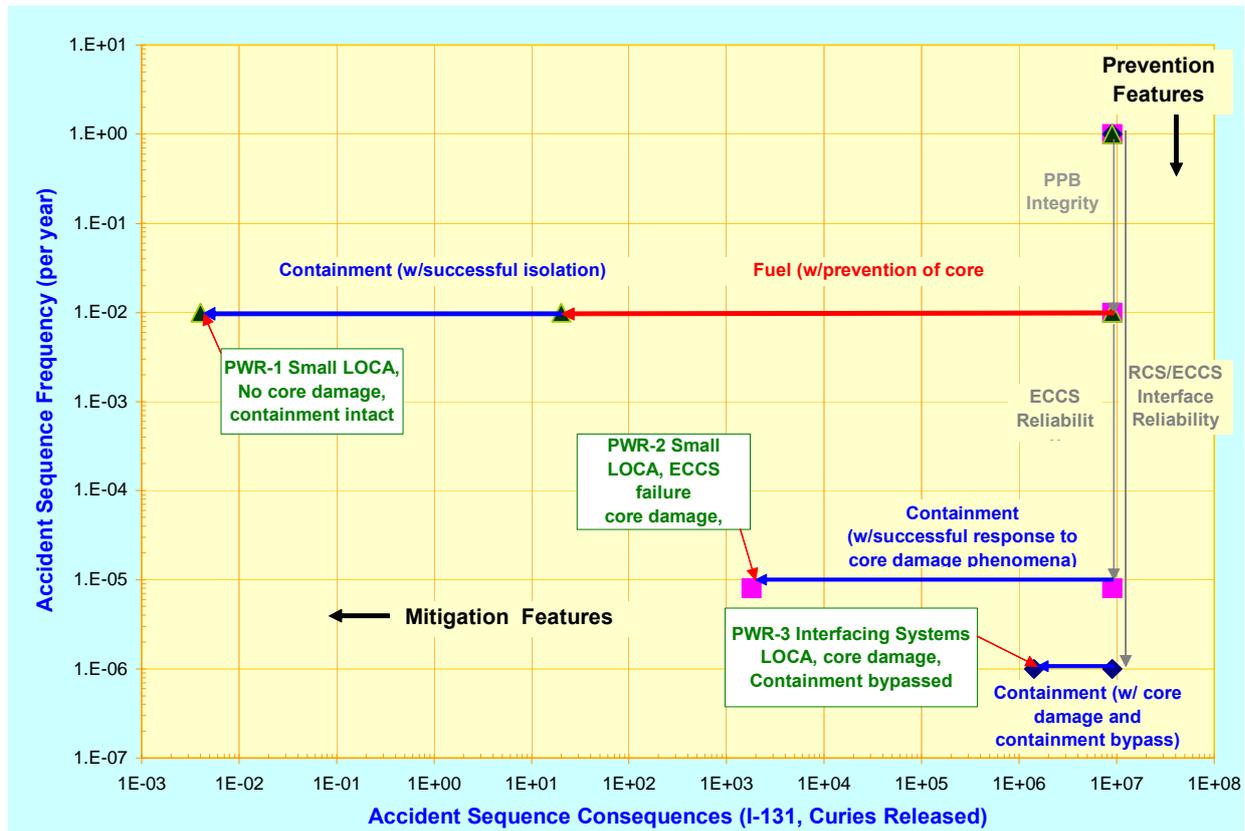


Figure 12: Design Features Contributing to Prevention and Mitigation of I-131 Releases from Selected PWR Sequences

This approach is used to estimate the quantitative contribution that each design feature makes to manage the risk of associated with an annual release of the I-131 inventory in relation to the risk of an annual release of the inventory. Information presented in this plot is used to develop the bar chart in Figure 13 which identifies the role of design features in determining the risk of an I-131 release for each sequence. The risk reduction factor quantified in Figure 13 corresponds to the order of magnitude (i.e. logarithm of the) reduction in risk computed by the risk reduction factors of Equation (1) associated with each design feature. The design features associated with prevention are those that contribute to lowering the frequency in relation to one occurrence per year. Those that contribute to mitigation are those that contribute to reducing the fraction of I-131 that is released in relation to the core inventory of I-131.

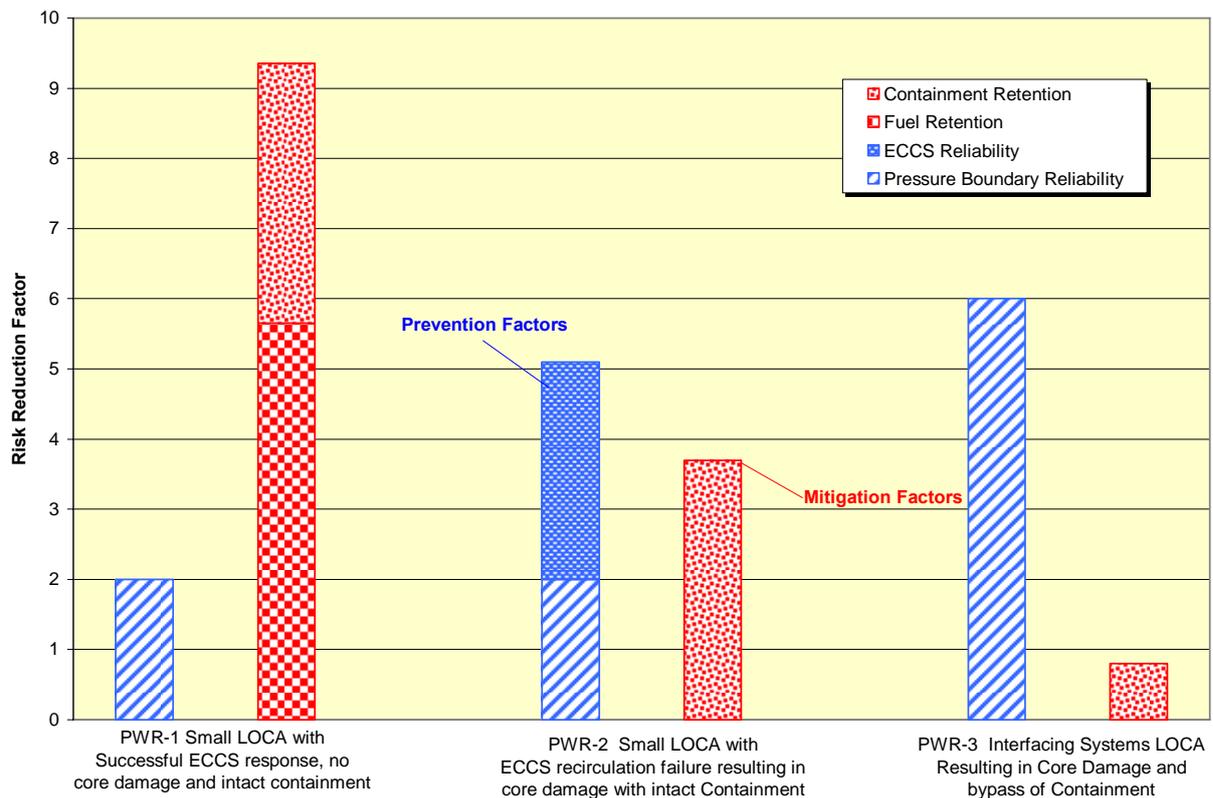


Figure 13: Risk Reduction Factors Associated with PWR Design Features Responsible for Prevention and Mitigation of I-131 Releases

As seen in Figure 13, for Sequence PWR-1 the reliability of the coolant pressure boundary as a prevention feature is responsible for a 2 order of magnitude effect in managing the risk, whereas there is a 9 order of magnitude impact of mitigation features that help limit the magnitude of the source term for this sequence. This reduction is provided by the fuel barrier (> 5 orders of magnitude) and the containment barrier (> 3 orders). For Sequence PWR-3, the interfacing pressure boundary contributes 6 orders of magnitude of prevention from the design features at the RCS/ECCS interface that reduce the likelihood of an ISLOCA, but there is only about 1 order of mitigation as there is core damage and a containment bypass condition. Only in Sequence PWR-2 is there a relative balance in the strategies of prevention and mitigation when viewed from this perspective, with 2 orders of magnitude prevention by the pressure boundary reliability, 3 orders of prevention by the ECCS reliability, and almost 4 orders of mitigation by the containment. A characteristic of these results that is typical for LWRs is that there is significant retention of radionuclides within the fuel barrier only when core damage is prevented. Another is, as discussed previously, that when the fuel barrier is postulated to fail as occurs in the core damage sequences, the coolant pressure boundary plays only a minor role in risk mitigation. These LWR examples as well as the MHTGR examples presented in the next section clearly show that the extent of balance between prevention and mitigation when measured in this way is highly sequence dependent.

6.1.3 Evaluation of Selected MHTGR Sequences

To demonstrate the application of these concepts to advanced reactors with fundamentally different characteristics than LWRs, examples from the MHTGR PRA [24] are used. This MHTGR design has a package of inherent characteristics and engineered features that are representative of various modular gas cooled reactor designs using particle fuel, graphite moderator, helium working fluid, and passive decay heat removal capabilities similar to that included in the PBMR. The numerical data used for these examples is summarized in Table

12. As with the PWR sequences, this sample of MHTGR sequences analyzed for one isotope does not tell the whole story. However these sequences are representative of the results of the supporting PRA and include those that dominate the risk of I-131 releases for this reactor concept.

MHTGR-1: Moderate size leak in the Helium Pressure Boundary (HPB) of less than 13 in²; successful reactor trip and continued operation of one of the forced convection cooling systems; releases limited to circulating activity and some lift off of plated out radionuclides.

MHTGR-2: Small leak in the HPB of less than 1 in²; successful reactor trip, failure of the active forced convection cooling systems; conduction cool down of the core using the active Reactor Cavity Cooling System (RCCS); releases limited to circulating activity and delayed release from small fraction of initially failed fuel particles that is minimized due to the successful HPB pump down along this sequence

MHTGR-3: Small leak in the HPB of less than 1 in²; successful reactor trip; failure of the active forced convection cooling systems; failure of the active RCCS; conduction cool-down to the passive reactor cavity heat sinks; releases limited to circulating activity and delayed release from small fraction of initially failed fuel particles (somewhat larger fraction than in Sequence 2)

The risk plots and bar charts for these MHTGR sequences that parallel the development for the PWR sequences are shown in Figure 14 and Figure 15. As seen in these figures the roles of prevention and mitigation for MHTGR-1 are similar to PWR-1 with 2 orders of magnitude of prevention by the reliability of the coolant pressure boundary, and 9 orders of magnitude of mitigation by the barriers, although in this sequence there is less of importance of the reactor building barrier as the MHTGR design employs a non-leak tight confinement concept. However, the pressure boundary retention in the form of plate out for this sequence compensates for the relatively small retention from the non-leak tight confinement.

MHTGR-2 has some functional similarities with PWR-2 in that both involve a small breach in the pressure boundary followed by failure of the active SSCs supporting core cooling functions. However the mitigation level for this sequence is aided by a passive core cooling capability that prevents significant releases from the fuel, although the releases are somewhat higher than in Sequence MHTGR-1. In MHTGR-3 there is failure of both active and passive core cooling systems following the pressure boundary breach, but the passive capability of the reactor to retain its fuel inventory is still significant as the core is still cooled by conduction and radiation to the reactor building heat sinks. What is striking about the prevention and mitigation analysis for these MHTGR sequences is that the mitigation importance of the fuel retention is significant for all envisioned sequences. This is to be expected because the safety design approach for the MHTGR design includes a capability to maintain fuel integrity for each of these selected sequences. The roles of the barriers and the SSCs supporting each barrier are seen to be significantly different than those for the LWR example due to the differences in the safety design approach.

Table 12: Data Assumed for MHTGR Sequence Evaluation (from Reference [24])

Sequence	MHTGR-1	MHTGR-2	MHTGR-3
Initiating event	Moderate Helium Pressure Boundary (HPB) failure	Small HPB failure	Small HPB failure
Active SSC response	Successful Helium pump-down and forced circulation cooling	Successful Helium pump-down, failure of forced circulation cooling systems	Failure of forced circulation cooling systems
Passive SSC response	Successful confinement response	Success of passive core cooling system and confinement	Failure of passive core cooling system
Initiating event frequency per yr.	8×10^{-3}	$\sim 3 \times 10^{-2}$	$\sim 3 \times 10^{-2}$
Active SSC response probability	0.8	$\sim 5 \times 10^{-3}$	$\sim 5 \times 10^{-3}$
Passive SSC response probability	~ 1	~ 1	$\sim 3 \times 10^{-6}$
Fractional release of I-131 from fuel	$\sim 2 \times 10^{-6}$	$\sim 2 \times 10^{-5}$	$\sim 6 \times 10^{-5}$
Fractional release of I-131 from HPB	$\sim 1 \times 10^{-3}$	$\sim 4 \times 10^{-1}$	$\sim 5 \times 10^{-1}$
Fractional release of I-131 from reactor building	$\sim 3 \times 10^{-1}$	$\sim 4 \times 10^{-2}$	$\sim 4 \times 10^{-2}$

While one can use this process to attribute SSC roles and to quantify the SSC importance in preventing and mitigating accidents, it is important to note that the assessment of risk for any sequence for any reactor type is a function of how the inherent features and engineered features respond to the initiating event and interact with each other to produce the definition, frequency, accident progression and consequence of the scenario. In particular the role and importance of leak tight reactor building barriers in implementing the defense-in-depth concept cannot be determined outside of the context of the inherent features, particularly those that determine the fuel performance under accident conditions. This integrated perspective of risk factors is an important principle of ***Risk-Informed Evaluation of Defense-in-Depth*** that is essential to defining and evaluating prevention and mitigation strategies.

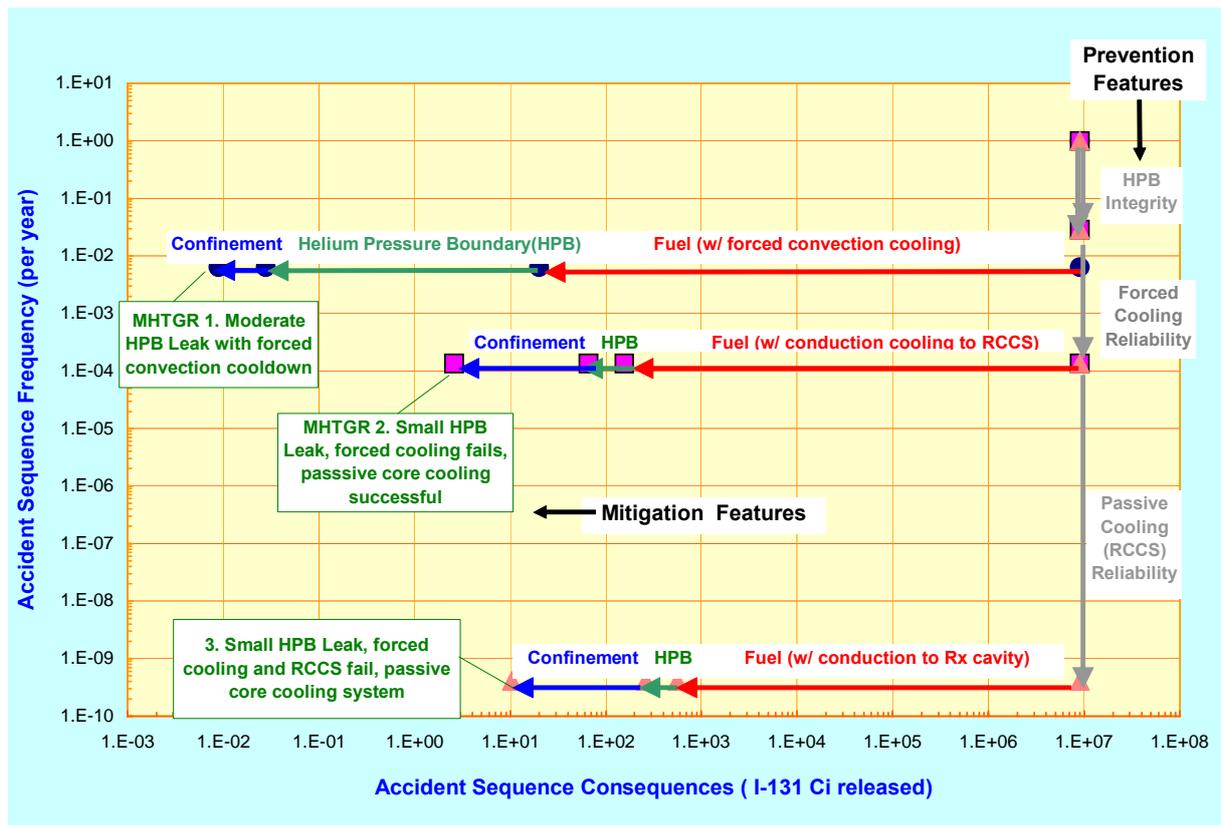


Figure 14: Design Features Contributing to Prevention and Mitigation of I-131 Releases from Selected MHTGR Sequences

Prevention and Mitigation Insights from PWR and MHTGR Examples

Upon review of two sets of sequences for two fundamentally different reactor concepts, it is instructive to review some of the elements of the earlier definitions of defense-in-depth. Several conclusions can be reached for these examples:

- These examples support the conclusion that there exists no single 'balance' between prevention and mitigation. The roles of these strategies are inherently different for different sequences for both the reactor examples. High frequency/low consequence accidents appear to be addressed in the respective reactor safety design approaches with more emphasis on mitigation than prevention, whereas low frequency/high consequence accidents rely more on prevention and progressively less on mitigation. If on the other hand the idea of balancing prevention and mitigation means that across the event sequence spectrum both strategies play an important role, these examples support the concept that prevention and mitigation have been balanced.
- There is no such thing as fully independent barriers to radioactivity release, as all the barriers are mutually dependent on the inherent features of the reactor and how these features interact with the respective barriers, which is different on different sequences. An important role of the PRA is to identify and evaluate the dependencies among the barriers. Barrier independence is a goal to strive for but in practice is only achieved to a degree.

- Differences in the safety design approach between PWRs and the MHTGR are reflected in differences in the roles that each barrier and SSC play in the prevention and mitigation of accidents. In the examples used, both reactors have applied prevention and mitigation using different combinations of inherent features, and passive and active SSCs. The examples clearly show how each barrier is used to prevent and mitigate accidents. Both reactor concepts exhibit **Plant Capability Defense-in-Depth** and **Programmatic Defense-in-Depth** as reflected in the PRA results but have assigned different roles to each barrier and SSC consistent with the respective safety design approaches.

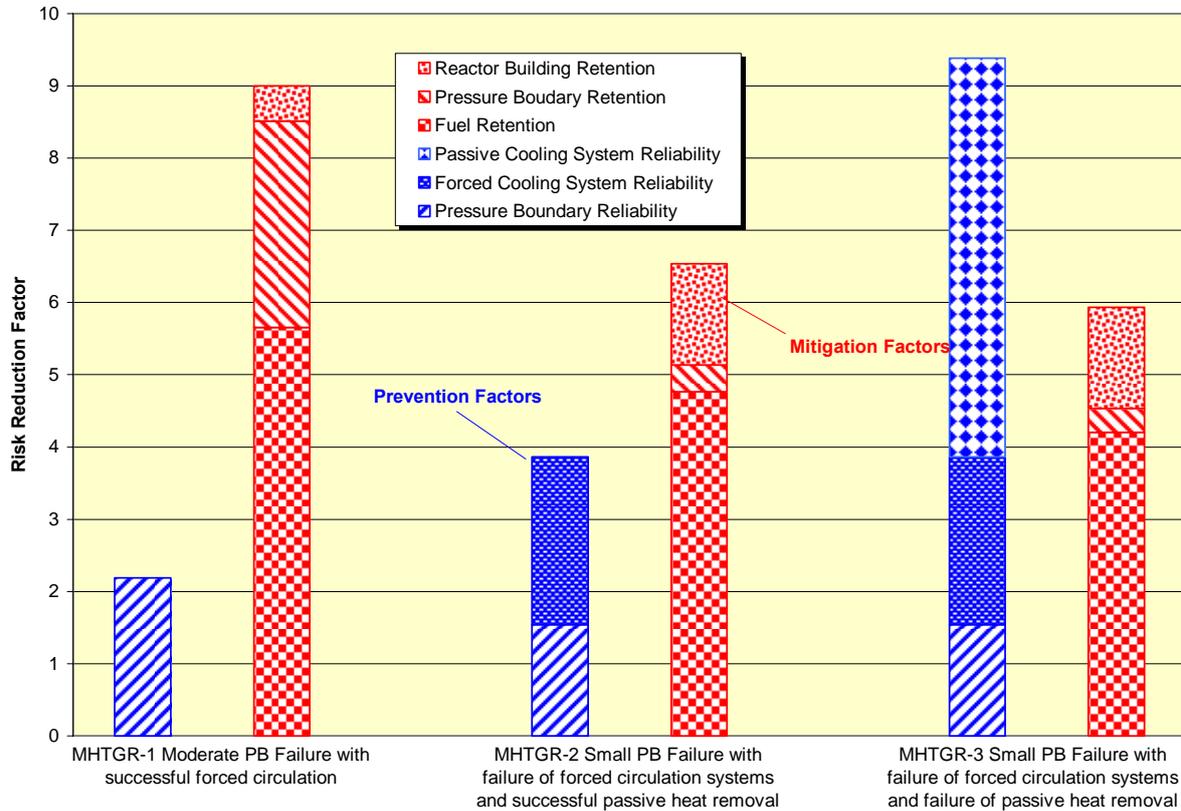


Figure 15: Risk Reduction Factors Associated with MHTGR Design Features Responsible for Prevention and Mitigation of I-131 Releases

As a final comment on this section it is acknowledged that there are uncertainties inherent in the PRA results that were used to support these examples. Hence, if one varies the PRA inputs selected for these examples, listed in Figure 11 and Figure 12, different results and conclusions could be obtained. A systematic review of the PRA uncertainties is an important element of **Risk-Informed Evaluation of Defense-in-Depth** and may be expected to reveal licensing issues that are most efficiently addressed by the addition of specific deterministic requirements.

These examples serve to demonstrate how PRA results can be used to examine and quantify the importance of specific design features in preventing and mitigating severe accidents. These order of magnitude estimates of risk reduction factors using PRA techniques are only intended to provide rough order of magnitude estimates of importance. Nonetheless, such estimates are believed to provide insights into the adequacy of defense-in-depth for reactors whose safety design approach is different than those of currently licensed LWRs. In the PBMR DCA, an evaluation similar to that shown in these examples will be performed to assist the NRC in their review of the adequacy of **Risk-Informed Evaluation of Defense-in-Depth** for the PBMR.

7. REFERENCES

- [1] PBMR (Pty) Ltd, 'U.S. Design Certification – Probabilistic Risk Assessment Approach for the Pebble Bed Modular Reactor,' June 13, 2006.
- [2] PBMR (Pty) Ltd, 'U.S. Design Certification – Licensing Basis Event Selection for the Pebble Bed Modular Reactor,' June 30, 2006.
- [3] PBMR (Pty) Ltd, 'U.S. Design Certification – Safety Classification of Structures, Systems, and Components for the Pebble Bed Modular Reactor,' August 24, 2006.
- [4] 10 CFR Part 50 Appendix R, Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979.
- [5] 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.
- [6] U.S. Nuclear Regulatory Commission, 'Regulation of Advanced Nuclear Power Plants; Statement of Policy,' Federal Register, Vol. 59, No. xx, pg. 35461-35463; July 12, 1994.
- [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, NUREG-0800, 'Standard Review Plan, Chapter 19, Use of Probabilistic Risk Assessment In Plant-Specific, Risk-Informed Decisionmaking: General Guidance', Revision 1, November 2002.
- [9] SECY-06-0217, 'Improvement to and Update of the Risk-Informed Regulation Implementation Plan', U.S. Nuclear Regulatory Commission, October 24, 2006.
- [10] Letter from B. John Garrick, Chairman U.S. NRC Advisory Committee on Nuclear Waste and Dana A. Powers, Chairman U.S. NRC Advisory Committee on Reactor Safeguards to the Honorable Richard A. Meserve, Chairman U.S. Nuclear Regulatory Commission, 'Use of Defense In Depth In Risk-Informing NMSS Activities', May 25, 2000.
- [11] J.N. Sorensen, G.E. Apostolakis, T.S. Kress, D.A. Powers, Advisory Committee on Reactor Safeguards, 'On the Role of Defense in Depth in Risk-Informed Regulation,' American Nuclear Society Conference, PSA '99, International Topical Meeting on Probabilistic Safety Assessment, Washington, DC (408-413), August 22-26, 1999.
- [12] SECY-05-0006, 'Second Status Paper on the Staff's Proposed Regulatory Structure for New Plant Licensing and Update on Policy Issues Related to New Plant Licensing', U.S. Nuclear Regulatory Commission, January 7, 2005.
- [13] SECY-98-144, 'White Paper on Risk-Informed and Performance Based Regulation', U.S. Nuclear Regulatory Commission, January 22, 1998.
- [14] 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.
- [15] SECY-00-0198, 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 50.44 (Combustible Gas Control), U.S. Nuclear Regulatory Commission, September 14, 2000.
- [16] 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.
- [17] SECY-04-0103, 'Status of Response to the June 26, 2003, Staff Requirements Memorandum on Policy Issues Related to Licensing Non-Light Water Reactor Designs', U.S. Nuclear Regulatory Commission, June 23, 2004.

- [18] INSAG-10, 'Defence in Depth in Nuclear Safety,' International Atomic Energy Agency, 1996.
- [19] 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 4 to 8, 2006.
- [20] U.S. Department of Energy, 'Probabilistic Risk Assessment for the Standard High Temperature Gas-Cooled Reactor', DOE-HTGR-86011, Revision 5, April 1988.
- [21] Letter from PBMR (Pty.) Ltd. to U.S. NRC, 'Transmittal of Presentation Materials for PBMR Familiarization Session', (enclosing presentations for February 28 – March 2, 2006 PBMR Safety and Design Familiarization Workshop – Session 1), USDC20060302-1, March 2, 2006.
- [22] Letter from PBMR (Pty.) Ltd. to U.S. NRC, 'Transmittal of Presentation Materials for PBMR Familiarization Session', (enclosing presentations for March 15-16, 2006 PBMR Safety and Design Familiarization Workshop – Session 2), USDC20060316-1, March 16, 2006.
- [23] U.S. Nuclear Regulatory Commission, 'Reactor Risk Reference Document,' NUREG-1150, Volume 1, February 1987.
- [24] NUREG-1338, 'Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)', U.S. Nuclear Regulatory Commission, December 1995.