FRAMEWORK FOR DEVELOPMENT OF A RISK-INFORMED, PERFORMANCE-BASED, TECHNOLOGY-NEUTRAL ALTERNATIVE TO 10 CFR PART 50

Working Draft Report
(Does not represent a staff position)

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research

April 2006

FOREWORD

The purpose of this draft NUREG is to discuss an approach, scope, and acceptance criteria that could be used to develop risk-informed, performance-based requirements for future plant licensing. The Nuclear Regulatory Commission (NRC) is making the latest working draft framework available to stakeholders. This working draft is to inform stakeholders of the NRC staff's consideration of possible changes to its regulations, and to solicit comments on the staff's direction as described in an advance notice of proposed rulemaking published in the Federal Register in April 2006.

This version of the framework is a working draft. It does not represent a staff position and is subject to changes and revisions. The framework is expected to be updated in June 2006 as a final draft. The NRC will post the final draft of the framework on Ruleforum when it is complete.

ABSTRACT

Table of Contents

Chapter Page

EXECUTIVE SUMMARY . . . . . -ix-

1. INTRODUCTION 1-1
   1.1 Background 1-1
   1.2 Objectives 1-2
   1.3 Scope 1-3
   1.4 Desired Principles of the Overall Framework 1-4
   1.5 Relationship to Current Licensing Process 1-5
   1.6 Relationship to Code of Federal Regulations 1-5
   1.7 Report Organization 1-6

2. FRAMEWORK ROADMAP 2-1
   2.1 Introduction 2-1
   2.2 Safety, Security, and Preparedness Expectations 2-2
   2.3 Defense-in-Depth 2-3
   2.4 Protective Strategies 2-4
   2.5 Design Objectives 2-6
   2.6 PRA Scope and Technical Acceptability 2-7
   2.7 Process for Development of Technology-Neutral Requirements 2-8
   2.8 Summary: A Risk-Informed, Performance-Based, Technology-Neutral Framework Roadmap 2-11

3. SAFETY, SECURITY AND PREPAREDNESS EXPECTATIONS 3-1
   3.1 Introduction 3-1
   3.2 Safety Expectations 3-2
      3.2.1 Level of Safety 3-2
      3.2.2 Implementing the NRC's Safety Expectations 3-3
      3.2.3 Subsidiary Risk Objectives 3-6
   3.3 Security Expectations 3-7
   3.4 Preparedness Expectations 3-8
   3.5 Integration of Safety, Security, and Preparedness 3-9

4. DEFENSE-IN-DEPTH: TREATMENT OF UNCERTAINTIES 4-1
   4.1 Introduction 4-1
   4.2 Types of Uncertainty 4-4
   4.3 Defense-in-Depth Objectives and Principles 4-5
   4.4 Defense-in-Depth Approach 4-14
   4.5 Process of Defense-in-Depth 4-16
   4.6 Technology-Specific Considerations for Defense-in-Depth 4-19

5. SAFETY FUNDAMENTALS: PROTECTIVE STRATEGIES 5-1
   5.1 Introduction 5-1
   5.2 Analysis to Identify Requirements 5-3
   5.3 The Protective Strategies 5-4
      5.3.1 Physical Protection 5-4
      5.3.2 Stable Operation 5-5
      5.3.3 Protective Systems 5-5
      5.3.4 Barrier Integrity 5-6
      5.3.5 Protective Actions 5-6

Table of Contents (conte'd)

Chapter Page

6. DESIGN CRITERIA . . . 6-1
6.1 Introduction . . . 6-1
6.1.1 Purpose and Organization . . . 6-1
6.1.2 Differences with Part 50 and Part 52 Approach . . . 6-2
6.2 Acceptance Criteria . . . 6-3
6.2.1 Acceptability of PRA Results . . . 6-3
6.2.1.1 Frequency - Consequence Curve . . . 6-3
6.2.1.2 Quantitative Health Objectives . . . 6-7
6.2.2 LBE Selection and Associated Criteria . . . 6-8
6.2.2.1 Probabilistic Selected LBEs . . . 6-9
6.2.2.2 Deterministic Selected LBE . . . 6-15
6.2.3 Selection of Risk Significant SSCs . . . 6-16
6.3 Safety Margin . . . 6-18
6.3.1 Bounding Set of Licensing Bases Events . . . 6-18
6.3.2 Use of Enveloping and Conservative Codes and Assumptions . . . 6-19
6.3.3 Suitable Acceptance Criteria . . . 6-19
6.3.4 PRA Event Sequences . . . 6-19
6.4 Security Performance Standards . . . 6-20

7. PRA TECHNICAL ACCEPTABILITY . . . 7-1
7.1 Introduction . . . 7-1
7.2 PRA Applications in the Framework . . . 7-2
7.2.1 Generate a Complete Set of Accident Sequences . . . 7-3
7.2.2 Develop a Rigorous Accounting of Uncertainties . . . 7-5
7.2.3 Evaluate the Quantitative Health Objectives (QHOs) . . . 7-6
7.2.4 Evaluate the Frequency-Consequence Curve (F-C Curve) . . . 7-6
7.2.5 Support the Assessment of Security . . . 7-6
7.2.6 Identify and Characterize the Licensing Bases Events . . . 7-7
7.2.7 Identify and Characterize the Treatment of Safety-Significant SSCs . . . 7-7
7.2.8 Support the Environmental Impact Statement (EIS) and the Severe Accident Mitigation Design Alternative (SAMDA) Analysis Development . . . 7-8
7.2.9 Maintain a Living PRA . . . 7-8
7.2.10 Risk-informed Inspections during Fabrication and Construction . . . 7-8
7.2.11 Startup . . . 7-9
7.2.12 Operation . . . 7-10
7.3 Functional Requirements for PRAs for Future Plants . . . 7-10
7.3.1 Technical Requirements . . . 7-11
7.3.2 Quality Assurance Criteria . . . 7-12
7.3.3 Consensus PRA Standards . . . 7-14
7.3.4 Assumptions and Inputs . . . 7-14
7.3.4.1 Assumptions . . . 7-14
7.3.4.2 Inputs . . . 7-14
7.3.5 Analytical Methods . . . 7-14
7.3.6 Analytical Tools . . . 7-14
7.3.7 Independent Peer Review . . . 7-15
7.3.7.1 Team Qualifications . . . 7-15
7.3.7.2 Peer Review Process . . . 7-15
7.3.8 PRA Documentation . . . 7-15
7.3.8.1 Submittal Documentation . . . 7-16
7.3.8.2 Archival Documentation . . . 7-17
7.3.9 Configuration Control . . . 7-17

Table of Contents (cont'd)

Chapter Page

8. REQUIREMENTS DEVELOPMENT PROCESS 8-1
8.1 Introduction 8-1
8.2 Process for Identification of Requirements 8-1
8.3 Technical Requirements: Topics for the Protective Strategies 8-7
8.3.1 Physical Protection 8-7
8.3.2 Stable Operation 8-13
8.3.3 Protective Systems 8-25
8.3.4 Barrier Integrity 8-31
8.3.5 Protective Actions 8-39
8.3.6 Summary of Technical Topics 8-45
8.4 Administrative Requirement Topics 8-49
8.5 Guidelines for Developing Technology-Neutral Requirements 8-55
8.5.1 Use of 10 CFR 50 Requirements and Their Supporting Regulatory Guides 8-55
8.5.2 Development of Stand Alone Requirements 8-56
8.5.3 Use of a Risk-Informed and Performance-Based Approach 8-56
8.5.4 Lessons Learned and Mistakes of the Past 8-57
8.5.5 Licensing Review and Plant Oversight 8-57
8.5.6 Technology-Neutral Requirements 8-58
8.6 Technology-Specific Considerations 8-58
8.7 Completeness and Consistency Check 8-58

List of Figures

Figure Page

1-1 Relationship of Framework to Title 10 of Code of Federal Regulations 1-6
2-1 Structure of the Risk-Informed, Performance-Based, Technology-Neutral Framework 2-2
2-2 Framework Approach to Defense-in-Depth 2-3
2-3 Protective Strategies as Elements of Defense-in-Depth 2-5
2-4 How Design Objectives Support Defense-in-Depth 2-6
2-5 Process for Developing Technical and Administrative Requirements from the Protective Strategies 2-10
2-6 The Risk-Informed, Performance-Based, Technology-Neutral Framework Roadmap 2-11
3-1 Structure of the Framework 3-1
3-2 Three Region Approach to Risk Tolerability/Acceptance 3-2
3-3 Frequency-Consequence Curve 3-4
3-4 Generalized Preparedness as Part of the Protective Actions Protective Strategy . . 3-8
3-5 Process for Developing Requirements 3-10
5-1 Role of Protective Strategies as Elements of Defense-in-Depth 5-1
5-2 The Complete Nature of the Protective Strategies 5-2
5-3 Process for Developing Requirements 5-3
5-4 Logic Tree Developing Requirements for Each Protective Strategy 5-4
6-1 How Design Objectives Support Defense-in-Depth 6-1
6-2 Framework approach 6-3
6-3 Frequency-consequence curve 6-6
6-4 F-C curve regions and deterministic LBE criteria 6-10
6-5 Selection of licensing basis events 6-13
6-6 LBE selection schematic example 6-14
7-1 Event Sequence Example 7-12
8-1 Process for identification of requirements topics. 8-5
8-2 Example logic tree. 8-6
8-3 Logic tree for the physical protection strategy 8-10
8-4 Logic Tree for the Stable Operation Strategy 8-22
8-5 Logic tree for the protective systems strategy. 8-28
8-6 Logic tree for the barrier integrity strategy. 8-35
8-7 Logic tree for the protective actions strategy. 8-42
8-8 Logic tree for the administrative area. 8-52

List of Tables

Table		Page
6-1	Proposed dose/frequency ranges for public exposures	6-5
6-2	LBE Frequency Categories	6-9
6-3	PRA and LBE Criteria	6-12
7-1	PRA Quality Assurance Requirements	7-13
8-1	Physical protection.	8-11
8-2	Stable operation	8-23
8-3	Protective systems	8-29
8-4	Barrier integrity.	8-36
8-5	Protective actions.	8-43
8-6	Summary of Technical Topics.	8-46
8-8	Administrative requirement topics.	8-53
8-9	Summary of administrative topics.	8-54

EXECUTIVE SUMMARY

The purpose of this report is to document the technical basis to support the development of a technology-neutral, risk-informed and performance-based process for the licensing of future nuclear power plants (NPP). As such, it documents an approach, scope and criteria that could be used by the NRC staff to develop a set of regulations that would serve as an alternative to 10 CFR 50 for licensing future NPPs. This alternative to 10 CFR 50 would have the following advantages:

- It would be written to be applicable to any reactor technology, thus avoiding the time consuming and less predictable process of reviewing non-LWR designs against the LWR oriented 10 CFR 50 regulations, which requires case-by-case decisions (and possible litigation) on what 10 CFR 50 regulations are applicable and not applicable and where new requirements are needed.

- It would require a broader use of design specific risk information in establishing the licensing basis, thus better focusing the licensing basis, its safety analysis and regulatory oversight on those items most important to safety for that design.

- It would stress the use of performance as the metrics for acceptability, thus providing more flexibility to designers to decide on the design factors most appropriate for their design.

The information contained in this report is intended to be applicable only to the licensing of commercial NPPs. Similar to 10 CFR 50, it covers the design, construction and operation phases of the plant lifecycle up to and including the initial stages of decommissioning (i.e., where spent fuel is still stored on-site). It covers the reactor, support systems, fuel handling and storage systems. The technical basis and process described in the report are directed toward the development of a stand alone set of requirements (containing technical as well as administrative items) that would be compatible and interface with the other existing parts of 10 CFR (e.g., Part 20, 51, 52, 73, 100, etc.) just as 10 CFR 50 is today. The approach taken in developing the technical basis and process is one that is a combination of deterministic and probabilistic elements and builds upon recent policy decisions by the Commission related to the use of a probabilistic approach in establishing the licensing basis.

At the highest level, the approach taken has as its goal developing a process and regulations that ensures that future NPPs achieve a level of safety at least as good as that defined by the Quantitative Health Objectives (QHOs) in the Commission's 1986 Safety Goal Policy Statement. This is considered consistent with the Commission's 1986 Policy Statement on Advanced Reactors which states that the Commission expects advanced reactor designs will comply with the Commission's Safety Goal Policy Statement, and is discussed further in Chapter 3. In addition, the approach continues the practice of ensuring that the allowable consequences of events are matched to their frequency such that frequent events must have very low consequences and less frequent events can have higher consequences. A set of probabilistic criteria have been developed to implement the above (Chapter 6) that address:

- allowable consequences of events versus their frequency;
- selection of events which must be considered in the design; and
- allowable cumulative individual risk to the public from the events which must be considered in the design.

In addition, a probabilistic approach is used for:
- establishing reliability goals; and
- safety classification of equipment.

Guidance on the scope and quality of the risk assessment needed to support the above is also given (Chapter 7). The use of the above approach has also led to other considerations such as the use of scenario specific source terms for licensing and the consideration of revised siting dose criteria.

To account for uncertainties, a deterministic defense-in-depth approach has been taken that, at a high level, calls for:

- the application of a set of defense-in-depth principles that result in certain deterministic criteria to account for uncertainties; and.
- multiple lines of defense against off-normal events and their consequences (called protective strategies).

The defense-in-depth principles discussed in Chapter 4, address the various types of uncertainty (i.e., parameter, modeling and completeness) and require designs include:

- consideration of intentional as well as inadvertent events;
- accident prevention and mitigation capability;
- ensuring key safety functions are not dependent upon a single element of design, construction, maintenance or operation;
- consideration of uncertainties in equipment and human performance;
- alternative capability to prevent unacceptable releases of radioactive material; and
- siting considerations that facilitate protection of public health and safety.

The protective strategies discussed in Chapter 5, address accident prevention and mitigation and consist of the following:

- physical protection;
- maintaining stable operation;
- protective systems;
- maintaining barrier integrity; and
- protective actions.

In Chapter 8, the protective strategies are examined to identify what needs to be done to ensure the success of each one. This is done through the application of a logic diagram and the defense-in-depth principles to each protective strategy to identify the topics which must be addressed by the regulations to prevent failure of that protective strategy and address uncertainties. The topics identified are organized by whether they apply to design, construction or operation and, if additional guidance related to the topic is provided in the framework, an appropriate reference is given. A summary of the technical topics is provided in Table 8-6. A similar process is also applied to the identification of topics for administrative requirements which are summarized in Table 8-9. The list of topics contained in Chapter 8 then forms the starting point for the development of requirements. Chapter 8 also provides guidance on how to develop the requirements, including utilizing a performance-based approach and using existing requirements in 10 CFR 50 where they are already technology-neutral. Finally, a completeness check was made by comparing the topics identified in Chapter 8 to other safety requirements (e.g., IAEA Standards, 10 CFR 50). The results of completeness check are also discussed in Chapter 8.

1. INTRODUCTION

1.1 Background

The purpose of this report is to provide the technical basis for the development of a risk-informed, performance-based, technology-neutral framework for licensing new commercial nuclear power plants. The guidance and criteria contained in the framework can be used to develop licensing regulations and requirements that are either technology-neutral or technology-specific as an alternative to 10 CFR Part 50.

The Commission, in its Policy Statement on Regulation of Advanced Nuclear Power Plants, stated its intention to "improve the licensing environment for advanced nuclear power reactors to minimize complexity and uncertainty in the regulatory process." [Ref. 2.1] The staff noted in its Advanced Reactor Research Plan [Ref. 2.2] to the Commission, that a risk-informed regulatory structure applied to license and regulate advanced (new) reactors, regardless of their technology, could enhance the effectiveness, efficiency, and predictability (i.e., stability) of new plant licensing. This new process, if implemented, could be available for use later in the decade. The need to develop a risk-informed, performance-based and technology-neutral framework for establishing requirements, which may be technology-neutral or technology-specific, for new reactors is based on the following considerations:

- While the NRC has over 30 years experience with licensing and regulating nuclear power plants, this experience (as reflected in regulations, regulatory guidance, policies and practices) has been focused on current light-water-cooled reactors (LWRs) and may have limited applicability to new reactors. The design and operational issues associated with the new reactors may be distinctly different from current LWR issues. The current set of regulations do not necessarily address safety concerns that may be posed by new designs, and the current set may contain specific requirements that do not pertain to new designs.

- The regulatory structure for current LWRs has evolved over five decades. Most of this evolution occurred without the benefit of insights from probabilistic risk assessments (PRAs) and severe accident research. It is expected that future applicants will rely on PRAs as an integral part of their license applications. Hence guidance and criteria on the use of PRA results and insights will be an important aspect of the licensing process.

- It is also expected that the regulations for new reactors will be risk-informed and performance-based. The use of risk metrics in evaluating safety focuses attention on those areas where risk is most likely and the use of performance measures provides flexibility to designers in emphasizing outcomes rather than prescriptive methods of achieving them. Both deterministic and probabilistic criteria and results will be used in the development of the regulations governing these reactors. Consequently, a structured approach towards a regulatory structure for new reactors that incorporates probabilistic and deterministic insights will help ensure the safety of these reactors by focusing the regulations on where the risk is most likely while maintaining basic safety principles, such as defense-in-depth and safety margin.

- The provision of a framework that is technology-neutral with respect to important probabilistic and deterministic criteria governing risk acceptance and performance will facilitate the development of a consistent, stable, and predictable set of requirements that are both risk-informed and performance-based. These requirements may be either technology-neutral, and so can be applied to any reactor design in conjunction with technology-specific regulatory guides, or technology-specific, i.e., focused on particular designs.

The NRC's past LWR experience, especially the recent efforts to risk-inform the regulations, has shown the potential value of a top-down approach to developing a regulatory structure for a new generation of reactors. Such an approach could facilitate the implementation of risk-informed performance-based regulation, as well as ensure a greater degree of coherence among the resulting regulations for new reactors than found among current regulations.

In addition to utilizing the benefits of PRA, the development of a risk-informed performance-based structure for new plant licensing has several advantages over continuing to use the 10 CFR Part 50 licensing process for designs substantially different than current generation LWRs. While the current Part 50 requirements are used to the extent feasible in developing the alternative, the use of a technology-neutral approach can provide greater efficiency, stability and predictability than continuing to use the 10 CFR Part 50 process. These points are further discussed below.

- Efficiency: When 10 CFR Part 50 is used to license a reactor design substantially different than a current generation LWR, the regulations must be reviewed for applicability to that design. In the review, determinations must be made regarding which regulations apply, which do not, and what additional requirements are needed to address the unique aspects of the design under review. Once these determinations are made, exemptions must be processed to formally document the rules that do not apply and the Commission may need to approve any new requirements (as was done in the certification of the ALWRs). The results of this process are also subject to challenge through the intervention and hearing process. This entire process must be done for each design reviewed using 10 CFR Part 50. Repeating this process for each new design is inefficient. A technology-neutral licensing process that applies regardless of reactor design will eliminate the case-by-case review process.

- Stability: Putting each reactor design through the licensing process described above does not lead to stability in licensing. With case-by-case reviews and intervention, similar issues may have different results. This situation can occur due to different staff involvement, different Commission involvement, or different public involvement. This licensing process has large uncertainties in both outcome and duration. A licensing process derived from a technology-neutral framework establishes a level playing field based on risk criteria and fundamental safety principles like defense-in-depth and safety margin that has acceptance criteria applicable to all reactor designs. This approach will reduce the uncertainties in the outcome and duration of the licensing process because acceptance criteria would be stable.

- Predictability: Having a set of requirements that are based on and derived from technology-neutral criteria and principles will promote predictability by stabilizing the licensing process, making the outcome and duration more predictable. Predictability is an important factor in any decision to pursue the licensing of a nuclear power plant.

The development of a licensing process based on a technology-neutral framework that is an alternative to the current Part 50 process will help ensure that a systematic approach is used to develop the regulations for the design, construction, and operation of new reactors. This will ensure a greater degree of uniformity, consistency, and defensibility in the development of the requirements, particularly when addressing the unique design and operational aspects of new reactors.

1.2 Objectives

The objective of this document is to develop a risk-informed, performance-based technology-neutral framework that provides the technical basis, including guidance and criteria, for writing the requirements for licensing new reactors. These requirements, that may be technology-neutral or

technology-specific, will demonstrate that the NRC mission of protecting the public health and safety is met.

The development of the framework is based on a unified safety concept that derives regulations from the Commission's Safety Goals Policy and other safety principles such as defense-in-depth and safety margin.

To meet this objective, the guidance and criteria need to address the following:

- safety, security and preparedness expectations
- defense-in-depth: treatment of uncertainties
- safety fundamentals
- design objectives
- PRA technical acceptability
- process for the identification of requirements.

Safety, security, and preparedness expectations for future plants to be licensed by the NRC are established that meet the Commission's expectations for future reactors and that will provide for the public health and safety.

A defense-in-depth structure is established such that the uncertainties are addressed that will ensure safety limits are met and that the design, construction and operation have enough safety margin to withstand unanticipated events.

Safety fundamentals are defined in terms of protective strategies, that when met, ensure the protection of the public health and safety.

Design objectives are established for the identification and selection of licensing events and for the classification of risk significant components.

High level requirements are established for PRA scope and acceptability to support the use of risk results and insights in the development of risk-informed requirements.

1.3 Scope

The risk-informed performance-based framework developed in this report applies to all new plants. It is expected that the regulations that derive from this framework will be applicable to all types of reactor designs, including gas-cooled, liquid metal, and heavy and light-water-moderated reactors. This applicability will be accomplished either by having the regulatory requirements specified at a high (technology-neutral) level, or by developing technology-specific requirements for particular designs based on the criteria and guidance offered in the framework.

The framework will address risks from all sources of radioactivity that are present at the plant. These include: reactor full-power, low-power and shut-down operation, and spent fuel storage and handling and the risks from both internal and external events. Therefore, it includes seismic, fire and (internal and external) flood risks, and risk from high winds and tornados. Issues related to security will also be considered. Risks from other sources that are an integral part of the licensing process, e.g., liquid sodium for liquid metal reactors, are also included in the scope of the framework.

The framework will cover design, construction, and operation. Operation includes both normal operation as well as off-normal events, ranging from anticipated occurrences to rare but credible events, for which accident management capabilities may be needed.

The framework is intended to provide guidance on the structure and key elements which will be used to develop the risk-informed, performance-based regulations that may be technology-neutral or technology-specific. In effect, the framework provides guidance on key technical issues and the scope of the technology-neutral or technology-specific requirements. Many of the details will only be developed as part of the regulation development.

The staff intends ultimately to codify the regulatory structure for new plant licensing in a new stand-alone part in 10 CFR. This new part will provide a technology-neutral alternative to the current 10 CFR Part 50. The new part, similar to the current 10 CFR Part 50, will also interface, as needed, with the other parts of 10 CFR (e.g., Parts 20, 51, 52, 54, 100).

The regulatory structure will be written to allow either a two-step licensing process (i.e., construction permit/operating license) or a one-step (combined operating license) licensing process, similar to the current 10 CFR Part 50. It will also include a provision for exemptions in case an applicant wishes to propose an alternative approach to one or more requirements.

1.4 Desired Principles of the Overall Framework

As the regulatory structure is developed and implemented, it should adhere to certain principles that are based on and consistent with the NRC's mission of protecting the public health and safety and the environment and the common defense and security as outlined in the NRC's Strategic Plan (Ref. 1.3). These principles essentially define the acceptance criteria of the technology-neutral framework and the technology-neutral and technology-specific requirements:

- **Safety**. The requirements will ensure protection of public health and safety and the environment.

- **Security.** The secure use and management of radioactive materials will be ensured.

- **Openness.** Openness in the regulatory process will be maintained.

- **Effectiveness**. The structure will ensure that NRC actions are effective, efficient, realistic and timely.

In addition, the framework must also ensure that it is:

- ***Technology-neutral***. The framework is developed in such manner that, as new information, knowledge, etc is gained, changes and modifications to the regulatory structure can be adapted to any technology-specific reactor design in an effective and efficient manner.

- ***Risk-informed.*** Risk information and risk insights are integrated into the decision making process such that there is a blended approach using both probabilistic and deterministic information.

- ***Performance-based***. When implemented the guidance and criteria will produce, a set of safety requirements that will not contain prescriptive means for achieving its goals, and therefore be performance oriented to the extent practical.

- ***Incorporates Uncertainty***. The guidance and criteria have to address the uncertainties, identification of key uncertainties, the impact of the uncertainties, and their treatment in the development of the requirements.

- ***Maintains Defense-in-depth.*** Defense-in-depth is maintained and is an integral part of the framework.

1.5 Relationship to Current Licensing Process

The purpose of the framework is to provide the technical basis to support the development of a technology-neutral, risk-informed and performance-based process for the licensing of new nuclear power plants (NPP). As such, it documents an approach that can be used to create a 'level playing field' for all new reactor technologies in terms of the safety criteria to be met. The framework approach, scope and criteria could be used by the NRC staff to develop a set of regulations that would serve as an alternative to 10 CFR 50 for licensing new NPPs. The regulations developed from the framework approach could still be used in conjunction with 10 CFR 52 for carrying out the licensing process, i.e., obtaining a combined operating license and/or design certification.

A key difference in the framework approach is the combination of deterministic and probabilistic criteria to establish the plant's safety. In the current Part 50/52 licensing approach the deterministic calculations carried out for the licensing basis events, i.e., the design basis accidents (DBAs) and, separately, for the probabilistic risk analysis (PRA) are important components of the safety analyses, but there is no direct link between these two components. The Framework approach links the PRA analysis with the other design objectives of licensing basis event selection and criteria, and SSC selection and treatment.

1.6 Relationship to Code of Federal Regulations

In establishing a technology-neutral approach to the development of the criteria and bases of the NRC regulation of new reactors in order to protect public health and safety, it is useful to review the relationship of the current 10 CFR Part 50 (and Part 52) to the entire set of regulations governing the nuclear fuel cycle as shown in Figure 1-1.

These regulations extend from Part 40 that cover the licensing of source material, through Part 70 that covers the licensing of various operations leading to the fabrication of fuel assemblies, Parts 72 and 63 that cover the licensing of reactor spent fuel storage either at the reactor site or in an independent spent fuel storage installation and final disposal in the high level waste repository, Part 73 that refers to the physical protection licensing aspects of plants and materials, and Part 100 that governs reactor siting. As shown in Figure 1-1 below, in addition to the regulations that govern individual steps in the manufacture, utilization, and disposal of fuel, there are cross-cutting regulations that impact every step of the overall fuel cycle. These cross-cutting regulations include: Part 20 that deals with radiation protection standards for the public, the workers and the environment, Part 51 that covers environmental protection regulations, and Part 71 that involves the safe and secure transport of radioactive material including reactor fuel.

Appendix B contains a review of each of the links of the regulations in Part 50 to the regulations in other parts of Title 10 of the Code of Federal Regulations (CFR) including the parts shown in Figure 1-1. Hence, in establishing a new technology-neutral Part 53, the links to other parts of 10 CFR and the contents of those links will need to be reviewed to determine their technology-neutral character.

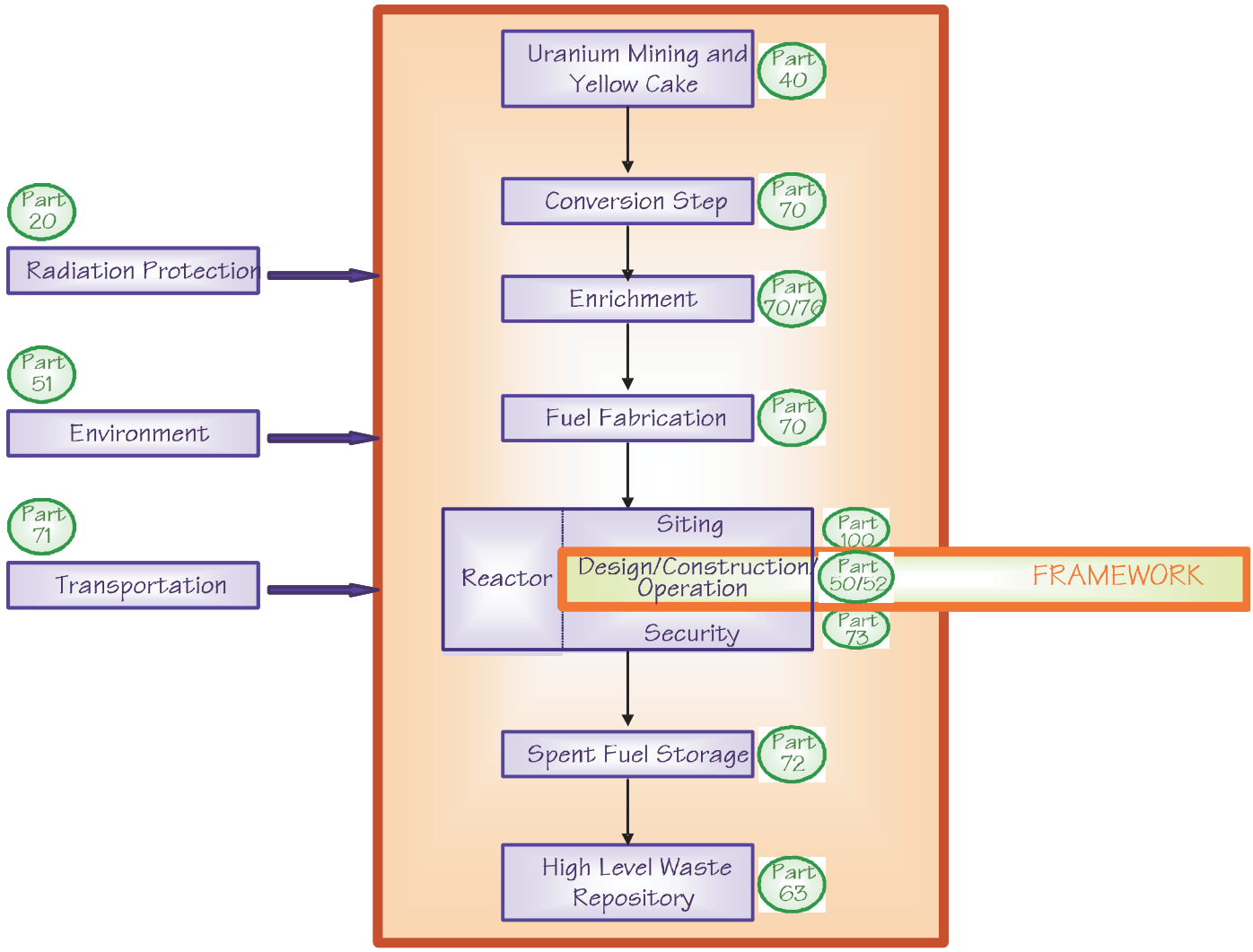

Figure 1-1 Relationship of Framework to Title 10 of Code of Federal Regulations

1.7 Report Organization

The report is organized into 8 Chapters and 9 Appendices. Following the Introduction, Chapter 2 presents a roadmap to the entire report, Chapters 3 through 7 contain details of the criteria, principles, and standards on which the technology-neutral framework is constructed, and Chapter 8 provides an account of the process for developing requirements. Appendices A through I contain additional details of various topics referred to in the framework report chapters including: an overview of the safety characteristics of selected new reactors, the relationship of 10 CFR 50 to other parts of 10 CFR and vice versa, principles related to the protection of the environment, derivation of the risk surrogates for LWRs, examples of the LBE selection process, PRA technical acceptability criteria, a completeness check of the applicability of 10 CFR 50 requirements to the technology-neutral framework, and guidance for the formulation of performance-based requirements.

2. FRAMEWORK ROADMAP

2.1 Introduction

The purpose of this chapter is to provide a roadmap to the risk-informed, performance-based, technology-neutral framework for new plant licensing. The roadmap is straightforward: it explains how the framework is rooted in the requirements of the Atomic Energy Act leading to

- A set of safety/security/preparedness expectations, which are ensured by
- Defense-in-depth expectations, which are fulfilled by
- A set of protective strategies and certain design objectives, which feed
- A process for development of technology-neutral requirements

The basis for nuclear reactor regulation originates with the Atomic Energy Act of 1954[(2.1)] and the statutes that amended it, which indicate that the mission of the NRC and the AEC before it is to ensure that commercial nuclear power plants (NPP) are operated in a manner that provides adequate protection of public health and safety and is consistent with the common defense and security, i.e., protects against radiological sabotage and the theft or diversion of special nuclear materials. [Ref. 2.3] The Atomic Energy Act sets the overall NRC safety mission to protect public health and safety. The amending statutes and the broad body of USNRC regulation implement an underlying safety philosophy that controls the risk to workers, offsite populations and surrounding lands(i.e., environment).

Over the past 50 years, the USNRC has developed a stable and predictable regulatory structure for light water reactors, based on requirements of the law. This framework for new plant licensing provides the guidelines and criteria for developing technology-neutral requirements for new reactors, including designs with little resemblance to current light water reactor designs. These designs may lie far beyond the current regulatory knowledge base and the current regulatory structure may not be best suited for the policy and technical issues they raise. Nevertheless, the experience gained in decades of regulatory experience has provided insights that help formulate the fundamentals of a new regulatory structure. The lessons learned include the importance of defense-in-depth, the benefit of integrating risk insights, the need to be performance-based. These are things that have contributed to and can maintain the stability and predictability of the current

---

[(2.1)] Excerpt from the Atomic Energy Act:

Sec. 3. Purpose.
It is the purpose of this Act to...[provide] for–

a. a program of conducting, assisting, and fostering research and development in order to encourage maximum scientific and industrial progress;
b. a program for the dissemination of unclassified scientific and technical information and for the control, dissemination, and declassification of Restricted Data, subject to appropriate safeguards, so as to encourage scientific and industrial progress;
c. a program for Government control of the possession, use, and production of atomic energy and special nuclear material, whether owned by the Government or others, so directed as to make the maximum contribution to the common defense and security and the national welfare, and to provide continued assurance of the Government's ability to enter into and enforce agreements with nations or groups of nations for the control of special nuclear materials and atomic weapons.
d. a program to encourage widespread participation in the development and utilization of atomic energy for peaceful purposes to the maximum extent consistent with the common defense and security and with the health and safety of the public;
e. a program of international cooperation to promote the common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit; and
f. a program of administration which will be consistent with the foregoing policies and programs, with international arrangements, and with agreements for cooperation, which will enable the Congress to be currently informed so as to take further legislative action as may be appropriate.

regulatory structure. [Ref. 2.4] Thus the framework is an evolution of the historical licensing process.

The framework for new plant licensing has been developed following a top-down approach, as shown in Figure 2-1. It is built upon the traditional NRC safety mission, beginning with the Atomic Energy Act and encompassing a set of safety, security, and preparedness expectations. The framework describes the NRC's criteria for meeting these expectations and provides guidance for achieving them through meeting a series of defense-in-depth expectations. Defense-in-depth is directed toward compensating for uncertainties and evolves from a set of defense-in-depth *principles* that are embraced throughout the design. Finally, a set of technology-neutral, risk-informed, performance-based requirements are developed to ensure that defense-in-depth is maintained throughout design, construction and operations. The framework, then, is a hierarchical approach to safety, one that assures that safety, security, and preparedness are maintained throughout design, construction, and operations.

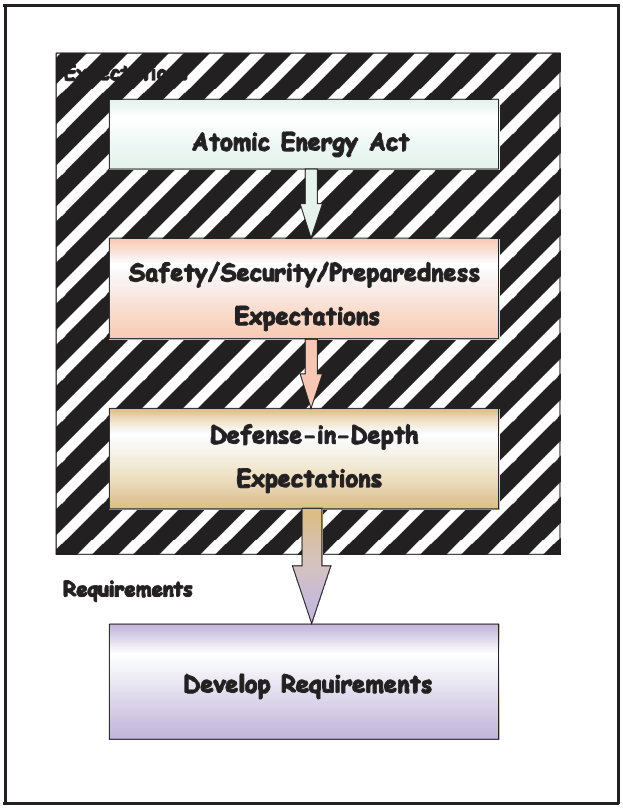

Figure 2-1 Structure of the Risk-Informed, Performance-Based, Technology-Neutral Framework

2.2 Safety, Security, and Preparedness Expectations

The framework integrates the NRC's expectations for safety, security, and preparedness to achieve the desired overall level of safety on a technology-neutral basis. That is, a licensing basis that can be applied to all new plants, regardless of technology. The approach requires that safety and security assessments realistically model plant and preparedness response and that the results of these assessments are integral with the development of technology-neutral regulatory requirements. The entire process ensures that safety and security design issues and preparedness requirements are addressed early in the design and regulatory review process so that the resulting design relies more on inherent features and less on extrinsic operational safety and security programs

The NRC's ***safety expectations*** are anchored in the Commission's safety goals [Ref. 2.5], which are based on the idea of minimizing additional risk burden to the population for the benefits of nuclear power. These underlying ideas are as appropriate for new reactors as they are for existing LWRs.

The Commission in their Policy Statement on "Regulation of Advanced Nuclear Power Plants," [Ref. 2.6] noted two expectations:

(26) that advanced reactors will provide enhanced margins of safety

(27) that advanced reactor designs will comply with the Commission's safety goal policy statement.

Accordingly, the framework is using the NRC safety goal QHOs as the level of safety that the requirements are intended to meet.

The NRC's ***security expectations*** are that new reactors shall have the same level of protection as established by the post 9/11 NRC requirements. However, new plant security expectations will be evaluated integral with the design, rather than an add-on consideration. In addition, a security assessment will be employed to look for vulnerabilities.

The NRC's ***preparedness expectations*** include the necessity for emergency preparedness capability, regardless of reactor technology or design or level of safety.

The NRC's safety, security, and preparedness expectations are more fully expanded in Chapter 3.

2.3 Defense-in-Depth

A core principle of the NRC's safety philosophy has always been the concept of defense-in-depth, and defense-in-depth remains basic to the safety and security expectations in the framework. "The defense-in-depth philosophy .....has been and continues to be an effective way to account for uncertainties in equipment and human performance." [Ref. 2.7] The ultimate purpose of defense-in-depth is to compensate for uncertainty–e.g., uncertainty due to lack of operational experience with new technologies and new design features, uncertainty in the type and magnitude of challenges to safety, uncertainty associated with physical, chemical, and aging phenomena under the wide range of possible conditions. In licensing new reactors, the treatment of uncertainties will play a key role in ensuring that safety limits are met and that the design is robust with respect to unanticipated factors.

In general, at the time of licensing, uncertainties associated with new plants will tend to be larger than uncertainties associated with existing plants
In laying the groundwork for defense-in-depth for new reactor designs, analysts can benefit from the experience of past designs, but at the same time must be willing to re-examine conclusions based on existing designs and consider new alternatives.

The aim of the framework is to develop an approach to defense-in-depth for new reactors that is consistent with the successful past practices used for operating reactors, but which improves on past practices by being more consistent and by making use of quantitative information where possible. The framework's defense-in-depth approach is one which combines deterministic and probabilistic elements (Figure 2-2).

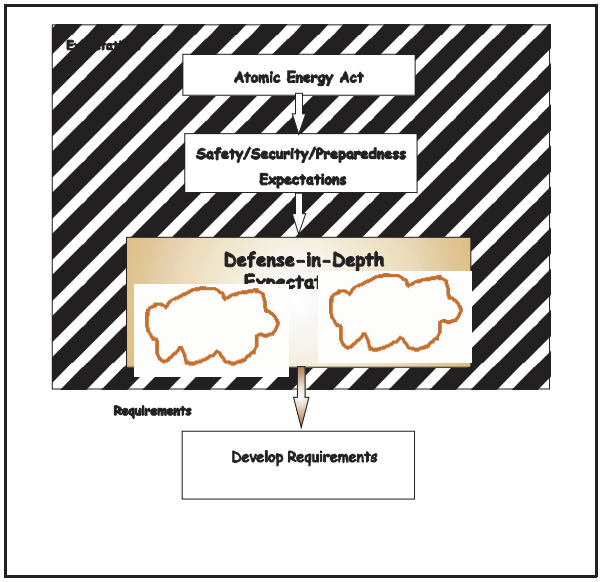

Figure 2-2 Framework Approach to Defense-in-Depth

The deterministic elements of the framework ensure that a set of defense-in-depth principles are followed. These principles[2.2] are established by examining the different kinds of uncertainties to be treated, and incorporating successful past practices and lessons learned related to defense-in-depth. They are applied regardless of the likelihood of failure. Therefore, a characteristic of this approach is that the high level lines of defense are maintained; accident prevention alone cannot be relied on to reach an acceptable level of safety; the capability to mitigate accidents is also needed. This is the approach to defense-in-depth that has been used in the past to achieve adequate protection and primarily address completeness uncertainties. A major guarantor of this approach is the maintenance of the five protective strategies[2.3] described in Section 2.4 below.

The probabilistic elements of defense-in-depth are the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. The probabilistic approach acknowledges PRA as a powerful tool in the search for the unexpected and the identification of uncertainties. This approach uses risk assessment to: (1) identify scenarios and, in doing so, identify as many originally unforseen scenarios as possible, (2) identify the associated uncertainties that lie in the plant design and operation, and, as far as possible, (3) quantify the extent of the uncertainty in frequency and consequences of the scenarios.

The probabilistic elements of the framework's defense-in-depth approach subsequently establish adequate defense-in-depth measures, including safety margins, to compensate for those scenarios and their uncertainties which are quantified in the PRA model. The ability to quantify risk and estimate uncertainty using PRA techniques and taking credit for defense-in-depth measures in risk analyses, allows a better answer to the question of how much defense-in-depth is enough. The approach to Defense-in-Depth is fully explained in Chapter 4.

2.4 Protective Strategies

The Protective Strategies approach is based on a philosophy of regulation that requires multiple strategies to ensure that there is little chance of endangering public health and safety. It is a top-down, hierarchical approach that starts with a desired outcome and identifies protective strategies (safety fundamentals) to ensure this outcome is achieved even if some strategies should fail. The protective strategies provide high-level lines of defense that offer multiple layers of protection of public health and safety.

The framework identifies the following five protective strategies: *Physical Protection, Stable Operation, Protective Systems, Barrier Integrity,* and *Protective Actions* as put in context in Figure 2-3. The protective strategies introduced here set the design, construction, and operating conditions that will ensure protection of public health and safety, workers, and the environment.

(2.2)

The Defense-in-Depth Principles discussed in Section 4.3 are: (1) Measures against intentional as well as inadvertent events are provided, (2) The design provides accident prevention and mitigation capability, (3) Accomplishment of key safety functions is not dependent upon a single element of design, construction, maintenance, or operation, (4) Uncertainties in SCCs and human performance are accounted for in the safety analyses, (5) The design has the capability to prevent an unacceptable release of radioactive material, (6) Plants are sited at locations that facilitate the protection of public health and safety.

(2.3)

The five protective strategies–Physical Protection, Stable Operation, Protective Systems, Barrier Integrity, and Protective Actions–are structuralist requirements and are discussed in Section 2.4 and Chapter 5.

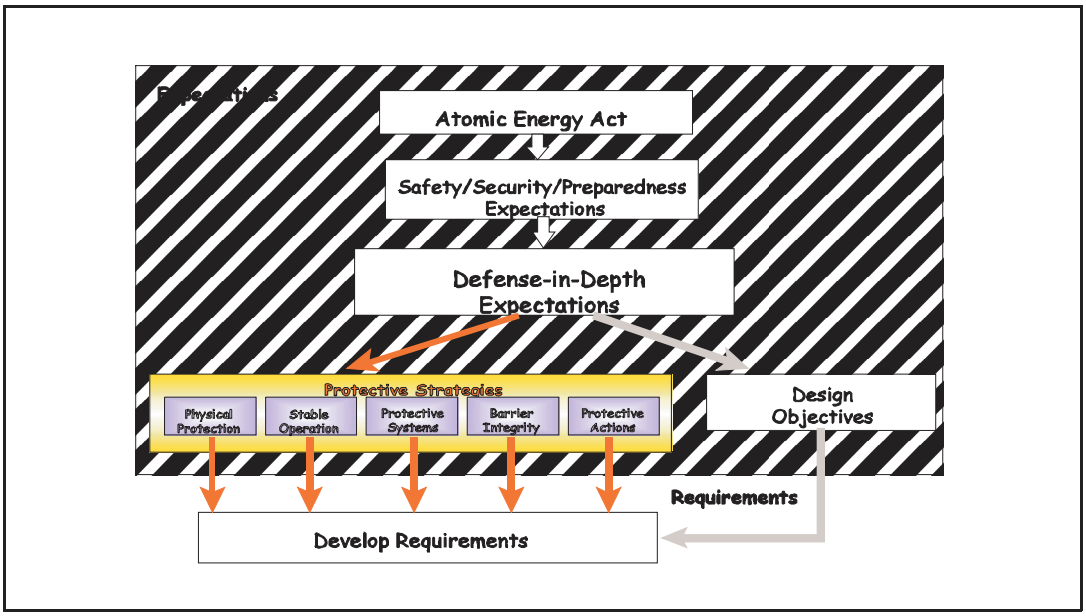

Figure 2-3 Protective Strategies as Elements of Defense-in-Depth

The objective of each protective strategy is introduced here and expanded in Chapter 5.

- The **Physical Protection** objective is to protect workers and the public against intentional acts (e.g., attack, sabotage, and theft) that could compromise the safety of the plant or lead to radiological release.

- The **Stable Operation** objective is to limit the frequency of events that can upset plant stability and challenge safety functions, during all plant operating states, i.e., full power, shutdown, and transitional states. Initiating events must be modeled that can affect any source of radioactive material on-site in any chemical and physical form.

- The **Protective Systems** objective is to ensure that the systems that mitigate[(2.4)] initiating events are adequately designed, and perform adequately, in terms of reliability and capability, to satisfy the design assumptions regarding accident prevention and mitigation during all states of reactor operation. Human actions to assist these systems and protect the barriers are included here.

[(2.4)]Protective systems provide a mitigation role by features and capabilities that fulfill safety functions in response to initiating events and thereby protect the barriers. They also provide a prevention role by application of design and operational features that contribute to their reliability and thereby reduce the probability that an initiating event will leadt to an accident involving protective systems failures.

- The **Barrier Integrity**[2.5] objective is to ensure that there are adequate barriers to protect the public from accidental radionuclide releases from all sources. Adequate functional barriers must be maintained to protect the public and workers from radiation associated with normal operation and shutdown modes and to limit the consequences of reactor accidents if they do occur. Barriers can include physical barriers as well as the physical and chemical form of the material that can inhibit its transport if physical barriers are breeched.

- The **Protective Actions** objective is to ensure that adequate protection of the public health and safety in the event of a radiological emergency can be achieved should radionuclides penetrate the barriers designed to contain them. Measures include emergency procedures, accident management, and emergency preparedness.

The manner in which these protective strategies are met is described in Chapter 5. A top-down analysis of each protective strategy leads directly to a categorization of the kinds of requirements that can ensure that the protective strategies are met. The protective strategies provide the primary basis for the development of technology-neutral requirements, as introduced in Section 2.7.

2.5 Design Objectives

Reactor designers use design objectives to provide anchor points for the economic, safety, and environmental, goals that they are trying to achieve. The regulator, who is primarily concerned with safety and environmental protection, is interested in design and operations objectives associated with safety. Design objectives are stipulated in terms of acceptance criteria and specific safety analyses required to demonstrate compliance.

The design objectives parallel and are complementary with the Protective Strategies, in support of the NRC's defense-in-depth expectations, as shown in Figure 2-4. They provide overall goals that the protective strategies are intended to meet. The design objectives are derived from the quantitative health objectives (QHOs) of the NRC's safety goals. Chapters 3 and 6 explain how risk goals and design expectations are to be used to ensure that the safety goal QHOs are met.

[2.5] Note that the purpose of barriers, protective systems and emergency preparedness is to mitigate the accident sequences by reducing their frequency or their impact. Historically engineers have spoken of preventing core melt and mitigating core damage. These terms are not especially helpful with some new reactor designs and prevention/mitigation definitions change as the object under discussion changes - core damage, release from the primary system, release off-site, etc.

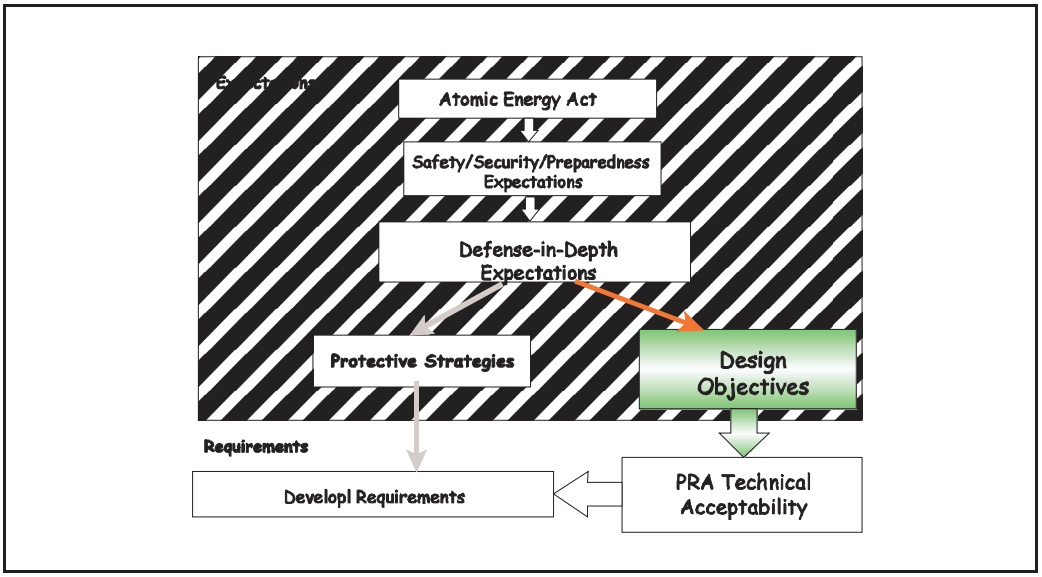

Figure 2-4 How Design Objectives Support Defense-in-Depth

In the framework, design objectives establish two basic parts of the licensing requirements: (1) identification and selection of those events that are used in the design to establish the licensing basis (licensing basis events or LBEs), and (2) the classification of systems, structures, and components (SSCs) by safety significance. The framework relies on defense-in-depth measures in both the LBE selection and the SSC selection, but, in addition, uses the risk information from the PRA to focus attention on the risk significant aspects of the design. LBEs must meet more stringent probabilistic acceptance criteria than other PRA sequences and, in the higher frequency event categories, meet additional deterministic criteria, as described in Chapter 6. In this manner the LBEs provide additional assurance that the design has adequate defense-in-depth in the form of sufficient margin to account for uncertainties. The LBEs also provide a detailed check on whether the PRA analysis meets the necessary risk guidelines and are used in assessment of site suitability.

2.6 PRA Scope and Technical Acceptability

Probabilistic risk assessment (PRA) will play a significant role in the licensing of advanced reactors. Because of this fact, the quality of the PRA used in making licensing decisions will have to be commensurate with the significance of the regulatory decision. The framework identifies uses of PRA during the pre-application, design certification, one-step (i.e., combined operating license) and two-step (i.e., construction permit and operating license) license reviews of new reactor designs. Many of the identified PRA applications are similar to those being applied to existing LWRs. In addition, new types of PRA applications are possible prior to designing and constructing a new reactor, such as establishing LBEs; identifying safety-significant SSCs and their corresponding special treatment requirements; identifying key uncertainties and associated research needs to address them; development of plant operating procedures and emergency response and accident management plans; and comparison of the plant design and operation against licensing risk criteria.

Based on experience with LWR PRA, the framework identifies the high level requirements necessary to ensure the quality of PRA necessary for the use of the PRA in licensing applications. High-level requirements are provided for evaluating both internal and external events during all

modes of operation. However modeling new reactors may necessitate extensions of current PRA methods.

New reactor designs may focus on the use of passive systems and inherent physical characteristics to ensure safety, rather than relying on the performance of active electrical and mechanical systems. For plants, with many passive systems, fault trees may be very simple when events proceed as expected and event sequences may appear to have very low frequency. The real work of PRA for these designs may lie in searching for unexpected scenarios. Innovative ways to structure the search for unexpected conditions that can challenge design assumptions and passive system performance will need to be developed or identified and applied to these facilities. The risk may arise from unexpected ways the facility can end up operating outside the design assumptions. For example, there may be a need for a HAZOP-style search scheme [Ref. 2.8] for scenarios that deviate from designers' expectations and structured search processes for construction errors, operator and maintenance errors, aging problems, and gradual degradation of passive systems.

PRA techniques can also be used to support the licensing effort by evaluating the risk from accidents involving other hazardous materials (e.g., spent fuel, radioactive waste, radioactive sodium). Thus, the identified high level requirements are such that they include accident analysis of all sources of hazardous materials. Finally, requirements for the use of PRA models to identify target sets (i.e., vital area analysis) are provided. Vital area analysis can be used to optimize a plant design not only from a security stand point but also from internal threats such as high energy line breaks, fires, and floods. The framework builds on existing PRA quality requirements delineated in Regulatory Guide 1.200 and the currently available PRA standards.

The framework provides methods to help ensure PRA quality, including establishment of PRA consensus standards that provide supporting requirements to the proposed high-level requirements, an independent peer review process, Regulatory Guides and Standard Review Plan guidance to assess PRA quality, and guidance on how to perform specific aspects of an advanced reactor PRA. The use of PRAs in the licensing and operation of new reactors will require that PRAs be living documents.

2.7 Process for Development of Technology-Neutral Requirements

The design objectives are linked to the protective strategies to develop technology-neutral requirements for new reactor concepts. These requirements, being technology-neutral, are compatible with acceptable safety performance for existing LWRs. Technical regulations and administrative regulations, organized by design, construction, and operation, will be developed from the requirements in order to anticipate and neutralize potential challenges that could prevent the risk objective from being achieved. Of course, the concern during design and construction is to control those aspects of each that could have positive or negative impacts on the risk during operations. Traditionally, NRC regulations and practices have ensured public health and safety is not compromised by commercial nuclear power plant operation by requiring the use of good :

- design practices,
- construction practices, and
- operational practices.

NRC's role has been to specify requirements associated with each of these three elements of "good practice," and through review, approval, and oversight, to monitor and judge a licensee's compliance with these requirements. Regulations for new plant licensing would also embody these good practices. In addition, they would enjoy the simplifying and focusing advantage of having the process structured to use risk insights throughout the process. The emphasis given to

each aspect will be developed according to how they address the threats that challenge one or more of the protective strategies and how they ensure meeting the safety/risk objectives and design/ construction/operation expectations.

The process for developing technical and administrative requirements from the protective strategies is outlined in Figure 2-5 and explained fully in Chapter 8. It begins with the protective strategies themselves. Then a deductive analysis of the logic of events that can defeat each protective strategy is performed. This leads directly to the questions staff must ask to ensure each protective strategy is accomplished. As a final check, the questions and answers are benchmarked against criteria for LWRs in 10 CFR Part 50, IAEA Standards, and other available historical information as a check on completeness. Finally, the answers to the questions are formulated as topics to be addressed in risk-informed, performance based requirements.

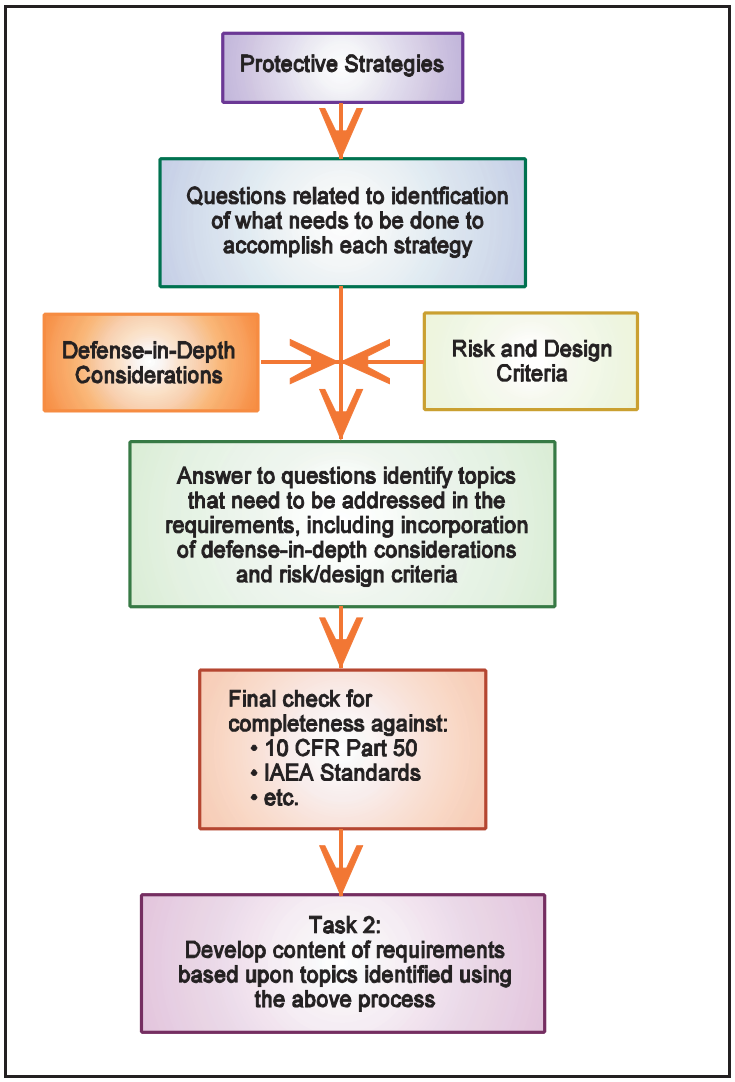

Figure 2-5 Process for Developing Technical and Administrative Requirements from the Protective Strategies

2.8 Summary: A Risk-Informed, Performance-Based, Technology-Neutral Framework Roadmap

This chapter has provided an introduction to the complete framework. The discussions of this chapter are summarized in the roadmap of the framework sketched in Figure 2-6.

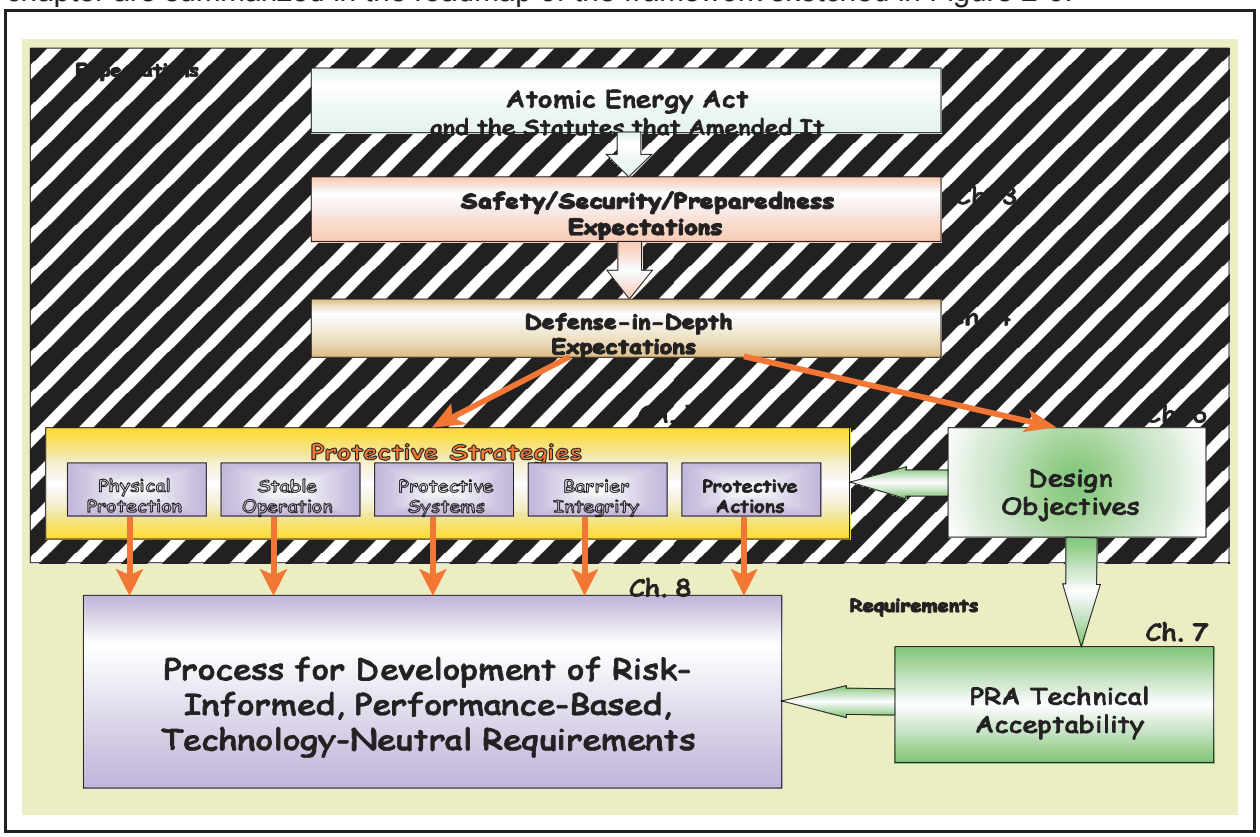

Figure 2-6 The Risk-Informed, Performance-Based, Technology-Neutral Framework Roadmap

How the elements and chapters of the framework relate and that defense-in-depth is comprised of two complementary approaches is shown:

- The Design Objectives approach sets frequency limits on the possible consequences of accidents to ensure that the NRC's safety goals are met. It also provides accident mitigation criteria, probabilistic criteria for the selection of events which must be addressed in the design and which constitute "licensing basis events," and probabilistic criteria for establishing the safety classification of systems, structures and components.

- The Protective Strategies are the safety fundamentals for safe nuclear power plant design, construction, and operation. They serve as the fundamental building blocks for the development of technology-neutral requirements and regulations. Acceptable performance in these protective strategies provides reasonable assurance that the overall mission of adequate protection of public health and safety is met.

The defense-in-depth features of the protective strategies and the combination of design and operations objectives and PRA technical acceptability lead to the establishment of technical

requirements that are technology-neutral. Administrative requirements[2.6] are also developed to ensure that the bases for the technical regulations (risk calculations, plant conditions, and other assumptions) are sound and do not degrade over time.

Protective strategies and administrative requirements take a protective, rather than an analytical approach. They directly address the questions: What if the models are wrong, at least in particular situations, or are incomplete? What if the assumptions are wrong or degrade with time? Requiring multiple Protective Strategies, regardless of the results of PRA analyses, provides protection against uncertainty in models and completeness. Even if our first layer of defense fails, additional layers are present to provide backup. Implementation of the Protective Strategies relies on the goal of independence to avoid vulnerability to the same source of uncertainty.

Within each protective strategy an approach can be taken that specifies certain deterministic requirements to help account for completeness uncertainties and probabilistic requirements to help guide the treatment of quantified uncertainties. Likewise the Administrative Requirements provide extrinsic control over the system: establishing rules for analysis; inspection requirements to identify degradation before failures occur; and tests to ensure that the as-built, operating facility is true to the designers' expectations. Results of the PRA and the sensitivity studies help in the evaluation of the necessary defense-in-depth in a risk-informed structure.

[2.6] Note that administrative requirements apply to all aspects of the framework: Protective Strategies, Design Objectives, Defense-in-Depth, and Technical Requirements in all life cycle phases of design, construction and operation.

3. SAFETY, SECURITY AND PREPAREDNESS EXPECTATIONS

3.1 Introduction

The purpose of this chapter is to delineate the expectations for safety, security, and preparedness required at future plants licensed by the NRC. The chapter's place in the structure of the framework document is indicated in Figure 3-1.

The framework integrates the expectations for safety, security, and preparedness to achieve the overall level of safety demanded by the NRC. The approach requires that safety and security assessments realistically model plant and preparedness response and that the results of these assessments are part of technology-neutral regulatory requirements. The entire process ensures that safety and security design issues are addressed early in the design development and regulatory review process so that the resulting design relies more on inherent design characteristics and features and less on extrinsic operational safety and security programs. The Framework is designed to ensure meeting the NRC's safety and security expectations on a technology-neutral basis, i.e., a licensing basis that can be applied to all new plants, regardless of technology.

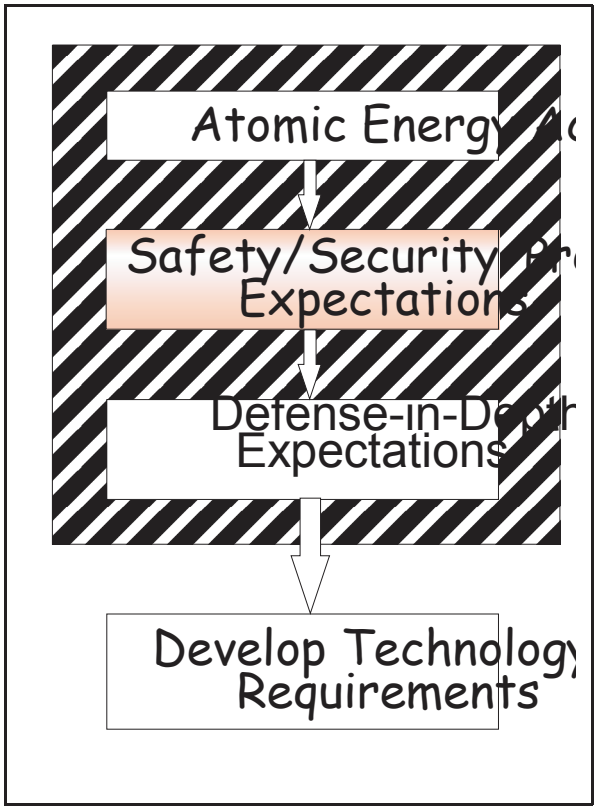

Figure 3-1 Structure of the Framework

The NRC's ***safety expectations*** are anchored in the safety goals, which seek to minimize additional risk burden to the population for the benefits of nuclear power. These underlying ideas are as appropriate for future reactors (or any new technology) as they are for existing LWRs. The development of the NRC's ***security expectations*** are elucidated in "Security Design Expectations for New Reactor Licensing Activities" [SECY 05-0120]. The approach anticipates that establishment of security design aspects early in the design process will result in a more robust and effective intrinsic security posture and less reliance on extrinsic operational security programs. New reactors must be protected at least as well as currently operating plants.[(2.7)] The NRC's ***preparedness expectations*** include the necessity for an emergency planning and preparedness capability, regardless of reactor technology or design.

[(2.7)] February 25, 2002, All Operating Reactor Licensees, Order Modifying License (Effective Immediately), EA-02-26, 67 FR 9792 (March 4, 2002); April 29, 2003, All Operating Reactor Licensees, Order Modifying License (Effective Immediately), EA-03-086, 68 FR 24, 517 (May 7, 2003).

3.2 Safety Expectations

3.2.1 Level of Safety

The level of safety that future reactors are expected to meet are the risk objectives, i.e., the quantitative health objectives (QHOs), embedded in the NRC's safety goal policy.

The Commission in their Policy Statement on "Regulation of Advanced Nuclear Power Plants," noted two expectations:

(32) that advanced reactors will provide enhanced margins of safety

(33) that advanced reactor designs will comply with the Commission's safety goal policy statement.

In order to illustrate the relation of the safety goal risk objectives to future plant licensing, and to address the Commission's expectations, a 3-region approach to risk acceptance is developed and defined as illustrated in the *conceptual diagram* of Figure 3-2.

Such a 3-region approach to risk acceptance for nuclear power plants, including operating reactors, has been discussed and employed in a number of forums. [Ref. 2.1] In considering this figure, the substantial uncertainty (see Chapter 4 for a discussion of uncertainty) in a plant's risk performance is taken into account. Conceptually, the lowest region represents the value of the risk metric that corresponds to the desired safety goal and/or risk objective. This region defines what is "safe enough", i.e., a region in which further safety enhancements are not needed. .[2.8]

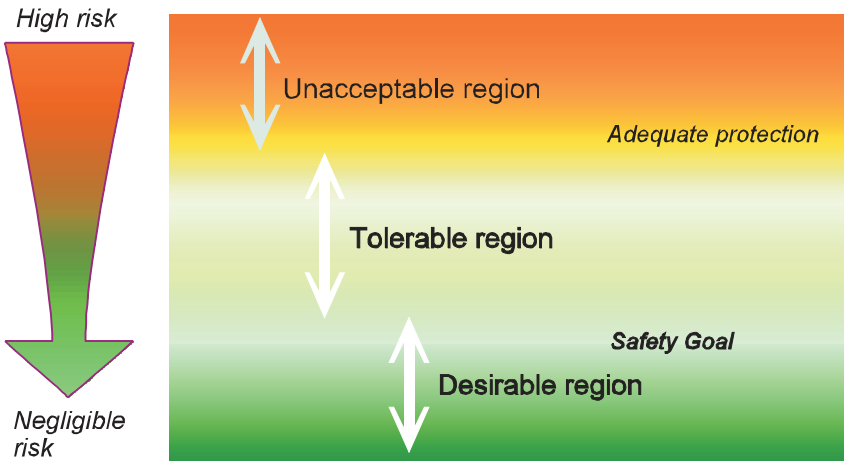

Figure 3-2 Three Region Approach to Risk Tolerability/Acceptance

The objective of the framework is to help develop requirements for future reactors that are consistent with the risk lying in the lower, desirable, risk region, i.e., requirements that will ensure

[2.8]Note that Figure 3-2 is conceptual in nature. The detailed considerations that would be necessary to implement this idea on a quantitative basis are discussed in Chapter 6.

there is only a small chance that the risk will extend into the tolerable region and essentially zero chance that it reaches the upper, unacceptable region. Accordingly, ***the technology-neutral regulatory requirements for new reactors are established to keep the risk in the desirable region, that is, the regulations are written to achieve the safety goal level of safety.*** The rationale for these requirements is twofold: they provide enhanced margins to account for uncertainties, in particular, those that may be associated with new designs and technologies, and they help implement the Commission's expectations for enhanced safety as expressed in the Advanced Reactor Policy Statement.

Adoption of the QHOs as the basis for the level of safety implies an increase in safety for future reactors compared to current LWR designs. However, the QHOs have been used to assess current LWR vulnerabilities and safety improvements have been made, where justified. Accordingly, current reactors are more safe than required by the letter of the regulations and, in many cases, achieve a level of safety comparable to the QHOs. Therefore, developing requirements that make the level of safety correspond to the QHOs ensures that future plants "comply with the Safety Goal Policy Statement" as stated in the Commission's policy statement on "Regulation of Advanced Nuclear Power Plants" and imparts stability and consistency to the regulatory process. Finally, the framework approach is consistent with industry initiatives which are directed at developing designs with enhanced safety over currently operating plants.

Note too that, given that new plants meet this enhanced level of safety, if they are added to sites with an existing reactor(s), they will add little risk to the site. Therefore, adding new plants with low risk to sites with older, but still adequately safe, plants should be permitted and may have the benefit of familiarity with the site that has been established over many years.

The above discussion should not be taken to imply that comparing a plant's safety profile to the QHOs can be accomplished with little uncertainty. The current PRA technology is relatively mature for estimating the risk from internal events for LWRs operating at full power. Techniques for estimating the risk related to fire, external events and other modes of operation for these types of reactors are less mature. Furthermore, for non-LWRs the state of the art in PRA is less advanced than for LWRs. Finally, estimating the risk from deliberate adversarial acts of theft, sabotage, and/or attack is very difficult. All these factors argue for the need to compensate for the significant uncertainties encountered in comparing the plant safety profile to the QHOs via the 'margins' implied in Figure 3-2 between adequate protection and the safety goals, and by the application of defense-in-depth as discussed in Chapter 4 of this report.

3.2.2 Implementing the NRC's Safety Expectations

With the level of safety expressed in terms of risk, PRA plays a significant role in the framework. With the framework approach the PRA information is used during the design stage and for selection of licensing basis events (LBEs) and safety significant systems, structures and components (SSCs). Therefore the scope of the PRA used encompasses the whole spectrum of events that credible occur during the life of the plant: normal operation, as well as frequent, infrequent and rare initiating events and accident event sequences. This is a broader scope than that used currently for LWR risk analysis, which concentrates on beyond design basis accidents, i.e. accidents leading to severe core damage.

For current LWRs the risk examined is almost always expressed in terms of the surrogate or subsidiary risk objectives: core damage frequency (CDF) and Large Early Release Frequency (LERF). One reason why CDF and LERF provide adequate risk metrics for the current LWRs is

that it can be demonstrated[2.9] that these parameters, viz., CDF and LERF, can be used as surrogate metrics for the NRC's safety goal QHOs. For new, non-LWR types of reactors, however, not only will the quantitative values for CDF and LERF be no longer applicable, CDF itself may no longer be a useful risk metric.

From a technology-neutral point of view the universally applicable risk metrics are ones which either express consequences directly or which can be linked to consequences without technology-specific metrics. Dose to the public from radiological releases is an example of a metric that is closely linked to consequences, and therefore is one of the parameters the results of the PRA can be expressed in. In addition, since frequent, infrequent, as well as rare events are included in the PRA, a single limiting criterion (such as CDF for LWRs) is not adequate. Instead, a criterion that specifies limiting frequencies for a spectrum of consequences, from none to very severe, needs to be established. This can be denoted via a frequency consequence (F-C) curve, (which provides guidance to a plant designer)[2.10] an example of which is shown in Figure 3-3. As explained in more detail in Chapter 6, the F-C curve shown relates the frequency of potential accidents to acceptable radiation doses at the site boundary from these accidents. It is based on, and derived from, current regulatory requirements in Parts 20, 50 and 100. 10 CFR Part 20 limits the radiation doses from licensed operation to individual members of the public. 10 CFR Part 50 Appendix I identifies design objectives for releases during normal operation to be as low as reasonably achievable (ALARA). Part 50.34 requires an applicant for a license for a power reactor to demonstrate that doses at the site boundary (and the outer boundary of the low

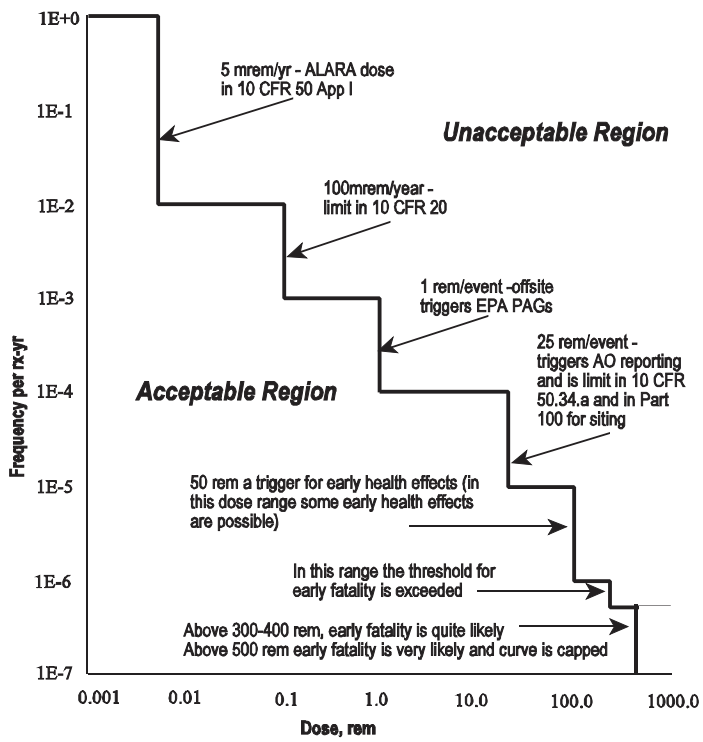

Figure 3-3 Frequency-Consequence Curve

[2.9] CDF and LERF were found to be surrogates for the QHOs for LWRs based on the amount and characteristics of the radionuclide inventory in currently operating LWRs, the timing and magnitude of potential releases in severe accidents at these plants, and the anticipated and planned emergency response of the nearby offsite population to these releases at operating sites.

[2.10] Whether the F-C curve applies to a single reactor or to the site as a whole is a matter of policy. It also depends on whether the focus is on a new 10 CFR Part 50, which relates to a single reactor, or whether the focus is on Part 100, which relates to the whole site.

population zone) from hypothetical accidents will meet specified criteria and 10 CFR Part 100 has similar dose criteria for determining site suitability. The principle underlying the F-C curve is that event frequency and dose are inversely related, i.e., the higher the dose consequences the lower is the allowed event frequency.

The sequences of the PRA populate the space under the F-C curve. Some scenarios will have little or no consequences, primarily because of the inherent characteristics and design features of the plant. Others are likely to approach the F-C curve and thus make up the important contributors to the plant risk profile. To be acceptable, the results of the PRA, in terms of the frequency and consequences of all the accident sequences examined, must lie in the acceptable region, (i.e., below) the F-C curve. With the curve of Figure 3-3 accident sequences that lie below the F-C curve will also satisfy the QHOs of the safety goal policy individually. Note that meeting the F-C curve imposes additional constraints in addition to satisfying the QHOs because specific dose limits are imposed at all frequencies.

In addition to meeting the consequence limits of the curve individually, the PRA sequences also have to meet the QHOs in the aggregate. This means the PRA results must demonstrate that the sum total of the integrated risk over all of the accident sequences in the PRA must satisfy both the latent cancer QHO and the early fatality QHO. The safety goals and consequently the QHOs are phrased in terms of the risk to an 'average' individual in the vicinity of (or 'area near') a nuclear power plant. The latent cancer QHO is defined in terms of the risk to an average individual within 10 miles and the early fatality QHO in terms of the risk to an average individual within 1 mile of the plant. The risk in the safety goals is the total risk per reactor year, summed over all accident sequences.

Note that with the kind of acceptance criterion for individual sequences described above, an accident sequence is acceptable even though it has a dose at the boundary associated with it, as long as its frequency does not exceed the limit for that dose, as specified by the F-C curve. For current LWR PRAs a single limiting frequency, associated with high consequence event sequences, is the acceptance criterion. For the PRAs required here, whose scope covers all types of off-normal event sequences, the criterion is a series of limiting frequencies whose value depends on the associated consequences; frequent event sequences must lead to no consequences or very minor ones; infrequent event sequences can have somewhat higher doses associated with them, and rare events can have higher consequences still. It should be noted that for specific technologies it may be possible to eventually develop surrogate metrics (such as CDF and LERF for LWRs) for the dose parameter, along with acceptable values for such surrogates. However, it will likely take some time to obtain the experience from testing and operation to have confidence in such surrogates.

In summary, in the framework approach to licensing a PRA is used to generate a sufficiently complete set of accident scenarios whose frequencies and consequences, individually and in the aggregate, provide an estimate of the overall risk profile of the plant. The framework advocates a PRA as the best available analysis method for showing how the interactions and dependencies among SSCs, human actions, and potential plant hazards can result in accident sequences being initiated, prevented, and mitigated. The scope and nature of the PRA will differ from the current LWR PRAs. Uncertainties must be addressed in the calculation of both frequencies and consequences of the accident scenarios. Since the accidents include rare events postulated to occur in complex systems for which limited experience exists, the consideration of uncertainties are a vital part of understanding the extent of the risk (and of selecting the LBEs). In addition to meeting a suitable F-C curve, the PRA information is used to select LBEs and safety significant SSCs.

3.2.3 Subsidiary Risk Objectives

The Commission's overall expectation for protection of public health and safety from accidents resulting from NPP operation is expressed in its 1986 Safety Goal Policy Statement. The goal of the framework for new plant licensing is to ensure that new plants achieve a level of safety at least equivalent to that expressed by the Safety Goal Policy Statement. For currently operating LWRs, subsidiary objectives related to core damage prevention and accident mitigation, (i.e., core damage frequency (CDF) and large early release frequency (LERF) or conditional containment failure probability (CCFP), have been developed and used as surrogates for the quantitative health objectives (QHOs) expressed in the Safety Goal Policy Statement (i.e., $2x10^{-6}$/ry individual risk for latent fatalities and 5×10^{-7}/ry individual risk for early fatalities). These subsidiary objectives focus on plant design and have eliminated the need for carrying out probabilistic consequence analysis in PRAs for currently operating LWRs.

These LWR specific subsidiary risk objectives have been used as the basis for various risk-informed activities for currently operating plants. The numerical values used for these surrogates (10^{-4}/ry for CDF, 10^{-5}/ry for LERF, and 0.1 for CCFP) are based upon the characteristics and risk analysis associated with currently operating light-water reactor plants (e.g., plant size, performance, source term, emergency preparedness) and their site characteristics (i.e., meteorology and population distribution). In effect, for current LWRs the 10^{-4}/ry CDF serves as a surrogate for the latent fatality QHO as well as a measure of accident prevention, and the 10^{-5}/ry LERF or 0.1 CCFP serves as a surrogate for the early fatality QHO for currently operating reactors. (See Appendix A for detailed discussion on derivation of surrogates for currently operating LWRs).

As discussed earlier, a frequency-consequence curve has been established to support achievement of the overall safety objective of the technology-neutral licensing approach and to define acceptance criteria for individual accident sequences in the PRA and for those accident sequences chosen as LBEs. This frequency-consequence curve is anchored in the safety goal QHOs and other existing requirements and is defined in terms of dose to an individual at specific distances that are defines in Chapter 6, e.g., the site boundary and the LPZ. Accordingly, a probabilistic consequence analysis is needed to implement the F-C curve. However, this frequency consequence curve is not a substitute for the QHOs which express goals for the cumulative latent and early fatality risk from accidents and also require a level 3 PRA analysis. Given the frequency-consequence curve and the QHOs, it is useful to ask: (1) if technology neutral subsidiary risk objectives would be useful as substitutes for the QHOs; (2) if so, how would they be used; and (3) what should they be?
Each of these is discussed below.

Although the frequency-consequence curve is anchored in the safety goal QHOs, it is not itself a measure of compliance with the QHOs (i.e., as mentioned above, the frequency-consequence curve is not an assessment of the cumulative risk from all event sequences considered in the design). Accordingly, to ensure the QHOs are met, either a probabilistic consequence assessment that calculates offsite early fatality and latent cancer risks is needed or, if possible, technology-neutral subsidiary risk objectives are developed that can account for the cumulative risk from all event sequences considered in the design and reduce the need for a probabilistic offsite consequence assessment . To be most useful, these subsidiary objectives should also focus more directly on plant design, thus simplifying the analysis needed.

Subsidiary risk objectives, if they can be defined in a meaningful technology-neutral way, can also be useful in defining the desired apportionment between accident prevention and accident mitigation (which is not defined by the QHOs or the frequency-consequence curve), as is done today for currently operating LWRs, via the use of CDF and LERF. Defining such a apportionment

quantitatively will be useful in implementation of the defense-in-depth principles discussed in Chapter 4.

It is envisioned that technology-neutral subsidiary risk objectives would be used in the following ways:

(1) as a simplified way to assess the design's compliance with the QHOs;

(2) as quantitative measures to implement the defense-in-depth principle on accident prevention versus mitigation;

(3) as the top level criteria for establishing reliability goals for protective systems and consistent with initiating event frequency;

(4) as a probabilistic counterpart to the deterministic criteria directed toward accident prevention (discussed in Chapter 6).

While CDF and LERF are acceptable subsidiary risk objectives for LWRs, this is possible due to the characteristics of LWR technology, in particular, the ways in which severe accidents can occur and the source terms related to these accidents. It is expected that subsidiary objectives for future reactors will, in general, be technology dependent and it is unlikely that surrogate measures similar to CDF and LERF could be identified on a technology-neutral basis.

3.3 Security Expectations

The NRC's security expectations are that new reactors shall have the same level of protection as established by the post 9/11 NRC requirements. [Ref. 2.2] [Ref. 2.3] There is a major difference in approach, for new plants, where security expectations will be evaluated integral with the design, rather than post-design compensatory measures. The amount of intrinsic protection and the ways in which it can be built into the design will depend on technology-specific features of the design. In general, NRC's expectations will be realized, when the regulations:

- Ensure health and safety and protect the environment
- Ensure the secure use and management of nuclear materials
- Ensure openness in the regulatory process
- Ensure that NRC actions are effective, efficient, realistic, and timely.

Note that the focus of the security expectations is on performance of the system, rather than on standards. Assessment is required, as well as development of requirements, to ensure performance is adequate. Security (physical protection) assessment involves characterization of the potential threat, the potential targets, and the potential consequences[(2.11)]. [Ref. 2.4] The likelihood of the threat depends on some factors only known to the adversary, so it is expected to be outside the scope of evaluations.[(2.12)] Nevertheless, the types, objectives, and capabilities, as

---

[(2.11)]This approach is adapted from technical conference papers, working notes, and a soon to be published methodology report of the Gen-IV International Forum Expert Group on Proliferation Resistance and Physical Protection. This group is called out in Reference 3-1.

[(2.12)]Of course, on a day-to-day basis, security experts make estimates of the threat based on the best available intelligence. The approach for design must address a range of threats and be flexible to provide protection regardless of the changing threat specifics.

well as the strategies, of the potential adversaries are taken into account in developing requirements. Detailed information about these threat descriptions is sensitive, because access to this information would allow potential adversaries to better predict the capabilities of physical protection systems.

During design, reasonable assumptions about the threat space that will apply over the full life of the facility can be made, together with a spectrum of threats the facility is likely to encounter. For the purposes of design and evaluation, it is most important that these threat assumptions include the broad categories of potential physical protection (PP) challenges.

The definition of a specific threat requires information both about the perpetrator of the threat, and about his strategy:

- type (e.g., outsiders, outsiders in collusion with insiders, and insiders alone),
- objectives (large-scale goals or aspirations), and
- capabilities

For physical protection the threat strategies include:

- radiological sabotage,
- material theft, and
- information theft.

Analysts investigate two broad classes of targets: material targets for theft of nuclear material, and equipment targets for attack, sabotage or theft of information. Targets are identified using a systematic process to ensure completeness. A number of approaches have been suggested for structuring such an analysis. Details of performing the systems level analyses to support the overall approach can be found in [Ref. 2.5], [Ref. 2.6], [Ref. 2.7], and [Ref. 2.8], as well as a number of other texts, papers, and classified or protected USNRC documents. Details of the approach are under development.

3.4 Preparedness Expectations

The NRC's basic preparedness expectation is to ensure the capability to effectively protect the public through dose-saving, should substantial amounts of radioactive material be released to the environment.

Criteria for determining the scope and nature of required offsite emergency preparedness measures are needed that address technology-specific factors, such as reactor size (power level), location, level of safety (i.e., likelihood of release), magnitude and chemical form of the radionuclide release, and timing of releases. Some conditions and considerations affecting the required response that have particular importance would include, but not be limited to, the following:

(1) consideration of the full range of accidents
(2) use of defense-in-depth
(3) prototype operating experience
(4) acceptance by federal, state, and local agencies

(5) acceptance by the public
(6) security considerations

In a more general and integrated sense, preparedness takes many forms and the NRC's preparedness expectations include preparedness with respect to safety and security. Both kinds of preparedness involve both on-site and off-site activities, as shown in Figure 3-4.

Integrated Preparedness

- Safety preparedness
  - On-site measures
    - main control room [EOPs and APs]
    - emergency response center [accident management guidelines]
  - Off-site emergency preparedness
- Security preparedness
  - On-site
    - Force-on-force
    - Plant design and operations
      - » Protected state
      - » Isolation
  - Off-site
    - emergency preparedness
    - police actions

Figure 3-4 Generalized Preparedness as Part of the Protective Actions Protective Strategy

Safety preparedness on-site involves the activities of both operators and plant management efforts to deal with conditions in the plant. It requires that operators are trained on the use of emergency and abnormal operating procedures and that these procedures are validated for the wide range of conditions under which they might be applied. Likewise senior supervisory personnel must understand the more conceptual accident management guidelines, exercise interactions with vendors, regulators, and other officials. Safety preparedness off-site involves traditional Emergency Preparedness fits within this structure.

Security Preparedness also has on-site and off-site elements. On-site activities include the preparedness of the guard force, maintenance of design features that enhance physical protection, and the operators readiness to isolate damaged equipment. Off-site security preparedness involves traditional Emergency Preparedness and also coordination with local and national police and first responder personnel.

This approach acknowledges that we need preparedness for both safety and security, both on-site and off site. It acknowledges that preparedness involves procedures and training, as well as hardware and software.

A key feature in preparedness is the application of a graded approach in which response plans and procedures are tailored to the hazard or threat they are meant to neutralize or effectively respond to.

3.5 Integration of Safety, Security, and Preparedness

Safety, security, and preparedness are never addressed independently; they operate in an integrated manner to preserve the overall protection of the public. For example, whenever security requirements are developed, their impact on safety and preparedness must be examined. As a further example, security requirements do not limit the ability for preparedness in protecting plant safety and the health and safety of nearby populations. From the beginnings of the design process, security and preparedness implications of design decisions are integrated with more traditional safety decisions.

Analyzing security in the design process results in a more robust, intrinsic security posture and less reliance on extrinsic, operational security programs. A consistent integration of safety and security using PRA methods and technology can provide a rational basis for decision-making by infusing

safety objectives with security concerns. Inclusion of preparedness in all aspects of safety and security integration leads to a plant that is safe and robust against all internal and external hazards and inadvertent and advertent threats and meets the NRC objectives of protecting the public health and safety and the common defense and security.

The approach for generating technology-neutral licensing requirements for safety, security and preparedness expectations is described in Chapter 5 as a process for moving from protective strategies (e.g., protective actions) to the generation of requirements to protect against those challenges, as shown in Figure 3-5.

Figure 3-5 Process for Developing Requirements

The protective strategies are developed in Chapter 5. The approach for identifying potential challenges is a deductive one using logic trees similar to fault tree analysis used in PRA. That analysis is carried out in Chapter 8, where the process of developing the associated requirements is explained and carried out.

4. DEFENSE-IN-DEPTH: TREATMENT OF UNCERTAINTIES

4.1 Introduction

The purpose of this chapter is to discuss the approach used for the implementation of defense-in-depth for new reactors. The core of the NRCs safety philosophy has always been the concept of defense-in-depth, and defense-in-depth remains basic to the safety and security expectations of the technology neutral framework. The ultimate purpose of defense-in-depth is to compensate for uncertainty. This includes uncertainty in the type and magnitude of challenges to safety, as well as in the measures taken to assure safety. Figure 4-1 schematically indicates the relationship of defense-in-depth to the rest of the structure of the Technology Neutral Framework.

The March 1999 Commission White Paper on risk-informed and performance-based regulation states that, *"Defense-in-depth is an element of the 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."* In its discussion on risk-informed approach and defense-in-depth the White Paper further states, "Although 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."

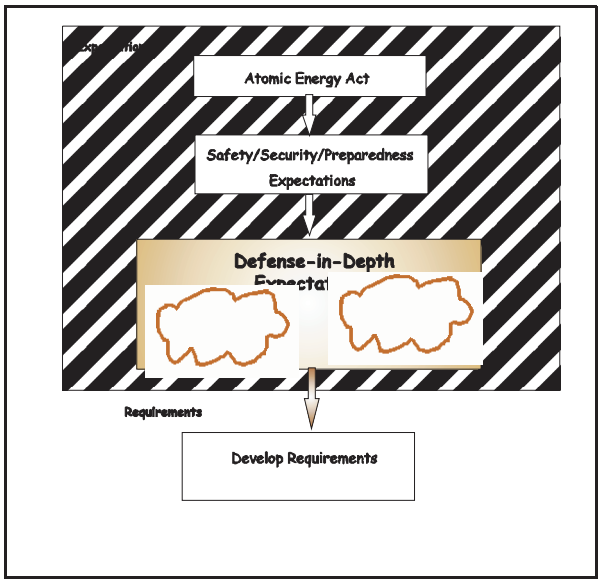

Figure 4-1 Framework Approach to Defense-in-Depth

In a broad sense, the objective of defense-in-depth is to ensure that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. This objective should always apply, except where the public health and safety consequences of the regulated activity and their uncertainties are small. This chapter discusses the implementation of defense-in-depth for new reactors and is based upon the following principles, which address the scope and approach taken for defense-in-depth:

36. both intentional acts and inadvertent events should be considered

37. measures for both accident prevention and mitigation should be provided

38. the accomplishment of key safety functions should not be dependent upon a single element of design, construction, maintenance or operation

39. uncertainties in equipment and human performance should be accounted for in meeting reliability and risk goals

40. low probability but credible events are considered in providing containment functional capabilities to meet onsite and offsite radionuclide dose acceptance criteria

41. regulated activities should be conducted at locations that facilitate protection of public health and safety.

Defense-in-depth measures associated with these principles (e.g., redundancy, diversity, safety margins) are also discussed. Redundancy enhances the reliability of independent means; diversity (and separation) generally provide protection against dependent (common cause) failures of multiple means. Physical safety margins ensure that the capacities of hydraulic, electrical and structural components are in excess of minimum requirements, so unanticipated increases in demand can be met. Temporal safety margins ensure preventive systems and operator actions can correct for deviations even after some initial lapses.

Safety analysts [Ref. 2.9] have pointed out that the key to safe operations in any activity is a focus on managing the "unexpected." The concept of defense-in-depth is essential for successfully coping with unexpected and uncertain events. Managing the unexpected includes identification, evaluation, and management of uncertainties. In licensing new reactors, the treatment of uncertainties will play a key role in ensuring safety limits are met and the design is robust with respect to unanticipated factors. In general, uncertainties associated with new plants will tend to be larger than uncertainties associated with existing plants due to new technologies being used, the lack of operating experience or, in the case of some proposed plants, new design features (e.g., increased use of passive systems). Any licensing approach for new plants must account for the treatment of these uncertainties.

Uncertainties have always been a factor to contend with in the safe operation of nuclear power plants, and, as stated in Regulatory Guide 1.174, “The defense in depth philosophy .....has been and continues to be an effective way to account for uncertainties in equipment and human performance.” Note, however, that the defense-in-depth discussed in Regulatory Guide 1.174 is focused on currently operating plants, where defense-in-depth has been well established and confirmed by extensive operating experience. Regulatory Guide 1.174 is primarily concerned with maintaining defense-in-depth when contemplating changes to the licensing basis of an existing plant. For new reactors the challenge is somewhat different: Establishing what constitutes an adequate level of defense-in-depth in the new reactor designs. In laying the groundwork for defense-in-depth for new reactor designs, analysts can benefit from the experience of past designs, but at the same time must be willing to re-examine conclusions based on existing designs and consider new alternatives.

A powerful tool in the search for the unexpected and the identification of uncertainties is Probabilistic Risk Assessment (PRA). PRA’s original purpose was exactly this kind of search and identification. (With repeated application to current plants that resemble each other, what was originally creative about PRAs has become routine.) Much of the work of PRA for new reactors will be to identify and evaluate initially unexpected scenarios. While PRA cannot compensate for the unknown and identify all unexpected events or event sequences, it can: (1) identify some originally unforseen scenarios, (2) identify where some of the uncertainties lie in the plant design and operation, and, for some uncertainties, (3) quantify the extent of the uncertainty, and therefore lead to a safer plant design. Therefore, PRA has a role to play, along with deterministic considerations, in establishing what constitutes adequate defense-in-depth.

PRA can quantify parameter uncertainty associated with the basic data used in the plant model. It can also address, to some extent, the model uncertainty associated with the analytical physical models and success criteria that appear because of modeling choices. For these uncertainties, that are able to be quantified, PRA can provide an indication of how much defense-in-depth, including margin, is needed to compensate for uncertainty to ensure safety.

Uncertainty associated with limitations in knowledge, such as unknown or unforeseen failure mechanisms, or unanticipated physical and chemical interactions among system materials, cannot

be identified by PRA. Defense-in-depth measures to address this type of uncertainty can be established from requirements that result from repeatedly asking the question, "What if this barrier, measure, or safety feature fails?" without a quantitative estimate of the likelihood of such a failure, as well as by ensuring consistency with established defense-in-depth principles. This is the approach to defense-in-depth that invokes specific deterministic provisions to compensate for the unexpected.

The aim of the framework is to develop an approach to defense-in-depth for new reactors which is consistent with the successful past practices used for operating reactors, but which improves on past practices by being more consistent and by making use of quantitative information where possible. As described in the remaining sections of this chapter, the framework's defense-in-depth approach is one which combines deterministic elements with probabilistic ones.

A paper dealing with defense-in-depth has grouped past approaches to applying defense-in-depth into two basic types: a more or less deterministic approach, referred to as the structuralist approach, and an approach that includes probabilistic assessments of uncertainty, referred to as the rationalist approach [Ref. 2.10]. According to the deterministic model defense-in-depth is embodied in the structure of the regulations and in the design of the facilities that are built in accordance with those regulations. The requirements for defense-in-depth result from repeatedly asking the question, "What if this barrier or safety feature fails?" regardless of the quantitative estimate of the likelihood of such a failure. Therefore, a characteristic of this approach is that a some reliance on each of the high level lines of defense is maintained; accident prevention alone cannot be relied on to reach an acceptable level of safety. This is the approach to defense-in-depth that has traditionally been used to achieve adequate protection. The elements of this deterministic, or structuralist, approach address primarily completeness uncertainties.

In the probabilistic model defense-in-depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. The probabilistic approach acknowledges PRA as a powerful tool in the search for the unexpected and the identification of uncertainties. Although PRA cannot compensate for the unknown and identify all unexpected events, this approach uses risk assessment to: (1) identify some originally unforseen scenarios, (2) identify where some of the uncertainties lie in the plant design and operation, and, for some uncertainties, (3) quantify the extent of the uncertainty. This approach recognizes that PRA can identify and quantify parameter uncertainty associated with the basic data used in the plant model, and can also address, to some extent, the model uncertainty associated with the analytical physical models and success criteria that appear because of modeling choices. The probabilistic approach seeks to evaluate the uncertainties in the analysis and to determine what steps are to be taken to compensate for those uncertainties. The adequacy of the defense-in-depth measures can be assessed in the probabilistic approach via quantitative criteria that appear in safety goals or more general frequency/consequence curves. The elements of the probabilistic approach address primarily modeling and parameter uncertainties and allow an estimate of how much defense-in-depth, including margin, is needed in these areas.

The two principal deterministic defense-in-depth elements of the framework approach are: (1) assuring the implementation of all of the five protective strategies introduced in Chapter 2 and discussed in detail in Chapter 5 (Physical Protection, Stable Operation, Protective Systems, Barrier Integrity, and Protective Actions), and (2) ensuring that the defense-in-depth principles, discussed in Section 4.4, are followed to develop licensing requirements. The protective strategies were selected based on engineering judgment, as a minimal set to provide protection with respect to lines of defense against accidents and exposure of the public and environment to radioactive material . As described in Section 4.3, the defense-in-depth principles are established by

examining the different kinds of uncertainties to be treated, and incorporating successful past practices and lessons learned related to defense-in-depth.

The probabilistic elements of the framework's defense-in-depth approach consist of using the PRA, to the extent possible, to search for and identify unexpected scenarios, including their associated uncertainties, and to subsequently establish adequate defense-in-depth measures, including safety margins, to compensate for those scenarios and their uncertainties which are quantified in the PRA model. The ability to quantify risk and estimate uncertainty using PRA techniques, where possible, and taking credit for defense-in-depth measures in risk analyses, allows one to provide a better estimate of how much defense-in-depth is enough. In this manner PRA complements defense-in-depth.

The remainder of this Chapter is organized as follows: In Section 4.2 the types of uncertainties that need to be defended against are described. Objectives for defense-in-depth and the subsequent defense-in-depth principles are detailed in Section 4.3. The integrated framework approach to defense-in-depth is outlined in Section 4.4, and the process for applying the approach is described in Section 4.5.

4.2 Types of Uncertainty

Uncertainties have generally been categorized into random, or stochastic uncertainty (sometimes referred to as aleatory) and state-of-knowledge uncertainty (sometimes referred to as epistemic [Ref. 4-2]. Random uncertainty arises from the fact that events or phenomena occur in a random or stochastic manner, such as a pump failing to start due to a random failure. Random uncertainty is sometimes called irreducible uncertainty because, in principle, it cannot be further reduced by additional empirical studies. However, additional study may lead to a better characterization, for example in terms of its magnitude, of the random uncertainty. Random uncertainty is well suited to analysis via probability theory and this type of uncertainty is usually addressed in PRAs because it is embedded within the structure of the probabilistic models used to describe the occurrences of these events.

State-of-knowledge uncertainty arises from a lack of knowledge or lack of scientific understanding that may be due to a variety of factors, such as the inability to make observations, measurement uncertainty, the prohibitive cost of investigating a phenomena, etc. State-of-knowledge uncertainty can be reduced, at least in principle, by additional study (theoretical research, experiments) or improved study techniques. Random and state-of-knowledge uncertainties are often intertwined and may be difficult to distinguish: measurement uncertainty usually has a random component; some apparent randomness may prove to be state-of-knowledge after closer examination. The state-of-knowledge uncertainties that need to be accounted for in a PRA fall into three basic categories:

- ***Parameter uncertainty*** is the uncertainty associated with basic data used in safety analysis such as failure rates, ultimate strength, etc. Part of parameter uncertainty is already included within random uncertainty, such as the beta or error factor; however, another part such as the limitations in data affecting the choice of failure distribution may be characterized as state-of-knowledge uncertainty. Parameter uncertainties are those associated with the values of parameters of the PRA models. (Note that the fact that a pump may or may not start is a random process, while determining the values to assign to the probability model for that failure event is a state-of-knowledge uncertainty.) Parameter uncertainties are typically characterized by establishing probability distributions on the parameter values. These distributions can be interpreted as expressing a degree of belief in the values these

parameters could take, based on current knowledge and conditional on the underlying model being correct.

- ***Model uncertainty*** is the uncertainty associated with the data limitations, analytical physical models and acceptance criteria used in the safety analysis. PRA models, as well as those used in traditional deterministic engineering analyses, are composed of models for specific events or phenomena. Often the state of knowledge regarding these events and phenomena is incomplete and there are varying expert opinions on how particular models should be formulated. Such uncertainties arise, for example, in modeling human performance; common cause failures; mechanistic failures of structures, systems and components; high temperature fuel phenomena; and large radionuclide releases. While some model uncertainties will apply over a large number of technologies, each particular technology will have its own special model uncertainties. Therefore ,model uncertainties have to be identified at the technology-specific level as well. Model uncertainties are large where phenomena are poorly understood or not well characterized. It is important to understand the model uncertainties inherent in a particular PRA prediction for any new reactor design and how they are treated in terms of the available defense-in-depth elements.

- ***Completeness uncertainty*** is the uncertainty associated with factors not accounted for in the safety analysis such as safety culture, unknown or unanticipated failure mechanisms, etc. Completeness uncertainty can be regarded as one aspect of modeling uncertainty, but because of its importance is usually discussed separately. In one sense, it can be considered a scope limitation. Because completeness uncertainty reflects the unanalyzed contribution to risk it is difficult to estimate its magnitude, and this can translate to difficulties estimating the true magnitude of the overall risk. Completeness uncertainty refers to things that are not modeled because of:

  (1) *Intentional exclusion from the scope*. This includes risk contributors that can be modeled but are excluded for reasons of time, cost, etc., and/or a belief that their risk contribution for the analysis performed is negligible or can be adequately bounded. Some prominent examples are the risk from external events and/or accidents at low power and shutdown for some plant specific analyses.

  (2) *Lack of knowledge*. This consists of the truly unknown and unexpected that remains after available (and practical) analytical and experimental methods have been exhausted. This uncertainty is made up of: a) risk contributors (e.g., initiators and accident scenarios) that have not been conceived, and b) considerations for which adequate methods of analysis have not been developed, for example, heroic acts and influences of organizational performance. It is this type of uncertainty which is most difficult to address in terms of what is adequate defense-in-depth. As noted in the Introduction to this Chapter, defense-in-depth measures to address this type of uncertainty cannot be established via specific deterministic or probabilistic analysis, but instead rely on adherence to well thought out defense-in-depth principles and from repeatedly asking the question, “What if this barrier or safety feature fails?”

4.3 Defense-in-Depth Objectives and Principles

As stated in the introduction to this chapter, the ultimate purpose of defense-in-depth is to compensate for uncertainty. All of the uncertainties described above can arise in the analysis of the challenges to safe operation, and in the design of actions and equipment to assure safety. As noted, uncertainties related to lack of knowledge are the most difficult to deal with. Based on these

considerations, the purpose of defense-in-depth can be expressed with the objectives shown below. Defense-in-depth is the ability to:

- compensate for uncertainties, including events and event sequences which are unexpected because their existence remained unknown during the design phase,

- compensate for potential adverse equipment performance, as well as human actions of commission (intentional adverse acts are part of this) as well as omission,
- maintain the effectiveness of barriers and protective systems by ensuring multiple, generally independent and separate, means of accomplishing their functions, and

- protect the public and environment in the event that these barriers are not fully effective.

The first objective emphasizes the importance of providing some means to counterbalance unexpected challenges. The second objective addresses uncertainty in equipment and human actions. It encompasses equipment design and fabrication errors, as well as both deliberate acts meant to compromise safety, and errors or inadequacy in carrying out procedures meant to assure safety. The third objective addresses the uncertainty in the performance of the systems, structures, and components (SSCs) that constitute the barriers to radionuclide release, as well as in the SSCs whose function it is to protect those barriers. The final objective emphasizes the concept of layers of protection, in that it addresses the need for additional measures should the barriers to radionuclide release fail after all.

Much can be learned from the successful past applications of defense-in-depth. The most well known is the use of multiple physical barriers , exemplified in current reactors by the fuel elements and cladding, reactor coolant system pressure boundary and containment systems and structure to prevent the release of significant quantities of radionuclides to the environment. The application here has also included the design of redundant and diverse independent active and passive systems which protect the integrity of these barriers.

Recurrent themes in applications of defense-in-depth are (1) do not rely on one element of design no matter how confident, and (2) guard against the unexpected, i.e., don't assume accidents will start and play out in the analyzed way. These themes of defense-in-depth have been applied in various ways. Redundant or diverse, generally independent, means are usually used to accomplish key safety functions, such as safe shutdown or removal of decay heat. Redundancy enhances the reliability of independent means; diversity (and separation) generally provides protection against dependent (common cause) failures of multiple means, and therefore some assurance that safety functions can be accomplished successfully despite the uncertainty in the mechanism of dependent failures. In some advanced designs additional emphasis is given to inherent reactor characteristics and passive features that minimize the potential for radionuclide release and reduce barrier failure modes, even for unanticipated accident scenarios, as ways of assuring safety functions are accomplished. In these designs safety functions may be achieved by inherent natural processes such as shutdown due to negative reactivity feedback, or decay heat removal through conduction and radiation to surrounding structures, and retention of fission products in high integrity fuel particles. While the discussion of defense-in-depth often uses examples related to the reactor, it is important to remember that defense-in-depth has to address all the radionuclide related hazards in the whole plant.

Defense-in-depth measures have been embodied in SSCs, in procedures (including accident management plans to protect the offsite public), or in the choice and design of the basic processes that promote safety (e.g., negative temperature coefficient of reactivity).

Based on these past defense-in-depth practices and lessons learned from operating experience, security assessments, and the consideration of the various uncertainties that are to be dealt with, a set of defense-in-depth principles has been established. To assure public safety despite uncertainties in knowledge or rigor, the first general principle of defense-in-depth is that:

(1) ***Measures against intentional as well as inadvertent events are provided.***

This principle assures that defense-in-depth measures are applied not just against random failures of SSCs or human errors, but also against acts of sabotage, theft of nuclear materials, armed intrusion, and external attack. Such measures can be incorporated in the design of the plant, be part of operating practices, and include the capability to respond to intrusion or attack. This principle then calls for defense-in-depth considerations to be applied to all types of plant disturbances: internal events arising from random equipment and human failure; to external events resulting from earthquakes, fires, floods, high winds, etc.; and intentional destructive acts such as sabotage, diversion, and attack. The importance of including defense-in-depth in physical protection measures that address deliberate destructive acts is increased by the fact that physical protection affects all the other protective strategies.

Past discussions of defense-in-depth, at least implicitly, focused primarily on the application of defense-in-depth to compensate for potential human errors, and component failures arising from 'inadvertent' causes such as aging, corrosive processes, poor design, etc. However, with the increased need to consider security issues, embodied in the protective strategy of physical protection, defense-in-depth considerations also include protection against intentional acts directed at nuclear plants that would threaten public health and safety.

This principle ensures that defense-in-depth is considered when implementing physical protection measures, and therefore also implies that the subsequent principles listed here are invoked for physical protection measures just as they are invoked for measures used to achieve the other protective strategies. For example, the strategy of physical protection calls for both preventive and mitigative measures. This is in keeping with conventional approaches to security. For new reactors physical protection measures can be considered during the design stage via vulnerability assessments at this stage. In this manner these measures can become integral with the design and the mitigative and preventive features thus applied are likely to be better than features added as an afterthought to the design.

From this first general principle of defense-in-depth, five additional defense-in-depth principles follow:

(2) ***The design provides accident prevention and mitigation capability.***

This principle ensures an apportionment in the plant's capabilities between limiting disturbances to the plant and mitigating them, should they occur. This apportionment is present in both the design and operation of the plant. It is not meant to imply an equal apportionment of capabilities. The protective strategies introduced in Chapter 2 provide an important illustration of this principle at a high level. Some of these strategies (stable operation, protective systems) are more preventive in nature, while others (protective actions, and to some extent barrier integrity) are more mitigative. Physical protection clearly falls into both areas. By requiring that all of the strategies have to be incorporated into plant design and operation, the presence and availability of both preventive and mitigative features is assured. The strategies are not 'equal' in terms of their contribution to quantitative risk

reduction, for example, but none are completely absent from the design and operation of the plant.

In technology-neutral terms accident prevention can be defined as the measures used to prevent the uncontrolled migration of radionuclides within the plant in excess of normal operating limits. Accident mitigation can be defined as measures used to prevent the uncontrolled migration of radionuclides from the plant to the environment in excess of normal operational limits. In these definitions measures refer to SSCs and procedures, and the plant refers to the physical structures that create a boundary between the environment and any sources of radioactivity at the site. Reducing the frequency of initiating events is generally viewed as a preventive measure; if the initiator occurs, then helping to cope with its consequences is seen as a mitigative measure. A given system, structure or component may, in fact, serve to prevent one challenge and mitigate another challenge, depending on where it occurs in an event sequence. Often prevention is emphasized relative to mitigation for a variety of reasons. Preventive measures are usually more economical, prevention avoids having to deal with the phenomenological uncertainties that arise once an accident progresses, etc. From a defense-in-depth standpoint such an emphasis is acceptable as long as it does not result in an exclusive reliance on prevention with a total neglect of mitigative features.

For both commercial and safety reasons, there is likely to be a great deal of emphasis on the protective strategy of stable operation. Such an approach tries to prevent deviations from normal operation, and to prevent system failures. Clearly, in the case of intentional events, the physical protection strategy will also have as its dominant focus the limitation of initiating events resulting from such acts.

The next protective strategy, ensuring that protective systems are available, recognizes that some initiating events are likely to occur over the service lifetime of a nuclear power plant, despite the care taken to prevent them. This strategy has a preventive component in that some of these systems are concerned with detecting and intercepting deviations from normal operation in order to prevent anticipated operational occurrences from escalating to accident conditions. However, protective systems also include systems that play a dual role of prevention and mitigation or a strictly mitigative role. In practice, safety systems will likely be used for both aspects of defense. This aspect of the protective system strategy recognizes that, although very unlikely, the escalation of certain anticipated operational occurrences or other initiating events may not be arrested and a more serious event may develop. These unlikely events are anticipated in the design basis for the plant, and inherent safety features, as well as additional equipment and procedures are likely to be provided to control their consequences and to achieve stable and acceptable plant states following such events. This leads to the need that engineered safety features are provided that are capable of leading the plant first to a controlled state, and subsequently to a safe shutdown state.

The strategy of barrier integrity plays mainly a mitigative role. While the barrier associated with the fuel prevents an off-normal event from escalating, successive barriers mitigate the consequences of the failure of the fuel barrier. The latter barriers often include the protection offered by a containment or confinement, but may also be achieved by complementary measures and procedures to arrest accident progression, and by mitigation of the consequences of selected severe accidents. Adequate safety margins in the equipment, structure and procedures used here are an important part of the strategy. The physical protection strategy may also introduce barriers against internal and external threats that could compromise plant safety systems.

The increased use of inherent safety characteristics and passive features could strengthen accident prevention as well as mitigation in new and innovative designs.

The strategy of protective actions, such as accident management, is purely mitigative in nature. This includes accident management procedures within the plant (for which margins in barrier strength and in the time needed to achieve successful accident management are essential), as well as emergency response. The emergency response part of the protective action strategy is aimed at mitigation of the radiological consequences of potential releases of radioactive materials that may result from accident conditions. This requires the provision of an adequately equipped emergency control center, and plans for the on-site and off-site emergency response to protect the public health and safety. Temporal margins are important considerations. Physical protection aspects introduce additional considerations into both on-site and off-site protective actions.

(3) ***Accomplishment of key safety functions is not dependent upon a single element of design, construction, maintenance or operation.***

This principle ensures that redundancy, diversity, and independence in SSCs and actions are incorporated in the plant design and operation, so that no key safety functions will be dependent on a single element (i.e., SSC or action) of design, construction, maintenance or operation. The key safety functions include: (1) control of reactivity, (2) removal of decay heat, and the functionality of physical barriers to prevent the release of radioactive materials. In addition, hazards such as fire, flooding, seismic events, and deliberate attacks, which have the potential to defeat redundancy, diversity, and independence, need to be considered.

An important aspect of ensuring that key safety functions do not depend on a single element of design, construction, or operation is guarding against common cause failures and consequential failures. Failure of a number of devices or components to perform their functions may occur as a result of a single specific event or cause. Such failures may affect a number of different items important to safety simultaneously. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human induced event (intentional or inadvertent) or an unintended cascading effect from any other operation or failure within the plant. Common cause failures may also occur when a number of the same type of components fail at the same time. This may be due to reasons such as a change in ambient conditions, repeated maintenance error or design deficiency. Measures to minimize the effects of common cause failures, such as the application of redundancy, diversity and independence, are an essential aspect of defense in depth. Redundancy, the use of more than a minimum number of sets of equipment to fulfill a given safety function, is an important design principle for achieving high reliability in systems important to safety. Redundancy enables failure or unavailability of at least one set of equipment to be tolerated without loss of the function. For example, three or four pumps might be provided for a particular function when any two would be capable of satisfying the specified acceptance criteria. For the purposes of redundancy, identical or diverse components may be used. Consequential failures may occur as a result of high energy line breaks, radiation damage, and structural failures.

The reliability of some safety functions can be improved by using the principle of diversity to reduce the potential for certain common cause failures. Diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components. Such attributes could be different principles of operation, different physical variables, different conditions of operation or production by different manufacturers, for example.

To ensure diversity is actually achieved, the designer needs to examine some of the more subtle aspects of the equipment employed. For example, to reduce the potential for common cause failures the designer examines the application of diversity for any similarity in materials, components and manufacturing processes, or subtle similarities in operating principles or common support features. In addition, if diverse components or systems are used, there is a reasonable assurance that such additions are of overall benefit, i.e., reliability is actually improved, taking into account the disadvantages such as the extra complication in operation, maintenance and testing, or the consequent use of equipment of lower reliability.

Another important aspect of this defense in depth principle is the use of functional isolation, physical separation, and physical protection to achieve independence among safety systems. The reliability of plant systems can be improved by maintaining the following features for independence in design:

- independence among redundant system components;
- independence between system components and the effects of certain initiating events such that, for example, an initiating event does not cause the failure or loss of a safety system or safety function that is necessary to mitigate the consequences of that event;
- appropriate independence between or among systems or components of different safety classes; and
- independence between items important to safety and those not important to safety.

Functional isolation can be used to reduce the likelihood of adverse interaction between equipment and components of redundant or connected systems resulting from normal or abnormal operation or failure of any component in the systems.

Physical separation in system layout and design can be used as far as practicable to increase assurance that independence will be achieved, particularly in relation to certain common cause failures, including deliberate acts intended to defeat safety systems.

Physical separation and physical protection by design includes:
- separation by location (such as distance or orientation);
- separation by barriers; or
- separation by a combination of these.

The means of separation will depend on the challenges considered in the design basis, such as effects of fire, chemical explosion, aircraft crash, missile impact, flooding, extreme temperature, humidity, or radiation level, etc, as well as deliberate acts of disabling or destroying safety systems. Certain areas of the plant naturally tend to be centers where equipment or wiring of various levels of importance to safety will converge. Examples of such locations for LWRs may be containment penetrations, motor control centers, cable spreading rooms, equipment rooms, the control room and the plant process computers. These locations are particularly scrutinized and appropriate measures are taken to avoid common cause and consequential failures, as far as practicable.

Functional isolation and physical separation are also likely to be important considerations for achieving adequate physical protection measures. 'Pinch points' in terms of functional performance as well as physical location can lead to vulnerabilities resulting from either accidental or intentional events.

Finally, this principle also requires that measures are included in the design and operation so that catastrophic events, such as an initiating event that prevents all safety features from operating, for example, are of low enough frequency that they do not have to be considered in the analysis. Examples of such events are pressurized thermal shock (in current reactors) that leads to catastrophic reactor vessel failure, or earthquakes beyond the design basis, but can also include deliberate attacks against the plant.

(4) ***Uncertainties in SSCs and human performance are accounted for in the safety analysis.***

This principle ensures that when risk and reliability goals are set, at the high level and the supporting intermediate levels, the design and operational means of achieving these risk and reliability targets account for the quantifiable uncertainties, and provide some measure of protection against the ones that cannot be quantified as well.

When allocating risk goals that meet the overall risk criteria a designer needs to include allowances for uncertainty. For example, a designer will allocate reliability targets at a high level for each of the protective strategies introduced in Chapter 2. These targets will be supported by maximum unavailability limits for certain safety systems to ensure the necessary reliability for the performance of safety functions and the strategies. Uncertainties are factored into the establishment of all these targets.

An important tool for achieving risk goals for design, construction and operation of the plant is the use of risk assessments that include estimates of uncertainty. The setting of success criteria for the achievement of safety functions are set, and the calculations that show they have been met are performed in such a way that uncertainties are accounted for with a high level of confidence. Note that, at least initially, this needs to be done for new reactor designs without always having the benefit of reviewing past performance.

The role of safety margins is important here in achieving a robust design. Both physical and temporal margins are incorporated in the plant equipment and procedures. Physical margins ensure that capacities of hydraulic, electrical and structural components are well in excess of minimum requirements, so unanticipated increases in demand can be met. Temporal margins ensure preventive systems can correct deviations even after some initial lapses. Therefore, careful attention is paid to the selection of appropriate design codes and materials, and to the control of fabrication of components and of plant construction. In addition, performance monitoring and feedback is employed over the life of the plant to assure reliability and risk goals continue to be met, or if not, corrective actions are to be taken.

Some new reactor designs use passive systems and inherent physical characteristics (confirmed by sensitive non-linear dynamical calculations and safety demonstration tests) to ensure safety, rather than relying on the performance of active electrical and mechanical systems. For such plants, with many passive systems, fault trees may be very simple when events proceed as expected and event sequences may have very low frequency and little apparent uncertainty. The real work of PRA for these designs may lie in searching for unexpected scenarios and their associated uncertainties, including unexpected safety system performance. Innovative ways to structure the search for unexpected conditions that can challenge design assumptions and passive system performance will need to be developed or identified and applied to these facilities. The risk may arise from unexpected ways the facility can end up operating outside the design assumptions. For example, a HAZOP-related search scheme for scenarios that deviate from designers' expectations and a structured search for construction errors and aging problems may be the appropriate tools. Examples

of uncertainties in design and operation that can lead to ways in which the facility can operate outside its design assumptions include scenarios:

- where the human operators and maintenance personnel place the facility in unexpected conditions,
- where gradual degradation has led to unobserved corrosion or fatigue or other physical condition far from that envisioned in the design, or
- where passive system behavior (e.g., physical, chemical, and material properties) is incorrectly modeled.

Measures employed for physical protection are designed to account for uncertainties as well. Security assessments for new reactors need to include some considerations of beyond design basis threats (DBTs) to address uncertainties.

(5) ***The plant design has containment functional capability to prevent an unacceptable release of radioactive material to the public.***

This principle ensures that regardless of the features incorporated in the plant to prevent an unacceptable release of radioactive material from the fuel and the reactor coolant system (RCS), there are additional means to prevent an unacceptable release to the public should a release from the fuel and RCS occur that has the potential to exceed the dose acceptance criteria. The purpose of this principle is to protect against unknown phenomena and threats, i.e., to compensate for completeness uncertainty impacting the magnitude of the source term.

The containment functional means for preventing unacceptable radionuclide releases to the environs has adequate capability to reduce radionuclide release to the environs to meet the onsite and offsite radionuclide dose acceptance criteria. In doing so, threats from selected low probability, but credible events, with the potential for a large source term and a significant radionuclide release to the environs are also considered.

Adequate data is required to provide the quantitative basis for the performance of each of the mechanistic barriers and obstacles for the range of plant conditions associated with the selected events in each category. For new reactor technologies it will be difficult to assure that complete data, spanning all credible events, will be available. Therefore, even if the mechanistic source term calculations indicate that releases from the fuel and RCS are small enough to meet release criteria, other means need to be available to prevent uncontrolled releases to the environment. These means will also be important for threats that are addressed under physical protection. Accordingly, each design needs to have the capability to establish a controlled low leakage barrier in the event plant conditions result in the release of radioactive material from the fuel and the reactor coolant system in excess of anticipated conditions. The specific conditions regarding the barrier leak tightness, temperature, pressure and time available to establish the low leakage condition will be design specific. The design of the controlled leakage barrier should be based upon a process that defines a hypothetical event representing a serious challenge to fission product retention in the fuel and the coolant system. The hypothetical event should be agreed upon between the applicant and the NRC consistent with the technology and safety characteristics of the design. The event could represent a cliff-edge event (where fission product retention in the fuel and coolant system suddenly changes) identified by the PRA, or an assumed fuel damage event, such as a graphite fire in an HTGR. (Chapter 8 provides additional details on analyzing such an event to demonstrate that this defense-in-depth principle is satisfied.) As

noted above, the particular means employed to retain or control the release will depend on the reactor technology.

(6) ***Plants are sited at locations that facilitate the protection of public health and safety.***

This principle ensures that the location of regulated facilities facilitates the protection of public health and safety by including consideration of population densities and the proximity of natural and man-made hazards in the siting of plants. Physical protection aspects associated with security concerns are additional considerations in the siting selection. Siting factors and criteria are important in assuring that radiological doses from normal operation and postulated accidents will be acceptably low, that natural phenomena and potential man-made hazards will be appropriately accounted for in the design of the plant, that site characteristics are such that adequate security measures to protect the plant can be developed, and that physical characteristics unique to the proposed site that could pose a significant impediment to the development of emergency plans are identified. The safety issues that need to be considered include geologic/seismic, hydrologic, and meteorological characteristics of proposed sites; exclusion area and low population zone; population considerations as they relate to protecting the general public from the potential hazards of serious accidents; potential effects on a station from accidents associated with nearby industrial, transportation, and military facilities; emergency planning; and security plans. The environmental issues to be considered concern potential impacts from the construction and operation of nuclear power stations on ecological systems, water use, land use, the atmosphere, aesthetics, and socio-economics.

For reactors, this principle is also intended to ensure that protective actions, including emergency preparedness (EP), are a fundamental element of defense-in-depth. EP will include an emergency plan that provides for appropriate notification, drills, training, sheltering, and evacuation.

These defense-in-depth principles are based upon and consistent with the Commission's white paper, quoted earlier, that states defense-in-depth is: (1) an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction or accident occurs at a nuclear facility and (2) ensures that safety functions 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 principles are also consistent with Regulatory Guide 1.174 where it is stated that consistency with the defense-in-depth philosophy is maintained if:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.

- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.

- System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system (the consequences may range from a minor or major degradation of a barrier all the way to the migration and potential release of radioactive materials to the environment) and uncertainties (e.g., no risk outliers).

- Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed.

- Independence of barriers is not degraded.

- Defenses against human errors are preserved.

- The General Design Criteria are not violated.

These points in Regulatory Guide 1.174 line up well with the defense-in-depth principles stated previously.

4.4 Defense-in-Depth Approach

As noted in the introduction, the framework's defense-in-depth approach is one which combines deterministic and probabilistic elements. The probabilistic elements are used to determine how much defense-in-depth is needed to compensate for the uncertainties that can be quantified. The deterministic elements compensate for the unquantified uncertainties, especially the unexpected threats resulting from completeness uncertainty.

The probabilistic aspects of the approach are the use of a PRA that includes in its calculations the uncertainty associated with the parameter values and models used in the PRA. The PRA is used ultimately to verify that the quantifiable margins and other defense-in-depth measures in the design make the quantified uncertainty range acceptable. The principal deterministic elements of the framework consist of assuring the implementation of all of the five protective strategies introduced in Chapter 2, and ensuring that the defense-in-depth principles of Section 4.3, are implemented in the design and operation of the plant. The Requirements Development Process of Chapter 8, describes the formulation of technology-neutral requirements based on each of the protective strategies. An essential part of the process is the application of the defense-in-depth principles in writing the requirements associated with each strategy.

Propagating the uncertainty distributions of the parameter values and models used in the PRA throughout the calculations provides a designer with estimates of the probability ranges of the modeled challenges to the plant. It also provides the probability ranges associated with the capabilities of the SSCs and procedures that address these challenges. During the design stage an iterative process is likely where the designer adds or modifies SSCs or procedures to achieve reliability goals with respect to their capability that adequately cover the uncertainty ranges of the challenges. The final design will have adequate margins, redundancy, etc. in SSCs and procedures to make the response to identified challenges, including their uncertainty, acceptable and to ultimately make the total risk acceptable. This is how probabilistic aspects of the approach are used to determine how much defense-in-depth is needed to achieve the desired quantitative goals to address the uncertainty that can be quantified in the risk assessment.

The deterministic aspects of the defense-in-depth approach are embodied first of all in applying the entire combination of the protective strategies to the design. The objective of these strategies are restated here:

- The **Physical Protection** objective is to ensure that adequate features and measures are in place to protect workers and the public against intentional acts that could compromise the safety of the plant and lead to radiological releases.

- The **Stable Operation** objective is to limit the frequency of events that can upset plant stability and challenge critical safety functions, during all plant operating states, i.e., full power, shutdown, and transitional states. Initiating events that can affect any source of radioactive material on-site in any chemical and physical form are considered.

- The **Protective Systems** objective is to ensure that the systems that mitigate initiating events are adequately designed, and perform adequately, in terms of reliability and capability, to satisfy the design assumptions regarding accident prevention and mitigation during all states of reactor operation.

- The **Barrier Integrity** objective is to ensure that there are adequate barriers to protect the public from accidental radionuclide releases. Adequate functional barriers are maintained to limit the effects of reactor accidents if they do occur. Barriers can include traditional physical barriers as well as those barriers that rely on physics and chemistry to inhibit the transport of radionuclides when physical barriers are breeched.

- The **Protective Actions** objective is to ensure that adequate protection of the public health and safety in the event of a radiological emergency can be achieved should radionuclides penetrate the barriers designed to contain them. Measures include emergency procedures, accident management and emergency preparedness.

Taken together the protective strategies are a classic example of the deterministic defense-in-depth approach: What if stable operation cannot be maintained, as a result of either intentional or inadvertent acts? Protective systems will restore the plant to normal operation or limit the accident consequences. What if protective systems fail? Barriers will confine the radioactive material. What if barriers are degraded and allow fission products to escape? Protective actions will mitigate the consequences.

Figure 4-2 shows this layered, defense-in-depth arrangement of the Protective Strategies. The figure shows the protective strategies in the order of the operational sequence of events that would occur during an accident situation. It also indicates that physical protection supports all the other strategies.

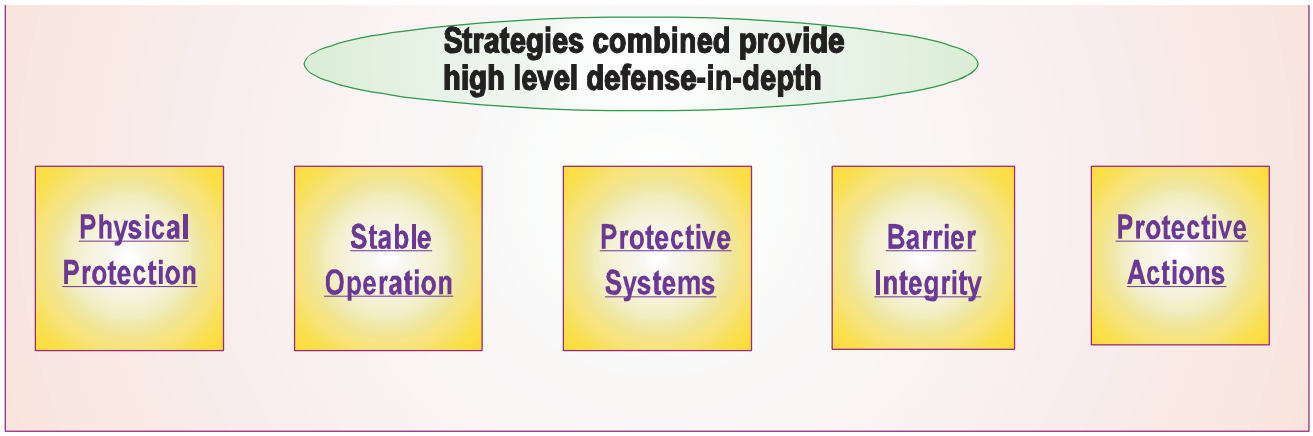

Figure 4-2 Protective Strategies as high level defense-in-depth

Depending on the inherent characteristics of various new designs, the protective strategies may be accomplished by means substantially different from those used in the current light water reactors. The discussion in Appendix B focuses on the safety characteristics of some of the new,

innovative reactor designs, and how these inherent characteristics promote the success of the protective strategies, thereby contributing to defense in depth.

As stated above, an additional deterministic defense-in-depth aspect of the approach is the adherence to the defense-in-depth principles in the implementation of the individual protective strategies. This is an essential part of the Requirements Development Process described in Chapter 8. All of the principles are met through the collective implementation of the protective strategies.

It is also well to restate here that in applying defense-in-depth security and preparedness are integral with safety. As stated in Chapter 3, an integrated and consistent approach to addressing safety, security, and preparedness is required. Consideration of security in the design process is intended to result in a more robust, intrinsic security capability and rely less on extrinsic, operational security programs. Inclusion of preparedness in all aspects of safety and security integration leads to a plant that is safe and robust against all internal and external hazards and inadvertent and advertent threats.

In summary, in this view of defense-in-depth a probabilistic approach to defense-in-depth is combined with a deterministic one. The next section describes how this defense-in-depth approach can be used by a licensee in the design development and by the regulator in the verification of defense-in-depth adequacy.

4.5 Process of Defense-in-Depth

The whole process of investigating whether the design incorporates the essential elements of the framework approach to defense-in-depth is outlined in Figure 4-3. The process is depicted as a series of iterative steps.

As the first box indicates, the new reactor design is assumed to have incorporated the protective strategies to provide a high-level deterministic form of defense-in-depth philosophy into the design process and into the future operation of the plant. Lower level defense-in-depth measures will be present as well. It is also assumed that a risk assessment has been carried out in which uncertainties are identified, and quantified or estimated.

The second box in the figure starts the iterative process of examining the defense-in-depth features of the design, and to modify them, if necessary, to meet the probabilistic and deterministic aspects of the defense-in-depth approach in the framework.

The first part of the examination, as depicted in Box 3, is carried out by using the risk assessment to determine if the plant equipment and operator actions are reliable enough to achieve the desired intermediate and final risk goals, including the uncertainties that are present in the magnitude of the challenges modeled and in the capabilities of the protective SSCs and human actions modeled. This is the probabilistic part of the application of defense-in-depth.

If the risk goals are not met, the process proceeds to Box 4, which calls for an addition to, or a revision of, the equipment and actions used to accomplish the safety functions that ensure adequate performance, thus adding to the defense-in-depth. A revised risk assessment (Box 5) is subsequently performed, to once again verify whether the quantified uncertainties are adequately addressed.

When sufficient defense-in-depth features are incorporated in the design to adequately address the quantified uncertainties, the process proceeds to Box 6. Box 6 starts the verification of the

adequacy of the deterministic elements of defense-in-depth implemented so far. It does so by examining each Protective Strategy, to ensure that the six defense-in-depth principles stated in Section 4.3 have been met. Not all principles are applicable to all protective strategies, but those that are applicable all have to be met by the strategy. For example:

- For physical protection all six principles will apply to the design aspects concerned with physical protection and/or the vulnerability assessment made to identify physical protection needs.

- For stable operation Principle 1, consideration of intentional and inadvertent events, certainly will play a role in the design. Principle 2, prevention and mitigation, can lead to limits on initiating events. Principle 3, no dependence on a single element of design, construction, or operation, applies, as does Principle 4, accounting for uncertainties. Principle 5, preventing uncontrolled release, does not apply, but Principle 6, siting can play a role for stable operation in terms of seismicity, grid reliability, etc.

- For protective systems certainly Principles 1, 2, 3, and 4 apply, while Principles 5 and 6 probably do not.

- For barrier integrity all except Principle 6, siting, would appear to be applicable.

- For protective actions all six principles can play a role.

If some of the principles are not met, the process again proceeds to Box 4 where equipment and actions are added or revised, this time with the intent of satisfying the considerations mentioned above. Once changes have been made to the plant design, the process goes back to the risk analysis of Box 5 and the probabilistic examination of Box 3, since, for example, equipment or procedures added in Box 4 to satisfy the defense-in-depth principles can replace some of the equipment or procedures previously considered in the risk analysis.

When both Box 3 and Box 6 are satisfied the process proceeds to Box 7, which verifies that all Protective Strategies have been checked. It also provides a final check on the adequacy of defense-in-depth measures to account for completeness uncertainty and the overall uncertainty. When this check is satisfied, the design is finalized (Box 8), and provisions for performance monitoring and feedback, to be used during operation, are specified as part of the design finalization.

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 defense-in-depth process outlined in Figure 4-3 will be reflected in the development of technology-neutral requirements, as discussed in Chapter 8. Licensees will be responsible for implementation of the defense-in process in their design, and regulators can use it to assess the adequacy of the defense-in-depth of the design.

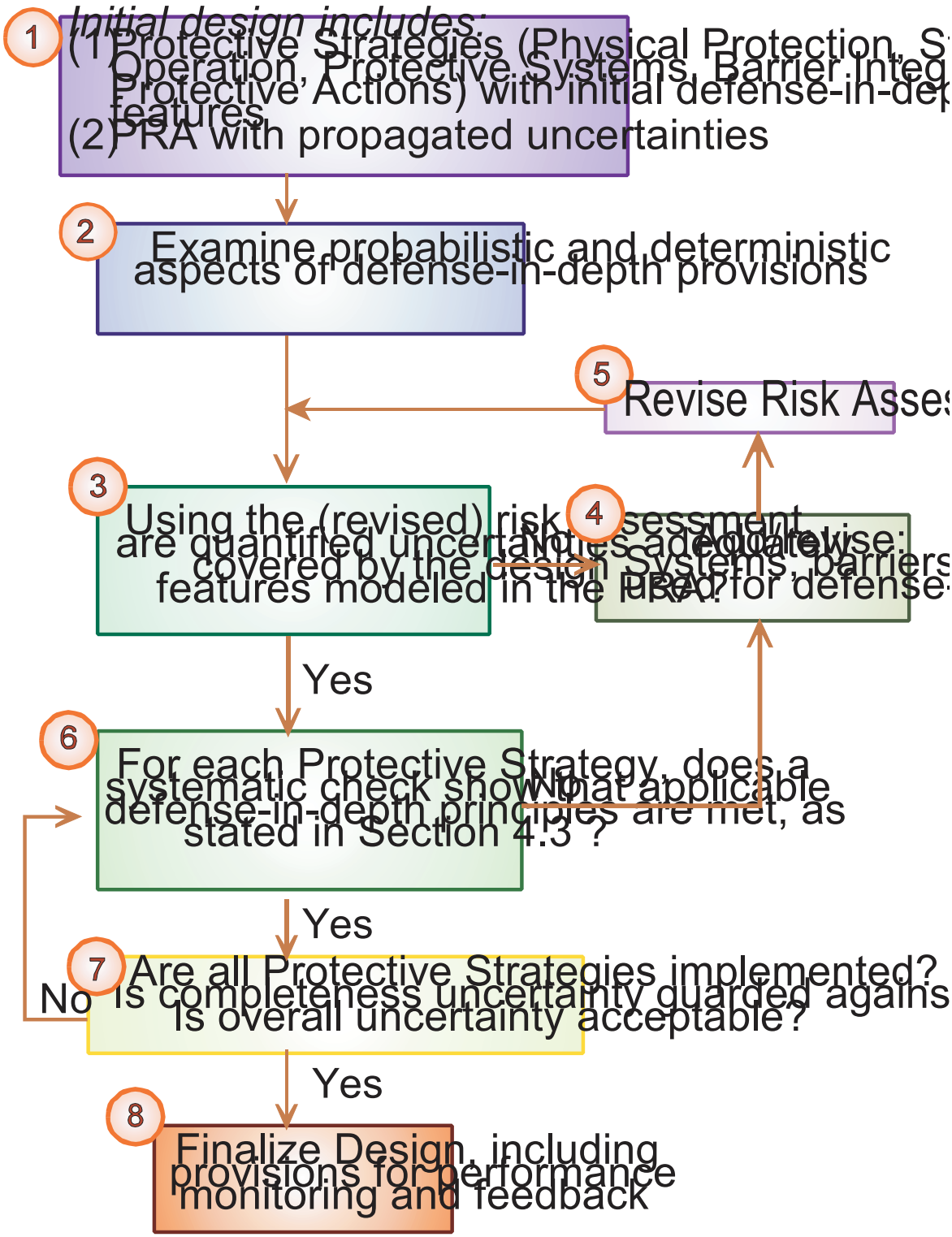

Figure 4-3 Implementation of defense-in

4.6 Technology-Specific Considerations for Defense-in-Depth

While defense-in-depth as a concept is technology neutral, and the principles and approaches described above are also technology neutral, there are obviously technology specific considerations in the application of defense-in-depth to a particular reactor design. Some examples of areas where technology-specific issues arise are listed below.

Identification of modeling uncertainties will have a large technology specific component. While some model uncertainties will apply over a large number of technologies, each particular technology will have its own special model uncertainties which have to be identified and addressed. Examples where model uncertainties arise include the modeling of human performance; common cause failures; mechanistic failures of structures, systems and components; high temperature fuel phenomena; accident progression phenomena, and large radionuclide releases. Each of these areas will include uncertainties peculiar to the technology under consideration, in addition to the more general uncertainties associated with each topic.

As noted earlier in this chapter, a principal objective of applying the defense-in-depth principles is to compensate for completeness uncertainty. However, the means used (equipment, actions, plans, etc.) to accomplish the defense-in-depth objectives will depend on the specific technology of the design in question. As an illustration consider the principle that states the plant design has containment functional capabilities to prevent an unacceptable release of radioactive material to the public. The particular means employed to retain or control the release will depend on the reactor technology. Containments provide such a means in current LWRs. A low leakage, pressure retaining building has been the traditional design feature provided on most existing plants to serve as the final barrier to the release of large quantities of radioactive material following an accident. However, some plants, most notably HTGRs, have been designed with non-pressure retaining buildings based on the inherent safety functions of those designs, including the performance of the fuel barrier over the spectrum of frequent, infrequent, and rare events. In the development of the framework, it has been a goal to define the performance desired (using risk-informed criteria) so as to provide flexibility to the designer. Hence, the means of achieving the principle of preventing uncontrolled releases to the environment is performance based.

5. SAFETY FUNDAMENTALS: PROTECTIVE STRATEGIES

5.1 Introduction

The purpose of this chapter is to define the five protective strategies, to explain why the protective strategies are a sufficient set of safety fundamentals, and to describe how they are used to develop technology-neutral requirements in Chapter 8.

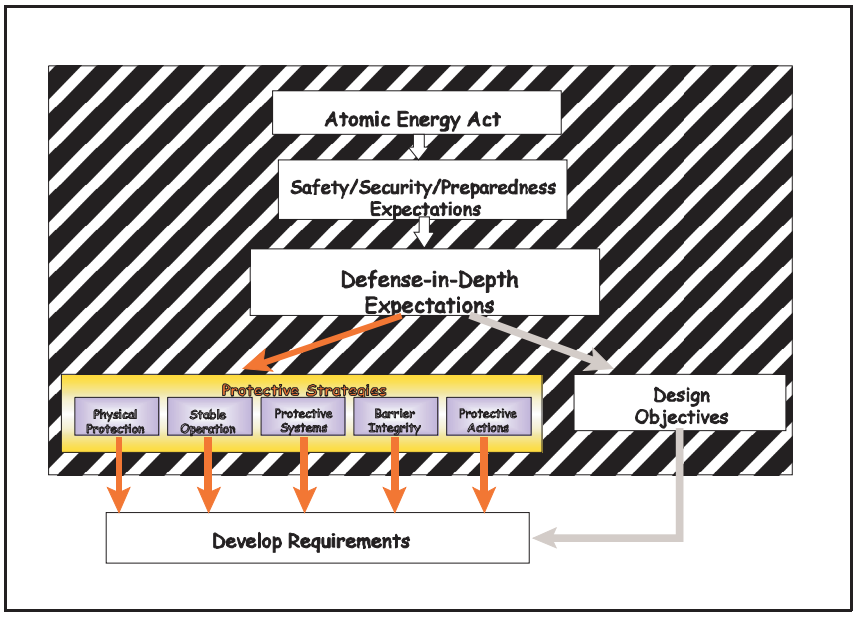

Figure 5-1 Role of Protective Strategies as Elements of Defense-in-Depth

The five protective strategies introduced in Chapter 2 – *Physical Protection, Stable Operation, Protective Systems, Barrier Integrity, and Protective Actions* – satisfy the deterministic (structuralist[(2.13)]) [Ref. 2.1] expectations for defense-in-depth. These protective strategies are the defense-in-depth safety fundamentals that complement the design objectives, as shown in Figure 5-1. This section describes how these five protective strategies were chosen and why they form a sufficient set. It provides a description of each strategy.

The five protective strategies form a sufficient set for two reasons–they meet a set of minimal needs from an engineering perspective and they map to the physical pathways that must occur in the plant, if damage is to occur.

The engineering perspective begins with the traditional view of defense-in-depth, the idea of multiple barriers to release–for LWRs there was fuel bound in an oxide matrix, clad in a tough alloy with good heat transport properties, contained within a leak tight primary coolant system, located inside a low leakage containment structure. If the design can maintain integrity of just one of these barriers, no hazardous materials are released. To protect the barriers, the design must have the capability to prevent damage and that can be ensured by maintaining stable operations (minimizing intrinsic challenges) and providing physical protection (to reduce the chance of successful extrinsic attack). If stable operations should be disturbed, protective systems and protective actions can terminate potentially dangerous event sequences. Finally, should the barriers be breached, protective systems and protective actions can mitigate the damage and minimize release.

Thus the five protective strategies provide layers of protection at all levels of engineering consideration.

[(2.13)] Defense-in-depth describes the deterministic approach as embodied in the structure of the regulations and in the design of the facilities.

There is another direct way to consider the protective strategies. Look at the pathways to damage illustrated in Figure 5-2. The top chart shows that to reach a damage state, the plant must follow a physical pathway to damage, departing stable operations via an inadvertent initiating event or an attack. Any pathway to damage must involve the failure of plant equipment and operators to terminate the pathway before damage. Next, plant systems and operators must fail to arrest the release and propagation of radionuclides. Finally, the pathway must carry sufficient material to the location of workers and the public to cause health effects (injuries or fatalities). Now note that at least two protective strategies can interfere with every stage of the pathway. By their interaction with all stages of pathways to damage, the five protective strategies are clearly a sufficient set.

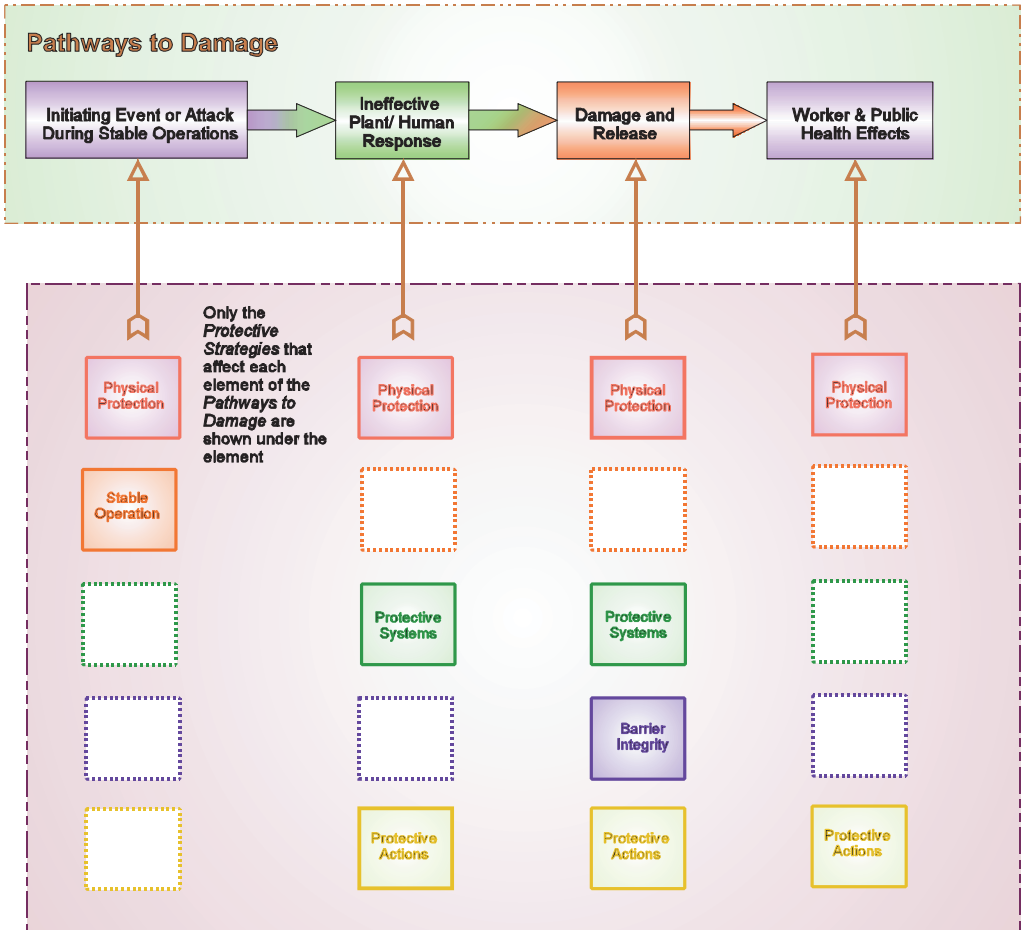

Figure 5-2 The Complete Nature of the Protective Strategies

An alternative way to view the physical pathways is to overlay the PRA. Its purpose is to predict those physical pathways to damage that can occur. For every source of radioactive hazard on site, the response to each possible initiating event is modeled in the PRA. Thus the PRA examines the ways in which multiple barriers[2.14] can be breeched; it models:

- initiating events
- successes and failures in the protection systems that are designed to protect barriers

[2.14] Barriers include physical barriers and the physical and chemical form of the material that can inhibit its transport if physical barriers are breeched.

- human actions that can perform or defeat the protective systems or barriers themselves
- the physical response of the integrated plant to event sequences, including radiological dispersion pathways
- the emergency response system developed to protect the public and workers in case barriers fail
- dose response, calculating the probability of frequency of human health effects and land contamination

Each protective strategy interacts with one or more elements of the PRA model. PRA models of the protective strategies are based on technology-specific design and implementation, which is itself guided by the technical and administrative regulations that apply to design, construction and operation. If the results of the PRA compare favorably with the safety/risk objectives, the protective strategies are adequate for the new technology system. Note that the protective strategies add a layer of protection beyond that implied by the PRA. Because they are all required, they provide a high level defense-in-depth structure for identifying safety requirements, as described in Chapter 8. Furthermore, this layer of defense-in-depth provides a measure of protection against uncertainties, even those that are due to technical knowledge gaps that are not known and not modeled in the PRA.

The link between the protective strategies and actual regulation, starting with the regulatory requirements, is established through an examination of the elements that affect each strategy. These are discussed below.

5.2 Analysis to Identify Requirements

The process for identifying requirements is carried out in Chapter 8. It begins with identifying the protective strategies and focuses on ensuring that they are maintained throughout the life of the plant through efforts in design, construction, operations, and regulation. Figure 5-3 sketches the process.

Figure 5-3 Process for Developing Requirements

If the protective strategies laid out in this chapter are maintained, no release of radioactive material can occur. Therefore the next step is to identify those challenges or threats that could damage or disable one or more protective strategies. In the final step, requirements are developed for design, construction, and operations that will ensure integrity of the protective strategies. This process is carried out in Chapter 8 and outlined below.

Potential challenges to the five protective strategies are analyzed deductively in Chapter 8. The approach is to develop a logic tree for each strategy, asking, how can this strategy (e.g., the set of barriers) fail to provide its function. This is a top-down analysis that begins by partitioning the functional failure into two or more classes of failure. It usually proceeds by identifying specific causes of failure. The basic structure of these logic trees is shown in Figure 5-4, where functional failure of a protective strategy is deductively examined by looking for failure to perform as required, failures through improper analysis or implementation, and unanticipated failures.

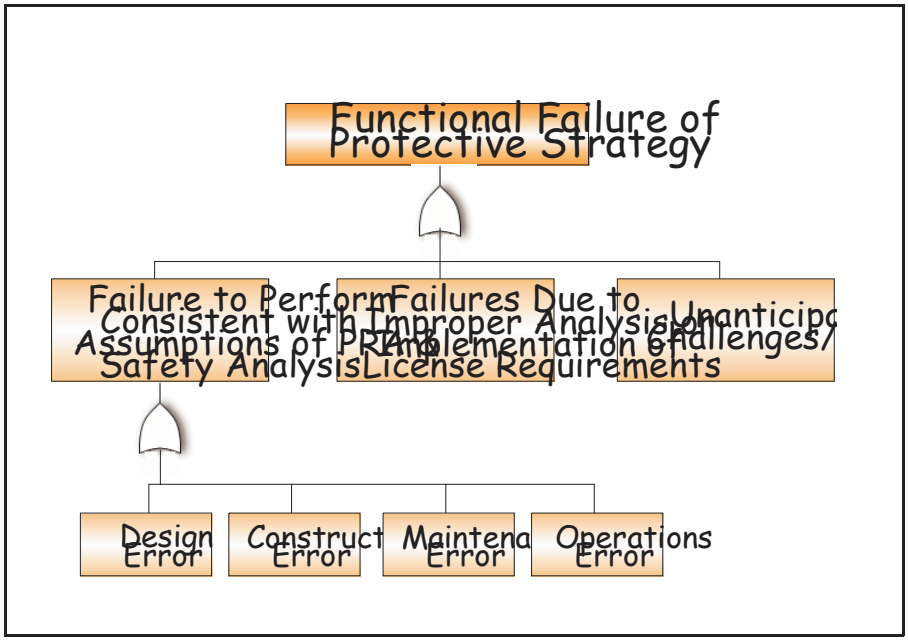

Figure 5-4 Logic Tree Developing Requirements for Each Protective Strategy

For each protective strategy, the logic tree is developed down to the level of specific failures to perform for the first branch; e.g., specific failures such as a design error to address corrosion or an operator error, because the procedures failed to account for all possible environments.

Next, these failure causes (bottom events in the logic tree) are examined for their relevance during design, construction, and operations. Questions are developed for regulators that, when answered, will identify the topics that will need to be addressed by the design, the facility, and the practices if the protective strategies are to remain functional. Finally performance requirements are developed to provide continuing confidence that the topics are addressed. In developing the requirements themselves, a performance-based approach is used wherever practical. Details of this process are carried out in Chapter 8, where technical and administrative requirements are developed to provide high assurance that the protective strategies can fulfil their functions.

5.3 The Protective Strategies

5.3.1 Physical Protection

The physical protection strategy provides measures to protect workers and the public against intentional acts (e.g., attack, sabotage, and theft) that could compromise the safety of the plant or lead to radiological release. Physical protection is provided by inherent design features and by extrinsic measures (“guns, guards, and gates”) to provide defense-in-depth against attack. This

requires that the design makes it unlikely that outsiders or insiders can reach sufficient sensitive areas of the plant to accomplish their goals, either using standoff weapons or by actual entry into the plant. Furthermore, the extrinsic features provide delay and opposing force. Physical protection requires an integrated view of the plant and the opposing forces.

Physical protection is tested by analysis similar in nature to the safety PRA. [Ref. 2.2] In this case one needs to characterize the threat, that is the type of actors, their objectives, their capabilities, and strategies. While the likelihood of an attack is difficult to assess, it is possible to characterize the range of possible threats. Next the system, including its operators and safeguards, is evaluated [Ref. 2.3] against the range of threats to understand the possible scenarios. [Ref. 2.4]

It is a goal of the framework to build physical protection into the plant design early in the design process to improve the intrinsic resistance of the plant and minimize the reliance on extrinsic factors such as guards and armed response.

5.3.2 Stable Operation

The stable operation strategy provides design and operations measures to make it unlikely that challenges to safety develop during operations. A thorough examination of potential initiating events is conducted as part of the risk analysis of the design. The initiators are identified, along with their mean frequency of occurrence. Uncertainty in their frequency is also considered and quantified as a probability of frequency distribution. Initiators will include events from both plant internal and external causes, as well as events during all operating states, since these are all in the scope of the risk analyses. Events that could affect any sources of radioactivity are modeled.

Initiating events vary in their potential impact. For example, an initiator that simply trips an operating reactor is fairly benign, while common cause initiating events (those that directly challenge barriers or disable or degrade protective systems) require fewer additional failures before radionuclide release. Thus it will be helpful to group initiators by their risk significance.

It may also be advantageous to group the initiators into certain classes depending on their frequency of occurrence, as frequent, infrequent or rare. Such a grouping allows the protective features (addressed in the next protective strategy) to have reliability and performance that is commensurate with the frequency of the initiator group, so as to limit the frequency of fuel damage accidents to acceptable levels.

For the new reactor technologies, initiating events may be substantially different from those for current US LWRs. As described in Chapter 7, appropriate techniques can ensure that the search for initiating events is thorough and well-structured.

5.3.3 Protective Systems

The protective systems strategy provides highly reliable equipment to protect plant functions, maintain barriers, and mitigate the effects of accidents and attacks. Plant features are provided to mitigate the consequences of initiating events by protecting the barriers identified in the following protective strategy. A critical part of the determination of these features is a qualitative review of the reactor-specific design philosophy, which includes a review of the design and performance features of the barriers, the reactor-specific safety functions that protect these barriers, the specific inherent and engineered safety features of the reactor concept in light of their capability to protect the barriers. Another critical part of the determination is the full scope (internal and external events, all operating modes) PRAs that are performed for the new designs. These PRAs not only determine the needed features, but also their required reliability and capability. The PRAs are used

to demonstrate that the safety/risk objectives are within the desirable range, with adequate consideration of uncertainty.

For some scenarios which appear to be credible but have very broad uncertainty (due to insufficient data, not well understood phenomena, etc.) additional protective features may need to be incorporated. If LBEs are needed to address such scenarios, as described in Chapter 6, then the protective features necessary to cope with the LBEs are identified and incorporated.

For the new reactor technologies, some mitigative considerations are substantially different from those for current US LWRs and can be appropriately modeled, as described in Chapter 7.

5.3.4 Barrier Integrity

The barrier integrity strategy provides isolation features that protect the primary radionuclide inventory from release. Functional barriers to radionuclide release are provided to maintain isolation of hazardous nuclear material within the system. Barriers can be both physical barriers and barriers to mobilization and transport of radioactive material, e.g. the physical and chemical form that retards the dispersion of the material. Again, the plant PRA can play a critical part in the determination of the number and type of these barriers, as well as their required reliability and capability. The PRAs are used to demonstrate that the frequency of radionuclide release is low enough, with adequate consideration of uncertainty. Uncertainties associated with barrier degradation, e.g., corrosion, erosion, aging, and other materials issues, need to be modeled. For some systems, chemical interactions are important.

Additional barriers, beside those identified from the risk analysis, may be needed to address credible scenarios not amenable to risk analysis and identified as LBEs (Chapter 6). They may be needed to provide assurance against uncertainties in modeling completeness as well.

5.3.5 Protective Actions

The protective actions strategy provides planned activities that protect the other strategies and, should those strategies fail in spite of attempts to protect them, mitigate the impacts of their failure. “Preparedness” is a function of how well procedures are written, how well personnel are trained, and how accessible needed equipment and personnel are. Protective actions are in place to protect the public, even if all design features fail and a release of radionuclides from the plant occurs.

Should functional barriers fail to adequately limit the radionuclide release, protective actions are provided to control the accident progression and ultimately to limit the public health effects of accidents. The analysis of the plant PRA helps to determine the measures that are effective in limiting the public health effects from radionuclide release accidents so that the risk remains below the QHOs.

Protective actions include actions of operators in response to departures from stable operations (i.e., actions specified in abnormal and emergency operating procedures), actions by personnel in the emergency response center (as prescribed by the SAMGs), actions by the security team in response to an attack, on-site health physics management of radiological hazards to workers, and the actions of first responders, state, and local officials in accordance with emergency plans.

6. DESIGN CRITERIA

6.1 Introduction

6.1.1 Purpose and Organization

The purpose of this chapter is to provide design criteria and associated guidance for the risk-informed licensing process that is part of the framework approach. This includes (1) criteria and guidance for the acceptability of PRA results, (2) guidance for the selection of licensing basis events (LBEs) and associated probabilistic and deterministic criteria, (3) criteria for the selection of systems, structures and components with safety significance, and (4) performance standards for security. The inclusion of security standards is in keeping with the framework's integrated and consistent approach to addressing safety, security, and preparedness. Consideration of security in the design process is intended to result in a more robust, intrinsic security capability and rely less on extrinsic, operational security programs. A consistent integration of safety and security using PRA methods and technology can provide a rational basis for decision-making in balancing safety objectives with security concerns. Figure 6-1 shows the place of this chapter in the framework document structure.

The design criteria developed in this chapter are based on a set of design objectives derived from the Framework objectives stated in Section 1.2. These design objectives are:

- To demonstrate compliance with the Commission's safety goal policy statement [Ref. 2.5],
- To develop a process for the identification and selection of a complete set of LBEs that demonstrate that the Commission's safety expectations for new reactors are met, and that adequate defense-in-depth for uncertainties is provided,

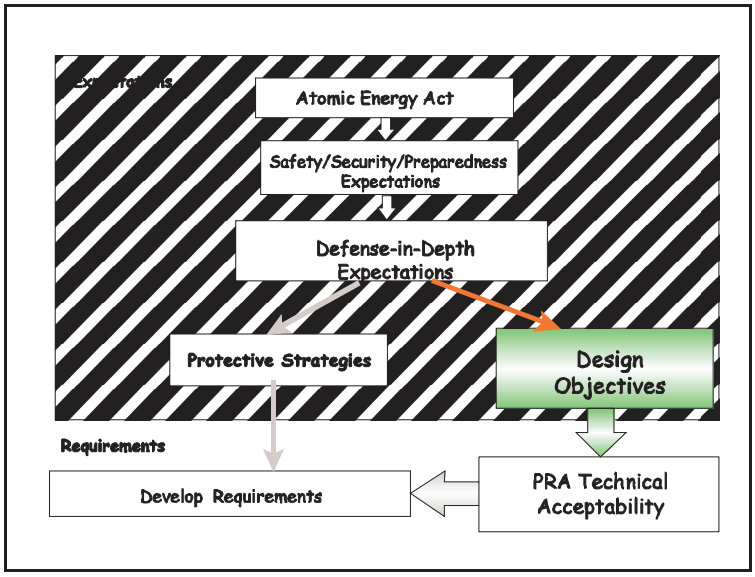

Figure 6-1 How Design Objectives Support Defense-in-Depth

- To integrate security into the design process at least at the same level of protection as established by the post 9/11 NRC requirements, and

- To develop a process for the classification of risk significant systems, structures and components (SSCs) to ensure that the reliability and functionality of the SSCs are consistent with their design, and their intended maintenance and operation.

This chapter is organized as follows: the second half of this introduction briefly highlights the differences of the framework approach and the current licensing process in Parts 50 and 52. Section 6.2 presents the relevant design criteria: Subsection 6.2.1 discusses criteria and guidance for the acceptability of PRA results, 6.2.2 presents guidance for the selection of licensing basis events (LBEs) and associated probabilistic and deterministic criteria, and 6.2.3 has criteria for the

selection of systems, structures and components with safety significance. Section 6.3 points out the margins built into the criteria of 6.2, and Section 6.4 lists performance standards for security.

6.1.2 Differences with Part 50 and Part 52 Approach

To focus the discussion in the rest of this Chapter, it is useful to ask: "What are the differences, at a high level, between the approach in the framework and the current approach to licensing as set out in 10 CFR Parts 50 and 52 ?."

For both the current and the framework approach an applicant must submit a Safety Analysis Report (SAR) in order to construct or operate a nuclear power plant. The SAR contains the design criteria and design information for the proposed reactor plant and comprehensive data on the proposed site. The SAR also identifies and analyzes various hypothetical accident situations and the safety features of the plant which prevent accidents or, if they should occur, mitigate their effects. It is the selection process of these hypothetical accidents, and the selection process of the systems, structures, and components (SSC) that prevent or mitigate these accidents, i.e., are important to plant safety, that are carried out via a new approach in the technology-neutral Framework.

In the current Part 52 licensing approach the calculations carried out for the design basis accidents (DBAs) and, separately, for the PRA are important components of the safety analyses, but there is no direct link between these two components. (The recent development of [voluntary] Part 50.69 does provide a risk-informed link between the PRA and the SSC selection for safety classification.) The Framework approach is a more risk-informed approach since it links the PRA analysis with the other design objectives of licensing basis selection and criteria, and SSC selection and treatment. The framework uses an approach with a probabilistic component, i.e., the framework uses the information from the PRA analysis, for:

(1) the selection of the licensing basis events (the framework uses the term 'licensing basis events [LBEs]' instead of DBAs since the LBEs include risk-significant events in the licensing basis down to a mean frequency of 1E-7 per year and have different acceptance criteria, dependent on their frequency, as explained further below), and

(2) the selection of systems, structures, and components for which special treatment is needed because of their safety significance (i.e., in maintaining risk below the chosen acceptance criteria).

The Framework approach is depicted in Figure 6-2. As the figure indicates, the framework relies on deterministic criteria and defense in depth considerations in both the LBE selection and criteria, and the SSC selection and treatment, but, in addition, uses the risk information from the PRA to focus attention on the risk significant aspects of the design.

The flow of the solid lines in the figure indicates the current process of selecting LBEs and the related SSC selection and treatment based on deterministic criteria and defense-in-depth. PRA results are not considered in the current process for LBE and SSC selection. The dashed lines indicate the new element that the framework approach adds, i.e., the use of the risk information in LBE selection and SSC selection and treatment. As the discussion in the next sections indicates, the framework still uses some deterministic criteria (although not identical to the Part 50 process) and, of course, retains defense-in-depth in the selection process.

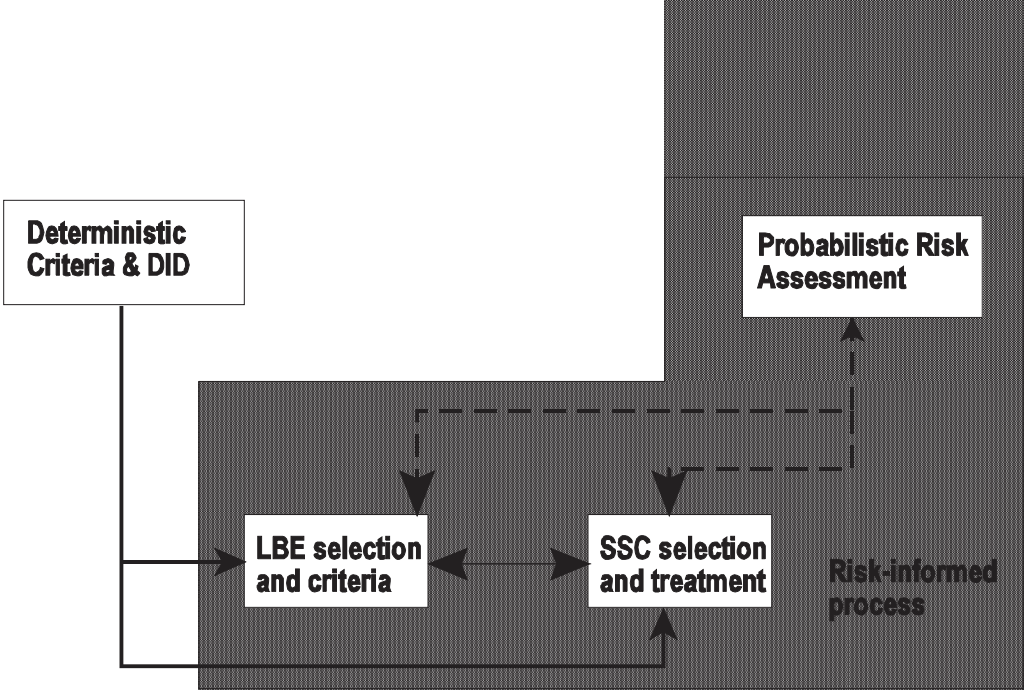

Figure 6-2 Framework approach.

6.2 Acceptance Criteria

In this section criteria are developed for: (1) the acceptability of PRA results, (2) selection of LBEs and associated probabilistic and deterministic criteria, and (3) selection of safety significant SSCs.

6.2.1 Acceptability of PRA Results

In the framework approach a PRA is used as part of the licensing of new plants to generate a sufficiently complete set of accident scenarios whose frequencies and consequences, individually and in the aggregate, provide an estimate of the overall risk profile of the plant. The framework advocates a PRA as the best available analysis method for showing how the interactions and dependencies among SSCs, human actions, and potential plant hazards can result in accident sequences being initiated, prevented, and mitigated. Uncertainties must be addressed in the calculation of both frequencies and consequences of the accident scenarios. Since the accidents include rare events postulated to occur in complex systems for which limited experience exists, the consideration of uncertainties are a vital part of understanding the extent of the risk.

With the framework approach the PRA information is used during the design stage and for selection of licensing basis events (LBEs) and safety significant systems, structures and components (SSCs). Therefore the scope of the PRA used encompasses the whole spectrum of events that credibly occur during the life of the plant: normal operation, as well as frequent, infrequent and rare initiating events and accident event sequences. This is a broader scope than that used currently for LWR risk analysis, which concentrates on beyond design basis accidents, i.e. accidents leading to severe core damage, and uses LWR specific surrogate metrics like core damage frequency (CDF) and large early release frequency (LERF).

6.2.1.1 Frequency - Consequence Curve

From a technology neutral point of view the universally applicable risk metrics are ones which either express consequences directly or can be linked to consequences . Dose at the plant site boundary is an example of a metric that is closely linked to consequences, and therefore is one of the

parameters the results of the PRA can be expressed in. In addition, since frequent, infrequent, as well as rare events are included in the PRA, a single limiting criterion (such as CDF or LERF for LWRs) may not be adequate. Instead, a criterion that specifies limiting frequencies for a spectrum of consequences, from none to very severe, needs to be established. This can be denoted via a frequency consequence (F-C) curve, an example of which is shown in Figure 6-3. The F-C curve shown relates the frequency of potential accidents to radiation doses as shown in Figure 6-4. For the frequent and infrequent categories, it is based on, and derived from, current regulatory requirements in Parts 20, 50 and 100. Part 20 limits the radiation doses from licensed operation to individual members of the public. Part 50 Appendix I identifies design objectives for releases during normal operation to be as low as reasonably achievable (ALARA). Part 50.34 requires an applicant for a license for a power reactor to demonstrate that doses at the site boundary (and the outer boundary of the low population zone) from hypothetical accidents will meet specified criteria and Part 100 has similar dose criteria for determining site suitability. The principle underlying the F-C curve is that event frequency and dose are inversely related, i.e., the higher the dose the lower is the event frequency.

10 CFR 50 Appendix I provides numerical guidance for doses that are ALARA from nuclear power plant normal operation. The recommended value is 5 mrem per year whole body (or, equivalently, 5 mrem per year total effective dose equivalent [TEDE]) to an individual in an unrestricted area, thus doses in the range of 1 mrem - 5 mrem are assigned a frequency of 1 per year. 10 CFR 20 limits public exposure from licensed operation to 100 mrem in any one year and the range from 5 mrem - 100 mrem is assigned a frequency of 1E-2 per year (events in this category would generally constitute what are currently known as anticipated operational occurrences or AOOs).

The next higher dose category ranges from 100 mrem to about 20-25 rem. This category involves doses that are above public limits for licensed operation but only involve stochastic health effects. Doses in the range of 100 mrem to 25 rem are subdivided into two ranges: those below the EPA protective action guideline [Ref. 2.6] of 1 rem offsite are assigned a frequency of 1E-3/year while those in the range of 1 rem to 25 rem are assigned a frequency of 1E-4 per year. 25 rem is the DBA offsite dose guideline in 10 CFR 50.34 and 10 CFR 100; it is also the dose that defines an abnormal occurrence (AO) as described in the Commission's April 17, 1997, policy statement on AOs, (62 FR 18820 [Ref. 2.7]) which defines substantial radiation levels to imply a whole body dose of 25 rem to one or more persons.

Doses above 50 rem fall in a category where some radiation effects are deterministic (ICRP 41 [Ref. 2.8] gives a threshold of 0.5 Sv, 50 rem, based on 1% of the exposed population showing the effect, for depression of the blood forming process in the bone marrow, from whole body exposure). Thus doses in the range of 25 rem - 100 rem are assigned a frequency of 1E-5 per year. Doses where early fatality is possible are characterized by a threshold (e.g., lethal dose to 1% of the population) and an LD_{50} value (median lethal dose). For bone marrow syndrome from whole body exposure, the threshold dose is 1 Sv (100 rem), for a population receiving no medical care and 2-3 Sv (200 - 300 rem) for a population receiving good medical care. In the NRC-sponsored MACCS probabilistic consequence analysis code [Ref. 2.9], the threshold and LD_{50} parameters for early fatality due to bone marrow syndrome are set at 150 rem and 380 rem respectively for a mixed population consisting of 50% receiving supportive medical care and 50% receiving no medical care based on the early health effects models developed in NUREG/CR-4214 [Ref. 2.10]. Based on these considerations, doses in the range 100 rem - 300 rem are assigned a frequency of 1E-6 per year, 300 rem - 500 rem a frequency of 5E-7 per year (the NRC early fatality safety goal), and the curve is capped beyond doses greater than 500 rem at 1E-7 per year. Note that the reference sources referred to for the 1 to 100 mrem range provide guidance in terms of annual doses, whereas the reference points for the higher doses are per event.

These values are shown below in Table 6-1 and are plotted in Figure 6-3.

Table 6-1 Proposed dose/frequency ranges for public exposures

Dose Range	Frequency (per year)	Comment (all doses are TEDE)
1 mrem - 5 mrem	1E+0	5 mrem/year is ALARA dose in 10 CFR 50 App I
5 mrem - 100 mrem	1E-2	100 mrem/year is the public dose limit from licensed operation in 10 CFR 20
100 mrem - 1 rem (1)	1E-3	1 rem/event offsite triggers EPA PAGs
1 rem - 25 rem (1)	1E-4	25 rem/event triggers AO reporting and is limit in 10 CFR 50.34a and in 10 CFR 100 for siting
25 rem - 100 rem	1E-5	50 rem is a trigger for deterministic effects (i.e., some early health effects are possible)
100 rem - 300 rem	1E-6	In this range the threshold for early fatality is exceeded
300 rem- 500 rem	5E-7	Above 300 - 400 rem, early fatality is quite likely
> 500 rem	1E-7	Above 500 rem early fatality is very likely and curve is capped

The sequences of the PRA will populate the space under the F-C curve. Some scenarios will have little or no consequences, primarily because of the inherent characteristics and design features of the plant. Others are likely to approach the F-C curve and thus make up the important contributors to the plant risk profile. To be acceptable, the results of the PRA, in terms of the frequency and consequences of all the accident sequences examined, must lie in the acceptable region, (i.e., below) the F-C curve. With the curve of Figure 6-3 accident sequences that lie below the F-C curve will satisfy the QHOs of the safety goal policy [Ref. 6.1] individually. Note that meeting the F-C curve imposes additional constraints in addition to satisfying the QHOs because specific dose limits are imposed at all frequencies. As discussed in the next section, in addition to meeting the QHOs individually, the PRA sequences also have to meet the QHOs in the aggregate.

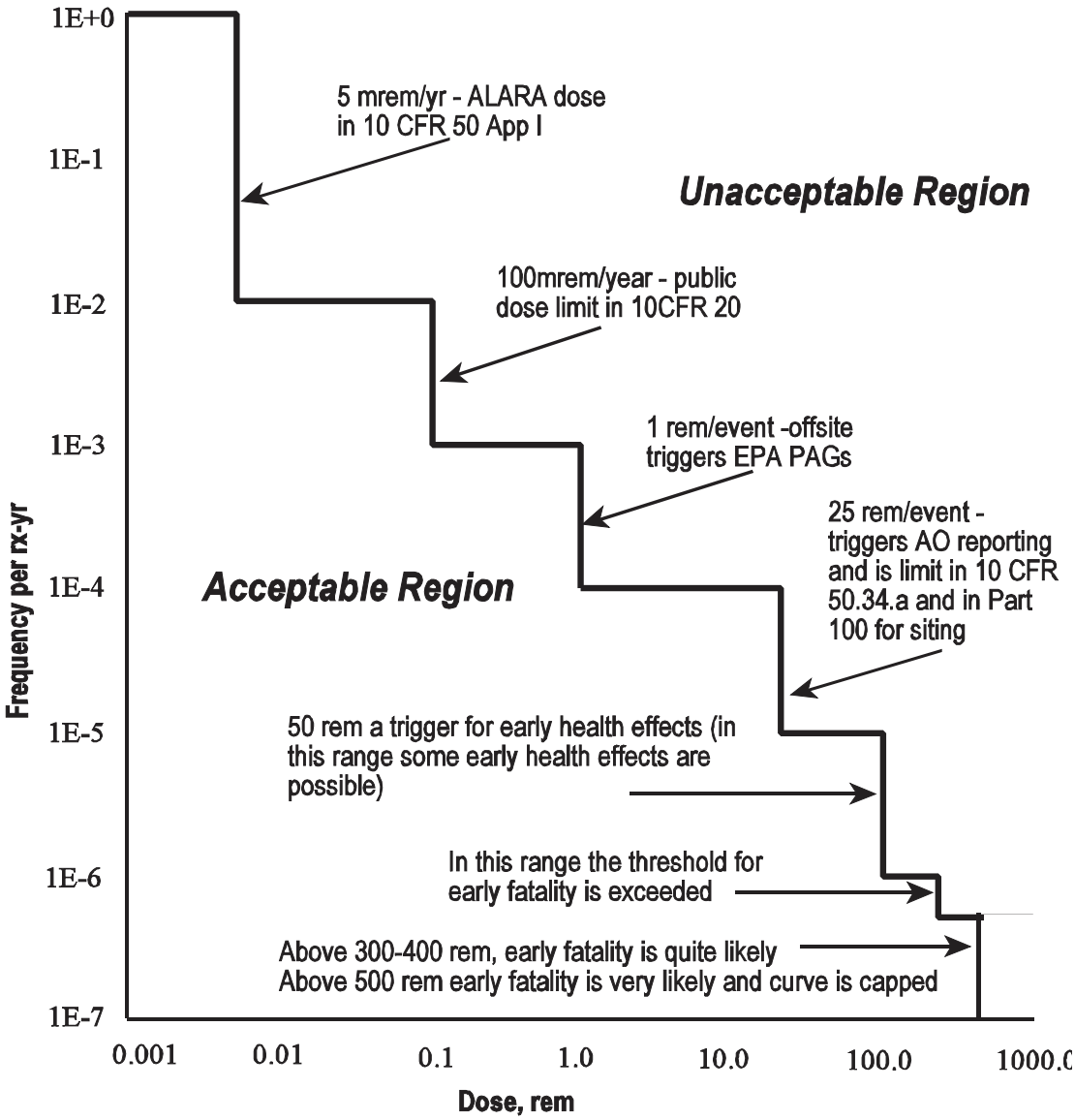

Figure 6-3 Frequency-consequence curve.

Note that with the kind of acceptance criterion for individual sequences described above, an accident sequence is acceptable even though it has a dose at the boundary associated with it, as long as its frequency does not exceed the limit for that dose, as specified by the F-C curve. For current LWR PRAs a single limiting frequency, associated with high consequence event sequences, is the acceptance criterion. For the PRAs required here, whose scope covers all types of off-normal event sequences, the criterion is a series of limiting frequencies whose value depends on the associated consequences; frequent event sequences must lead to no consequences or very minor ones; infrequent event sequences can have somewhat higher doses associated with them, and rare events can have higher consequences still. It should be noted that for specific technologies it may be possible to eventually develop surrogate metrics (such as CDF and LERF for LWRs) for the dose parameter, along with acceptable values for such surrogates. However, it will likely take some time to obtain the experience from testing and operation to have confidence in such surrogates.

6.2.1.2 Quantitative Health Objectives

With the curve of Figure 6-3 accident sequences that lie below the F-C curve will satisfy the QHOs of the safety goal policy individually. Note that meeting the F-C curve imposes additional constraints in addition to satisfying the QHOs because specific dose limits are imposed at all frequencies.

In addition to meeting the QHOs individually, the PRA sequences also have to meet the QHOs in the aggregate. This means the PRA results must demonstrate that the total integrated risk from the PRA sequences satisfy both the latent cancer QHO and the early fatality QHO. The QHO calculation is based on PRA event sequence dose consequence calculation using the mean value of the resulting dose and frequencies. The following are definitions of the QHOs taken directly from the Safety Goal Policy Statement [Ref. 6.1]:

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

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

The risk in the safety goals is the total risk per reactor year, summed over all accident sequences.

One question raised about the safety goals is whether they apply to a single unit or to the whole site, i.e., should the integral risk from multiple units meet the safety goals. As the statement above indicates, the QHOs address the risk to an individual that lives in the 'vicinity' of a nuclear power plant. If the plant consists of multiple units the individual is exposed to the risk from those units and therefore the site. The framework position is that the integrated risk posed by all new reactors (and their related radionuclide sources, such as a spent fuel storage) at a single site should not exceed the risk expressed by the QHOs. This is complementary to the minimum level of safety recommended for new reactors in Chapter 3. Both the individual risk of each new reactor and the integrated risk from the new reactors, associated with a future combined license application, should not exceed the risk expressed by the QHOs.

This position does not require that the integrated risk from existing reactors, where there are multiple reactors at a single site, meet the risk expressed by the QHOs, even though the site may be considered for new reactors. In the policy statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants [Ref. 2.11]," the Commission concludes that existing plants pose no undue risk to public health and safety and sees no present basis for immediate action on generic rulemaking or other regulatory changes for these plants ...." This statement is supported by the Commissions policy statement on Safety Goals for the Operation of Nuclear Power Plants that states that current regulatory practices are believed to ensure that the basic statutory requirement, adequate protection of the public, is met. In considering new plants at a site with or without existing plants, it should be assured that the new plants pose no undue risk to the public. Limiting the integrated risk for new plants to the risk expressed by the QHOs (and thereby imposing enhanced safety for these new plants), ensures that the new plants pose no undue risk to the public.

6.2.2 LBE Selection and Associated Criteria

The term licensing basis events (LBEs) is used in the Framework to indicate those accidents that must be considered in the safety analysis of the plant and must meet some deterministic criteria in addition to meeting the frequency-consequence curve. As the discussion below will make clear, the concept of LBEs is similar, but not equivalent, to the concept of design basis accidents (DBAs) in the current regulations.

The event sequences that make up the LBEs are selected from the PRA sequences. Before LBE selection, it is assumed that a complete PRA of the plant design covering both internal and external events and all modes of operation has been performed and that all accident sequences have been identified in terms of a distribution of their frequencies and end-states that are defined through consequences (estimated by the doses at the site boundary).[(2.15)] The results have to meet the criteria of the proposed F-C curve, i.e., the frequencies and consequences of all sequences have to lie in the acceptable region of the F-C curve. It is also assumed the PRA meets the appropriate review criteria, standards, etc., as outlined in Chapter 7.

In the technology-neutral approach used in the framework the LBEs are characterized as event sequences which represent a challenge to plant safety. These event sequences include those that involve a radionuclide release and lead to a dose at the site boundary. However, particularly at high event frequencies, the LBEs may also include sequences that do not involve any release of radionuclides. In the case of LWRs, for example, this characterization would subsume events, similar to AOOs, involving either no release or very small amounts of release (e.g., from iodine spiking events, gap release, etc.), design basis accidents as described in Part 50.34 or Part 100.11 (where significant core damage is assumed to occur such that a large quantity of fission products is assumed to move from the fuel pellets/fuel rods to the reactor coolant system or the reactor vessel and ultimately into containment) and large releases (a significant quantity of fission products released from containment into the environment with a potential for causing early health effects to the offsite population).

The purpose of the LBEs is similar to the purpose of the DBAs in the current licensing process: to provide assurance that the design meets various accident challenges with adequate margin and to evaluate the design from the standpoint of the dose guidelines in the siting criteria of 10 CFR Part 100. By using the PRA to select certain sequences as LBEs, the selection process can ensure that the LBEs represent potential risk significant accident challenges. Since the LBEs are sequences from the PRA, they also provide a more detailed check on the PRA analysis, but they have to meet more stringent criteria than the PRA sequences as well as some deterministic criteria.

In addition to the probabilistically selected LBEs using the PRA there is at least one deterministic LBE that must be considered for defense in depth purposes, as discussed below in Subsection 6.2.2.2. Additional LBEs could also be added based on the designer's or reviewer's judgement.

[(2.15)] For the designer to make these calculations, they must either be for a particular site or NRC must define a reference site, with sufficient detail to ensure it is adequate for any U.S. site. (i.e., consequences for the reference site will be greater than for real sites). An 80-th percentile site with respect to weather (i.e., consequences greater than at 80 percent of existing reactor sites with respect to variability of weather alone) is defined in NUREG/CR-6295 "Reassessment of Selected Factors Affecting the Siting of Nuclear Power Plants."

6.2.2.1 Probabilistic Selected LBEs

To assure the safety margin of the design over the whole spectrum of off-normal events, individual LBEs are chosen so that their aggregate covers the entire frequency range represented under the F-C curve. It is also desirable to have more stringent deterministic safety acceptance criteria for LBEs with a relatively high frequency, i.e., 'frequent' sequences, somewhat less stringent deterministic criteria for 'infrequent' LBEs, and even less stringent ones for 'rare' LBEs. With this in mind the region under the F-C curve can be divided into frequency categories for purposes of specifying frequency related deterministic criteria. Table 6-2 lists the proposed categories and their basis. The criteria for selecting the frequency categories take into account those events that are:

- Expected to occur during the lifetime of a plant,
- Expected to occur during the lifetime of the population of plants,
- Expected to challenge the Commission's Safety Goals

Table 6-2 LBE Frequency Categories

Category	Frequency	Basis
frequent	$10-2/ry	Capture all event sequences expected to occur at least once in lifetime of a plant, assume lifetime of 60 years
infrequent	< 10-2/ry to $10-5/ry	capture all event sequences expected to occur at least once in lifetime of population of plants, assume population of 1000 reactors
rare	<10-5/ry to $10-7/ry	capture all event sequences not expected to occur in the lifetime of the plant population, but needed to assess Commission's safety goals
• applies to all internal and external events • based on these categories, events with mean frequency <10-7/ry do not have to be considered in the design for licensing purposes, but they may be included for defense-in-depth purposes		

Table 6-2 applies to event sequences not just initiating event (IE) frequencies. However, the IE frequencies themselves are also subjected to limits in the various frequency categories. In the framework approach, to ensure that the assumptions in the PRA on initiating events (IEs) are preserved, each applicant proposes cumulative limits on IE frequency for each of the LBE event frequency categories. The cumulative initiating event limits are to be agreed upon between the applicant and the NRC consistent with the technology and safety characteristics of the design. These limits will be monitored during the plant operation as part of the living PRA program. Requirements related to the living PRA are stated in Chapter 7 and Chapter 8.

Figure 6-4 shows the F-C curve divided into the three frequency regions and also indicates the additional deterministic criteria to be applied to LBEs from the frequent and infrequent region.

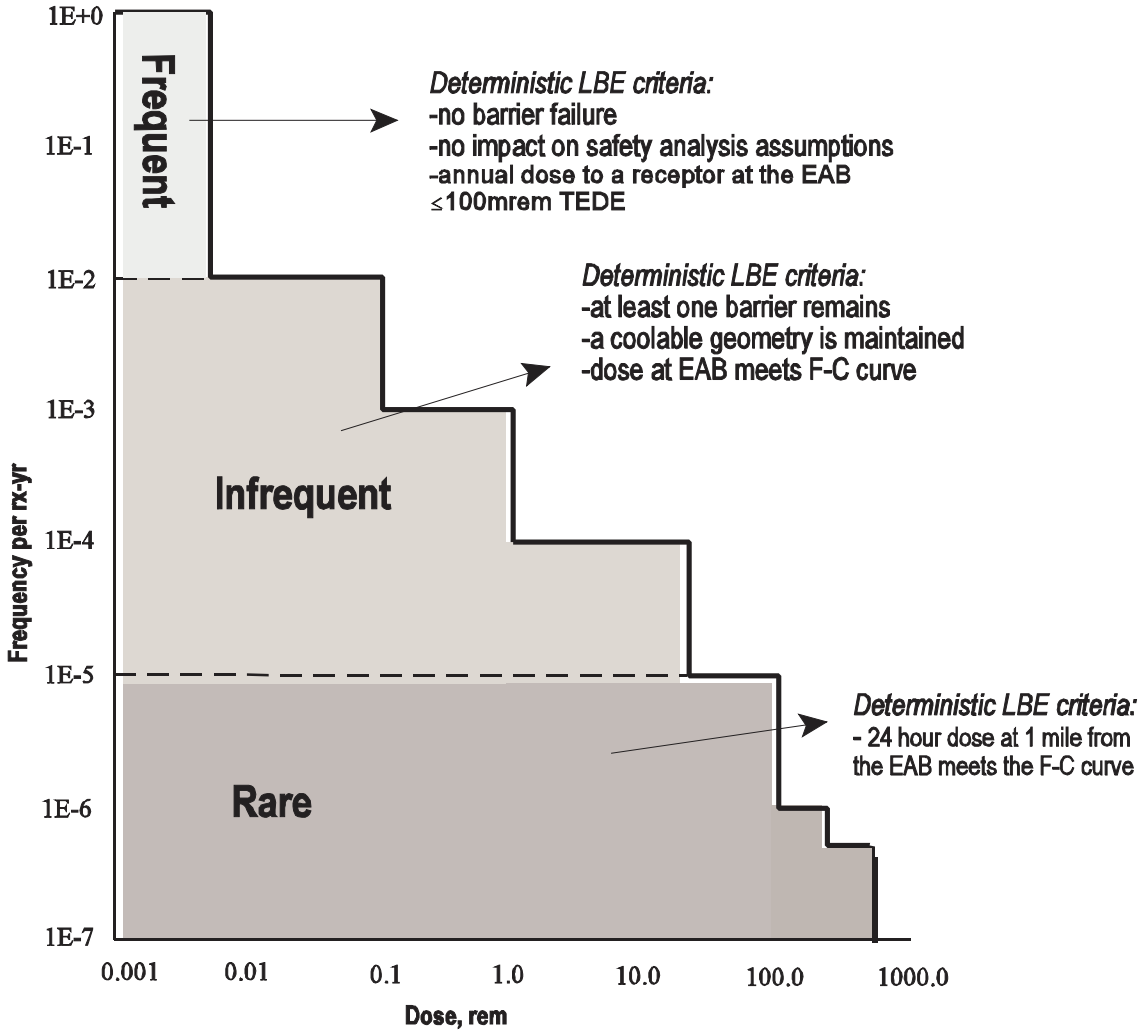

Figure 6-4 F-C curve regions and deterministic LBE criteria.

The probabilistic and the deterministic requirements for the LBE calculations (as well as the PRA calculations) are summarized in Table 6-3. As the table indicates, a realistic analysis is carried out to obtain mean values and uncertainty distributions for all the important parameters of the PRA sequences as well as those sequences chosen as LBEs. The exceptions are the source term calculations, which are calculated using the 95% value of the uncertainty range for the amount of radionuclides released for both the PRA and the LBE calculations.

Scenario specific source terms are used for the dose calculations based on the following criteria: (1) The scenarios to be used for the source term evaluation are selected from the design specific PRA with due consideration for uncertainty, (2) The source term calculation, using the selected scenarios, is based on analytical tools that have been verified with sufficient experimental data to cover the range of conditions expected and to determine uncertainties, (3) The source terms used for licensing decisions should reflect the scenario specific timing, form and magnitude of radioactive material released from the fuel and coolant. Credit may be taken for natural and/or engineered attenuation mechanisms in estimating the release to the environment, provided there is adequate

technical basis to support their use, and (4) The source terms used are 95% confidence level values based upon best estimate calculations with quantified uncertainties. Where uncertainties cannot be quantified, engineering judgement is used. These criteria provide a flexible, performance-based approach for establishing scenario specific licensing source terms. However, the burden is on the applicant to develop the technical bases, including experimental data, to support their proposed source terms. Specifically, the use of scenario specific source terms requires the applicant to do sufficient testing to confirm the magnitude and rate of release, the timing and energy of release, the chemical form, and transport properties of fission products from the fuel, reactor coolant system, and reactor building under the range of conditions analyzed in the PRA. This includes accounting for the impact of different burnup levels that the fuel can experience and the physical and chemical conditions associated with various accident scenarios on the release fractions and release rates of major fission product groups. Applicants can propose to use a conservative source term for LBEs, provided the use of such a source term does not result in design features or operational features that detract from safety. The use of scenario specific source terms may result in smaller source terms being used for siting purposes compared to the source terms traditionally used for LWR siting.

The confidence level with which the dose levels of the F-C curve are met are mean value for the PRA, but 95% for the event sequences selected as the LBEs[(2.16)]. LBEs from the frequent and infrequent region also meet the additional deterministic criteria indicated in Table 6.3. As stated above, for the frequent category the doses are calculated at the EAB, and for the infrequent category the doses are calculated at the EAB and the outer LPZ boundary. For the rare category, which involves event frequencies < 1E-5 per year, the doses are calculated 1 mile from the site boundary for comparison with the F-C curve. One mile from the site boundary is the distance for estimating average individual risk for comparison with the early fatality safety goal. Rare category sequence doses at this distance that lie within the F-C curve provide additional confidence that the early fatality safety goal is met.

The difference in the confidence level between the standard PRA sequences and the LBE sequences with which the F-C dose criteria are met (mean versus 95%) establish a safety margin the design must satisfy. In addition, the deterministic criteria the LBE sequences must satisfy add to the defense-in-depth in the design.

[(2.16)] Further guidance will be provided on how to calculate source terms at the 95% confidence level.

Table 6-3 PRA and LBE Criteria

	Calculations	Acceptance Criteria	
Category *(Mean Event Frequency Per ry)*		*Confidence level for meeting REM criteria* *PRA/LBE*	*Additional deterministic acceptance criteria for LBEs*
frequent ($10^{-2})	*With the exception of the source term, realistic calculations are carried out to obtain the mean and uncertainty distribution of the important parameters for estimating frequency and consequences.* *Source Term calculations use the 95% value of the amount of radionuclides released, obtained from a mechanistic calculation, and use RG 1.145 or the equivalent for calculating atmospheric dispersion*[2.17]	mean/95%	-no barrier failure -no impact on safety analysis assumptions - annual dose to a receptor at the EAB #100mrem TEDE
infrequent (< 10-$^{-2}$ to $10-$^{-5}$)		mean/95%	-at least one barrier remains -a coolable geometry is maintained -dose at the EAB meets the F-C curve
rare (<10-$^{-5}$ to $10-$^{-7}$)		mean/mean	- 24 hour dose at 1 mile from EAB meets the F-C curve
Deterministic		95%	worst two-hour dose at the EAB and the dose at the outer edge of the LPZ for the duration of the event do not exceed 25 rem TEDE (this criterion is also used for siting)
EAB - exclusion area boundary TEDE - total effective dose equivalent LPZ - low population zone			

For the LBEs the question remains at what 'level' are the selected sequences defined: cut-set, systemic, or functional? In the Framework approach the LBEs are sequences selected from the PRA at the 'systemic' level in terms of front-line systems that provide the needed safety functions. The specific level of detail for these 'front-line' systems for different technologies will be determined in the technology specific Regulatory Guides.

In this approach, the LBEs are chosen by grouping similar accident sequences. Similar accident sequences are those that have a similar initiator and display similar accident behavior in terms of system failures and/or phenomena and lead to similar source terms. In the case of LWRs for example, similar accident sequences would be events such as ATWS, various LOCAs (of different break sizes) with similar equipment response, containment bypass, transients of various types

[2.17] Further guidance will be provided on how to calculate source terms at the 95% confidence level.

where each type exhibits similar equipment response, etc. Similar accident sequences are also likely to have the same SSCs credited for accident prevention and/or mitigation. What are considered 'similar' groupings will be determined on a technology specific basis.

The proposed approach to the identification and selection of LBEs is described below, and is shown in the schematic diagram of Figure 6-5. Event sequences with a mean frequency < 1E-8 per year do not need to be considered for licensing purposes. However, uncertainties in the frequency are considered and an appropriate methodology for analyzing uncertainty is utilized.

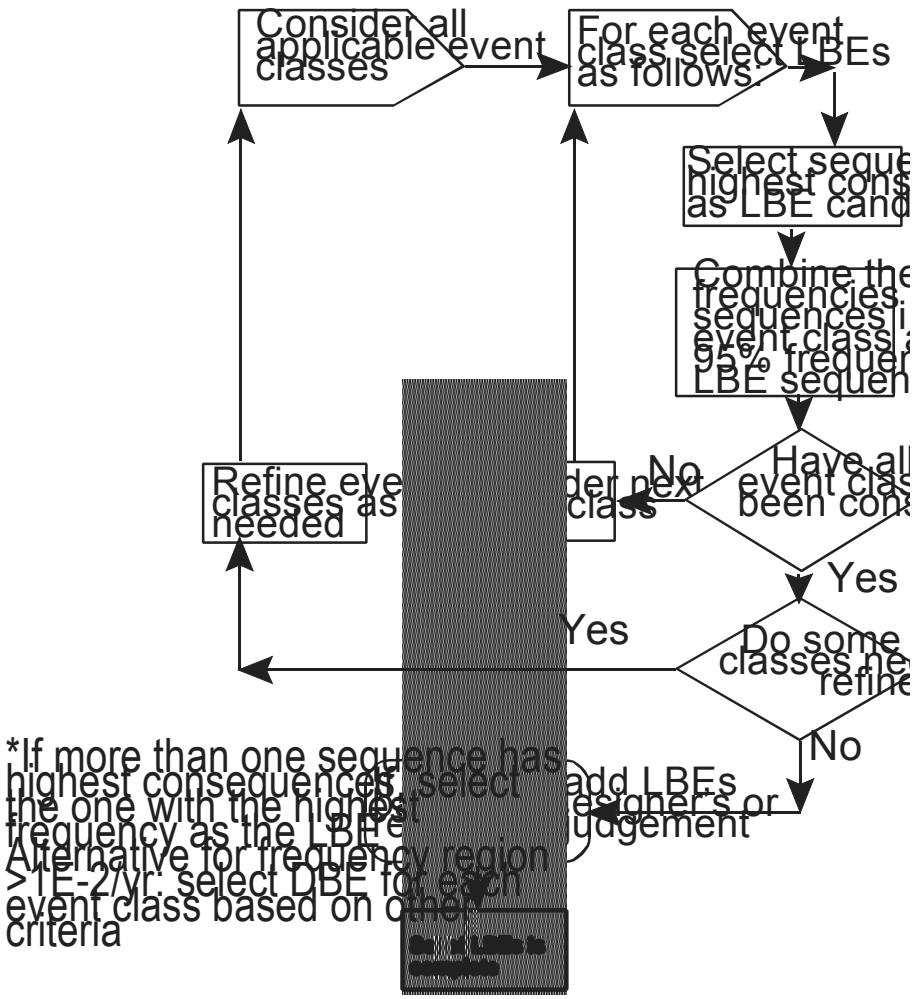

Figure 6-5 Selection of licensing basis events.

The PRA's accident sequences are grouped into similar event classes, as explained above, dictated by the particular design under consideration, and one or more LBEs is associated with each event class as follows: For each event class, the sequences that display similar accident behavior or phenomena in terms of being associated with a specific accident scenario source term are identified. Consideration is given to the frequency uncertainty of each sequence and the frequencies of the identified sequences in each event class are appropriately combined, accounting for dependencies, to obtain an overall distribution with respect to frequency for the event class. The 95th percentile confidence level with respect to frequency is selected as the LBE frequency

corresponding to the particular event class. With regard to the dose level that this LBE must satisfy, after the scenario specific source term is selected, it is input to a probabilistic consequence code that evaluates a distribution of doses with respect to weather variables (stability class, windspeed, etc) at any specific distance such as the EAB. The LBE selected must meet the dose level of the F-C curve at the 95th percent confidence level of the dose distribution corresponding to the particular source term.

The goal of the grouping process is to account for all the event classes with 95th percentile frequency greater than 1E-7, and to strike a reasonable balance between the number of event classes and the degree of conservatism used in the grouping process. As a result of the grouping process all sequences are covered by an LBE. Sequences resulting in small doses can be covered with a few 'high' frequency LBEs, representing general event classes, that still satisfy the F-C curve and the associated frequency-range related criteria of Table 6-3. Higher dose sequences can be covered with more numerous LBEs, representing more detailed event classes, to show that they satisfy the F-C curve and associated criteria. For example, a particular set of event classes that start out with similar failures may be broken down into 3 different classes and related LBEs, as indicated schematically in Figure 6-6, to meet the F-C curve and associated criteria.

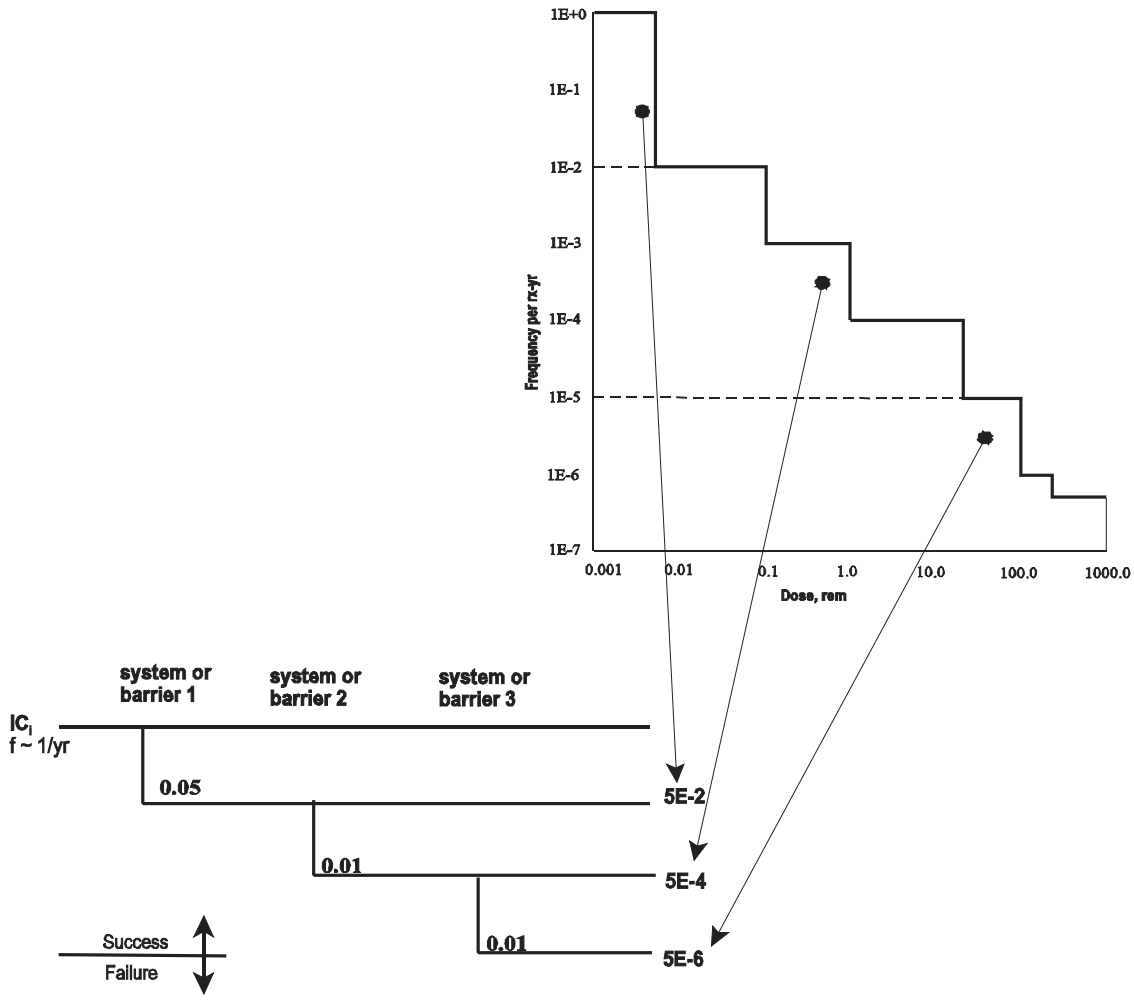

Figure 6-6 LBE selection schematic example.

The LBE associated with a relatively high frequency of 5E-2/yr has to have, by design, little consequence in terms of dose at the boundary. The LBE sequence with a lower frequency of 5E-4/yr can have higher consequences, as shown, and the LBE with 3 failures can have even higher consequences yet, but a lower frequency of 5E-6/yr. As stated above, other sequences besides the ones shown in Figure 6-6, which belong to the same event class, will contribute in terms of frequency to the LBE frequency of that class.

The PRA has to meet the F-C curve in terms of the mean with respect to frequency and dose of the various event classes in which the accident sequences are grouped while the LBEs have to meet the F-C curve at the 95% confidence level with regard to both frequency and consequence. This gives added confidence that the design will be able to withstand the expected challenges with a high margin of safety. This process is repeated for each event class in to obtain the complete set of LBEs. Event classes with 95th percentile frequencies less than 1E-7 are identified, justified as to their uniqueness and excluded from further consideration. For the more frequent events (> 1E-2) it is possible that there is no non-zero value of the dose that is associated with any of the event sequences. In that case, engineering judgment may be used to select the sequence as a LBE.

As noted, an alternative LBE selection process may be needed for the highest event frequency category (i.e., events with frequencies $ 1E-2 per year). In this frequency region, the PRA sequences may not lead to any releases or releases with any measurable consequences at the site boundary, hence it would be difficult to use the PRA to select the LBEs in this region. For this region, engineering judgment or experience (based, for example, on the event that is regarded as the most challenging with respect to SSC design criteria and plant safety) and knowledge of the physics of the design may be used to select the LBEs for each class of events, for reasons of practicality. Since the PRA being used is a living PRA, LBEs can change if the PRA changes during the life of the plant. Requirements related to the living PRA are stated in Chapter 7 and Chapter 8.

In addition, as indicated in Figure 6-5, further LBEs can be added, if needed, based on the designer's or reviewer's judgement. This may be done, for instance, to analyze the performance of a particularly critical design feature that has not been fully exercised in the other LBEs (a particular design feature which renders certain sequences not risk significant could be scrutinized here); or it may be necessary to supplement the selection of LBEs[(2.18)] where uncertainties may not be adequately addressed in the PRA.

It should be noted that the main reason for including rare events is to ensure that no potentially high consequence event is excluded due to the uncertainty in frequency alone. This provides additional confidence in the robustness of the design to withstand low frequency, high consequence events with regard to risk goals (such as the QHOs).

An example application of the selection process described above can be found in Appendix E.

6.2.2.2 Deterministic Selected LBE

In Chapter 4 a defense-in-depth principle was introduced to protect against unknown phenomena and threats, i.e., to compensate for completeness uncertainty impacting the magnitude of the source term from an accident. The principle ensures that regardless of the features incorporated in the plant to prevent an unacceptable release of radioactive material from the fuel and the reactor coolant system (RCS), there are additional means to prevent an unacceptable release to the public

[(2.18)] Note that LBEs with frequency less than 10^{-7}/ry could enter the design basis via this requirement.

should a release from the fuel and RCS occur that has the potential to exceed the dose acceptance criteria.

Accordingly, as a deterministic defense-in-depth provision, each design needs to have the capability to establish a controlled low leakage barrier in the event plant conditions result in the release of radioactive material from the fuel and reactor coolant system in excess of anticipated conditions. The specific conditions regarding the barrier leak tightness, temperature, pressure and time available to establish the low leakage condition will be design specific. The design of the controlled leakage barrier should be based upon a process that defines an event representing a serious challenge to fission product retention in the fuel and coolant system. This event should be agreed upon between the applicant and the NRC consistent with the technology and safety characteristics of the design. The event could represent an assumed fuel damage event, such as a graphite fire in an HTGR. (Chapter 8 provides additional examples.)

The deterministic LBE event is to be analyzed mechanistically to determine the timing, magnitude and form of radionuclide released into the reactor building, and the resulting temperature, pressure and other environmental factors (e.g., combustible gas) in the building over the course of the event. The timing of closure and the allowable leak rate should then be established such that the worst two-hour dose at the EAB and the dose at the outer edge of the LPZ for the duration of the event do not exceed 25 rem TEDE.

A dose of 25 rem is the current offsite dose guideline for design basis accidents in 10 CFR 50.34 and 10 CFR 100. It is also the dose that defines an abnormal occurrence (AO) as described in the Commission's April 17, 1997, policy statement on AOs (62 FR 18820) which defines substantial radiation levels to imply a whole body dose of 25 rem to one or more persons.

As noted in the previous Subsection, in addition to the above deterministic LBE, other LBEs can be added, if needed, based on the designer's or reviewer's judgement. This may be done, for instance, to analyze the performance of a particularly critical design feature that has not been fully exercised in the other LBEs (a particular design feature which renders certain sequences not risk significant could be scrutinized here); or it may be necessary to supplement the selection of LBEs[(2.19)] where uncertainties may not be adequately addressed in the PRA.

6.2.3 Selection of Risk Significant SSCs

In the technology neutral process the aim is to incorporate a safety classification scheme in which all the plant SSCs fall into two categories, safety significant or non-safety significant, distinguished by whether the SSC needs special treatment or not[(2.20)]. However, for those classified as safety significant, the special treatment they receive will vary since the treatment will be aligned with the mission the SSC needs to fulfill. In other words, the treatment ensures that the SSC will perform reliably (as postulated in the PRA) under the conditions (temperature, pressure, radiation, etc.) assumed to prevail in the accident scenarios for which the SSC's successful function is credited in the risk analysis.

The term 'safety significant' is used in the framework to designate those systems needing special treatment. The safety significant SSCs can be identified in a technology-neutral sense as those SSCs that are relied upon to remain functional during the LBEs. That is, the safety significant

---

[(2.19)] Note that LBEs with frequency less than 10^{-7}/ry could enter the design basis via this requirement.

[(2.20)] This differs from the scheme for current reactors, where distinction is made between 'safety related,' 'safety significant,' and 'important to safety' equipment. The current definitions of these terms are provided in the glossary.

SSCs are those whose functionality plays a role in meeting the acceptance criteria imposed on the LBEs. Since the safety significant SSCs are linked to the LBEs and the LBEs were chosen in a risk-informed manner, the framework approach for selecting SSCs for special treatment is also risk-informed.

Other SSCs, besides those required for the LBEs may also be included with appropriate justification. The justification could be based on the risk importance of the SSC in the PRA model. Special attention will also have to be paid to safety important inherent design features that may not be obvious in the PRA model. However, because of the way the LBEs are selected, as described in the previous section, it would appear unlikely that an SSC would have high risk importance in the PRA, but not be needed in the LBEs, and any such findings would have to be investigated thoroughly.

The justification for additional safety significant SSCs could also be based on defense-in-depth considerations presented in the framework via the six defense-in-depth principles:

(1) measures against intentional as well as inadvertent events are provided

(2) the design provides both accident prevention and mitigation capability

(3) accomplishment of key safety functions is not dependent on a single element of design, construction, maintenance or operation

(4) uncertainties in SSCs and human performance are accounted for in safety analyses

(5) the design has the capability to prevent an unacceptable release of radioactive material

(6) plants are sited at locations that facilitate protection of public health and safety

The possible risk importance calculations alluded to above would have to use other risk measures than the CDF and LERF used for LWR calculations. For calculating SSC risk importance based on the F-C curve a process like the following could be used:

1) From the PRA that is carried out as part of the design of the plant, all sequences that can potentially result in a dose at the site boundary greater than a certain selected dose, for example $ 1 rem, are selected.

2) Next, an importance measure or measures (IM) are defined. These measures can be defined analogous to importance measures related to core damage frequency (CDF) or large early release frequency (LERF) for LWRs, i.e., analogous to risk achievement worth, RAW, risk reduction worth, RRW or the Fussell-Vesely, F-V. This IM can be based, for example, on the notion of a “1 rem exceedance frequency”, EXF[1], i.e., the sum of frequencies of all sequences that exceed the criterion of a 1 rem dose at the site boundary.

3) Then the value(s) of the IM related to EXF[1] is calculated for all SSCs that appear in the sequences that result in doses greater than 1 rem. These are trial values of IM. If desired, additional weight can be given in the definition of IM to SSCs that appear in (lower frequency) sequences leading to higher values of dose at the site boundary, e.g., in excess of 25 rem, 50 rem, or 100 rem as displayed on the F-C curve. This would involve calculating analogs of IM that are related to EXF[25], EXF[50], EXF[100], etc., and then choosing appropriate weights for the values of IM that result, in order to calculate the total value of the importance measure.

Such a process may be useful for providing graded treatment to the safety significant SSCs related to their importance measures. The type of treatment that safety significant SSCs receive is determined from the conditions that the SSC is assumed to operate under, based on the scenarios where it is needed. Verification of the functionality of the SSC under the required conditions is demonstrated via a reliability assurance program.

For the safety-significant SSCs, programmatic requirements related to quality assurance and control, testing, monitoring, etc. will be applied. The process envisaged here also includes a "living" PRA that extends to plant operation. Requirements related to a living PRA can be found in Chapter 7 and Chapter 8. As stated previously, the living PRA could impact the selection of licensing basis events that were originally selected based on the design PRA. Based on operational experience, input from maintenance, inspection, and new knowledge (from experiments, tests, and theoretical advances) the PRA would be updated. Updates to the design PRA based on operational experience could lead to a change in the risk profile of the plant based on a new identification of the event sequences that are major risk contributors. Therefore the set of SSCs designated as safety significant, based on LBEs, defense-in-depth, and possibly importance measures, would also be periodically re-analyzed based on data from the living PRA. Any change in the risk analysis results could lead to a change in the risk-significant SSCs: a finding that some SSCs previously designated as non-safety significant are now needed for limiting risk, or a finding that previously safety significant SSCs are no longer needed for limiting risk. A reassessment of defense-in-depth would also be needed to verify that existing safety significant SSCs are sufficient for defense-in-depth, or to verify that the newly designated non-safety significant SSCs are not needed any more for defense-in-depth.

An example application of the selection process described above can be found in Appendix E.

6.3 Safety Margin

Safety margin is incorporated into the Framework as an element of defense-in-depth. Adequate safety margin is achieved through the selection of a bounding set of licensing bases events, the use of enveloping and/or conservative codes and assumptions and the selection of suitable acceptance criteria in order to provide confidence that the plant operation will not result in unexpected consequences [Ref. 2.12]. This margin provides a means of accounting for quantifiable uncertainties and provides some measure of protection against those uncertainties that cannot be quantified.

Adequate safety margins are inextricably linked to acceptance criteria – limiting values imposed on safety parameters to ensure that a physical barrier or system fulfills its intended function. Thus, when operating conditions stay within the acceptance criteria, the barrier or system has a negligible probability of loss of function, and an adequate safety margin exists [Ref. 2.13]. The framework requires safety margin for specific acceptance criteria and encourages the use of margin beyond that required by the framework, to minimize changes in the licensing bases (e.g., the identification of new licensing bases events) that may result from unexpected changes in performance or knowledge.

6.3.1 Bounding Set of Licensing Bases Events

The Framework includes a process for identifying a complete set of probabilistic LBEs that bounds all PRA event sequences that are greater than 1E-8. It also includes a deterministic LBE that addresses the limiting challenge to the final radiological barrier to address uncertainties that are not fully known. The identification of this complete set of LBEs is key to ensuring that adequate

safety margin is achieved as it provides the starting point for which codes, standards and assumptions are applied.

The use of a design-specific PRA to identify a bounding set of LBEs ensures that unique accident behavior and phenomena are assessed. The use of a deterministic LBE for assessing the challenge to the final radiological barrier adds margin for completeness or knowledge uncertainty.

6.3.2 Use of Enveloping and/or Conservative Codes and Assumptions

The set of LBEs are analyzed to verify compliance with the Framework's acceptance criteria and defense-in-depth requirements. The analyses of these events need to account for uncertainties related to the codes and plant conditions. Generally, there is no restriction on how close to the acceptance criteria the results may go, but the acceptance criterion can not be exceeded in any LBE.

6.3.3 Suitable Acceptance Criteria

There are two applications of LBE safety margin within the Framework: consequence margin and frequency margin. Consequence margin is the difference between the predicted dose and acceptance dose for a given LBE frequency. It is determined by comparing the predicted dose to the applicable dose on the frequency-consequence curve. Frequency margin is the difference between the calculated frequency and the frequency used to establish the acceptance criteria and the defense-in-depth requirements.

For consequence margin, the probabilistic requirements for the LBEs dose consequence calculation are determined using the 95th percentile value for the resulting dose. For frequency margin, the framework approach for determining an LBE's frequency is based on the 95th percentile of the appropriately combined frequencies from the individual sequences that are in the event class represented by the LBE. This approach increases the evaluated frequency of the LBE and potentially results in a lower maximum acceptance dose and a possible shifting of the LBE into a higher frequency category with more restrictive defense-in-depth requirements. In addition, the PRA event sequence frequencies are influenced by the selection of reliability and availability goals. If margin is included in these goals by the designer, then this margin will be reflected in the overall frequency of each event sequence.

6.3.4 PRA Event Sequences

Success criteria are used to distinguish the path between success and failure for components, human actions, trains, systems, structures and sequences. In all cases, the success criteria are to be fully defensible and biased towards success such that issues of manufacturer or construction variability, code limitations and other uncertainties are unlikely to shift a success path to a failure path. The Framework does not specify a safety margin for success criteria used within the event sequences. However, the degree of bias included in the success criteria needs to consider the individual impact of the shift of an event sequence success path to a failure path. The Framework also requires the establishment of reliability and availability goals for SSCs within the PRA. These goals may vary depending on the SSC's function and/or importance. These goals should be such that variations in SSC performance are unlikely to change the selection and characteristics of the LBEs.

6.4 Security Performance Standards

The purpose of this section is to define the performance standards to be used in assessing the adequacy of security for new plants. The goal of the performance standards is to ensure multiple lines of defense are provided against security related threats and that there are no significant vulnerabilities to the threats considered. It is expected that each new plant will be required to perform a security assessment integral with the design. The scope and guidelines for performing the security assessment are discussed in Section 8.6. The results of the security assessment are to be compared to the performance standards (to be defined). The security performance standards are still under development and will be included in a future update of the framework.

7. PRA TECHNICAL ACCEPTABILITY

7.1 Introduction

The purpose of this chapter is to establish the high-level requirements for PRA scope and technical acceptability that are necessary to support the PRA applications identified in the technology-neutral framework. These requirements were developed in recognition of the increased role that PRA will play in the establishment of the licensing framework for new reactors and the limitations of the current guidance, requirements and standards due to their specificity towards the existing light water reactors (LWRs).

As stated in Chapter 1, it is expected that future applicants will rely on PRAs as an integral part of their license applications. This integration of PRA into the design and licensing process creates new challenges in the construction and maintenance of PRAs, and causes completeness, defensibility and transparency to be more important than ever in the past. Traditionally, the scope of LWR PRAs has been confined to the analysis of beyond design basis accidents, i.e., accidents leading to severe core damage. With the framework approach, the PRA and therefore the scope of the PRA has to encompass a whole spectrum of off-normal events including frequent, infrequent and rare initiating events and event sequences. These events include a spectrum of releases from minor to major and sequences that address conditions less than the core damage sequences of the current reactors and those similar to current reactor core damage sequences. It also needs to address the dose consequences of these event sequences as measured at the site boundary, LPZ boundaries and at one mile.

The scope needed for the framework is also broader than that typically considered in today's PRAs. It not only needs to address at-power and shutdown reactor operation, but also needs to be able to support the assessment of non-traditional events, such as; security, fuel handling events, radiological waste events.

One of the objectives of the technology-neutral framework is to develop a framework that is applicable to all types of reactor designs, including gas-cooled, liquid metal, and heavy and light-water-moderated reactors. Current guidance, requirements and standards are constructed on the bases of applying PRAs to LWR applications. Metrics such as core damage and large early release may not be applicable to some advanced reactor designs. The current set of PRA levels that addresses progression to core damage, containment response and public-health consequences may also be less applicable as these are technology specific to LWRs. Therefore, in addition to issues associated with the role of the PRA, the applicability of the available guidance needs to be assessed and updated to reflect the application of PRAs in the technology-neutral framework.

The consideration of uncertainties is a vital part of understanding the extent of the risk. Therefore, part of the examination of the design is identification, evaluation, and management of uncertainties.

Future reactor designs are likely to make more extensive use of passive systems and inherent physical characteristics to ensure safety, rather than relying on the active electrical and mechanical systems. As a result, the assessment of potential errors that occur during the design, manufacturing, fabrication and/or construction processes will be critical to ensuring safety. These latent errors are especially important for advanced designs, in which there is likely to be greater reliance than in the past on factory fabrication (as opposed to field fabrication).

As such, this chapter presents the high-level requirements for PRA scope and technical acceptability that account for the above issues. Section 7.2 addresses the application of the PRA

in the framework. It collects and summarizes the framework uses of the PRA. Section 7.3 identifies the high-level requirements necessary to ensure the scope and technical adequacy of PRA for framework applications. This section builds on existing PRA quality requirements delineated in Regulatory Guide 1.200 and the currently available PRA standards.

Methods to help establish PRA quality are also provided in Section 7.3. The methods include the establishment of a PRA quality assurance program, the use of consensus standards which provide supporting requirements to the proposed high-level technical requirements identified in Appendix F, and an independent peer review process. The use of PRAs in the licensing of advanced reactors and operation (e.g., the maintenance of LBEs) will require PRAs to be living documents. Section 7.3.9 addresses the need to update and manage the configuration of the PRA to reflect changes in plant operation and design and to review if past licensing decisions are still valid.

7.2 PRA Applications in the Framework

PRA plays a significant role in the framework. Its primary mission is to generate a complete set of accident sequences including a rigorous accounting of uncertainties. These sequences are used to evaluate the level of safety by comparing the PRA results with the Quantitative Health Objectives and the Frequency-consequence curve. They are also used to generate the set of Licensing Basis Events (LBEs). These LBEs are assessed against the framework's LBE acceptance criteria using the calculated frequency and consequence of the PRA sequences. The generation of sequences and LBEs, and other applications of the PRA within the framework are presented using the following life-cycle phases of the plant: design, construction, startup and operation. PRA requirements for each phase are summarized below. The identified application bullets are explained in the sections following this summary.

Design

The PRA developed during the design phase will likely evolve as the design matures. Although the framework is structured around an evolving PRA analysis that both influences the design and is influenced by the design, the PRA applications listed below are expected to be completed when the design is submitted for licensing.

- Generate a Complete Set of Accident Sequences
- Develop a Rigorous Accounting of Uncertainties
- Evaluation of the PRA Results Against the Quantitative Health Objectives
- Evaluation of the PRA Results Against the Frequency-Consequence Curve
- PRA Supported Assessment of Security
- Identification and Characterization of the Licensing Bases Events
- Identification and Characterization of the Special Treatment SSCs
- Support the Environmental Impact Statement (EIS) and the Severe Accident Mitigation Design Alternative (SAMDA) Analysis Development

The PRA submitted for licensing is to reflect the proposed design and the expected operation and performance of the plant staff and equipment.

Construction

Future reactor designs will likely use passive systems and inherent physical characteristics to ensure safety, rather than relying on the active electrical and mechanical systems. However, fabrication and construction errors are one way in which design assumptions can be invalidated. Therefore, the identification of adverse latent conditions that could occur during fabrication and

construction will be critical to ensuring safety. As such, risk-informed inspection insights will help focus inspectors to maximize the likelihood of identifying these conditions. In addition, changes that occur during construction need to be reflected back into the PRA and assessed for their impact on the level of safety. The following PRA-related activities are expected to occur during fabrication and construction.

- Maintain a Living PRA
- Risk-informed Inspections

Startup

This phase focuses on the initial staffing, training and programmatic issues that are expected to be finalized prior to startup and includes the following activities:

- Maintain a Living PRA
- Support the Determination of Staffing Requirements
- Support the Development of the Technical Specifications (or equivalent)
- Support the Development of Inspection, Testing and Preventative Maintenance
- Support the Development of Procedures and Training
- Support the Development of Emergency Preparedness

Operation

On completion of the design, construction and startup phases, the updated PRA reflecting the final design and operating philosophy will continue to be used to support licensing activities and plant operations. As this PRA is directly integrated into the design and licensing processes, it requires a comprehensive maintenance and update process. In addition, it is expected that a risk-informed philosophy will be integrated into the operation of the plant at a greater level than that of the current plants. The following activities are expected:

- Maintain a Living PRA
- Assess and Manage Operational Risk
- Assess and Manage Plant Changes
- Monitor SSC Performance
- Maintain a Risk-informed Training Program

7.2.1 Generate a Complete Set of Accident Sequences

A key mission of the PRA analysis is to generate a complete set of accident sequences. These sequences are the foundation for many of the PRA's framework applications and are a direct input into the determination of the proposed design's level of safety. They encompass a whole spectrum of off-normal events including frequent, infrequent and rare initiating events and event sequences. They include a spectrum of releases from minor to major and sequences that address conditions less than the core damage sequences of the current reactors and those similar to current reactor core damage sequences. These sequences will also be used to aid in the application of the design's deterministic requirements including the assessment of barrier integrity requirements; protective system redundancy, diversity, reliability and availability requirements; and protective action effectiveness. As stated in Chapter 8, events that could defeat the protective systems, barrier integrity and protective action strategies simultaneously need to be identified and are required to be less than 1E-7/plant year. The application of the PRA to each protective action strategy is discussed below.

Physical Protection

The PRA application to this protective strategy is discussed in Section 7.2.5.

Stable Operation

The PRA will be used to develop a complete set of initiating events. As discussed in Chapter 8, one of the defense-in-depth requirements will be to establish cumulative limits on frequency of these initiating events. Similar to the three categories developed for event sequences in Chapter 6, initiator events will also be divided into categories of frequent, infrequent and rare events each with a cumulative frequency limit. These limits will help to ensure there is a reasonable balance between plant challenges, accident prevention and mitigation.

Note that initiating event consideration for future designs may differ substantially from what is done for current LWRs. Given the unfamiliarity and lack of operating experience with advanced designs, search techniques such as master logic diagrams may have to be employed to identify initiators. This is similar to what was done early on in the application of PRA to LWRs, and has been done in the application of PRA to DOE facilities, medical systems, etc.

Protective Systems Requirements

Deterministic requirements have been established for the functions of reactivity control (reactor shutdown) and decay heat removal. A review of the PRA event sequences will aid in ensuring that for frequent and infrequent event sequences, there are redundant, diverse and independent means for reactor shutdown and decay heat removal as discussed in Chapter 8.

The framework also requires the establishment of reliability and availability goals for the SSCs within the PRA. Therefore, the PRA sequences need to reflect these goals. These goals may vary depending on the sequence frequency. Protective systems responding to events that are expected to occur one or more times during the life of the plant (frequent events in Chapter 6) should have high availability and reliability, whereas protective systems that are in the design to respond to events not expected to occur (infrequent and rare events in Chapter 6) may have a lower availability and reliability. The results of the sequences will confirm the adequacy of these goals. Note that these goals need to be consistent with the expected performance of the equipment and will be monitored during the operation phase.

Protection against common-cause failures has been, and will continue to be important as these types of failures can be expected to dominate the unreliability of systems with some degree of built-in redundancy. The PRA will provide a means of assessing the importance of common cause failures and provide the designer the ability to ameliorate the potential for these failures through selection of diverse materials, components, and manufacturing processes. It is worth noting that the current treatment of common cause failures is often data-driven, i.e., historical data is use to determine which common cause events are most likely and, hence, should be incorporated into the PRA. While some of this data may be relevant to new plants, other information (including qualitative and quantitative screening) may be needed to identify significant common cause events associated with new or novel equipment.

Barrier Integrity Requirements

The PRA will aid in the determination of what barriers need to be in the design and how they should be designed. As discussed in Chapter 6, sequences that are categorized as Frequent can not contain any failed barriers and those categorized as Infrequent must have at least one barrier remaining intact. The PRA generated sequences will be used to verify that this requirement is met.

Barriers also need to be designed to maintain their integrity during the normal operational conditions such that their failure does not become an initiating event. The assessment of initiating event frequencies including those resulting from barrier failures such as loss of coolant accidents is in the scope of the PRA.

Protective Actions Requirements

The human action analysis used to support the development of the accident sequences needs to be consistent with the protective actions in the proposed EOPs, accident management and EP procedures; and the proposed staffing levels. It is also expected that the EOPs, accident management and EP procedures will be developed with insights from the PRA such that all relevant accident PRA sequences are addressed. The analysis of accident sequences will also help to ensure that dependence on a single protective action included in these procedures does not prevent an exceeding of the frequency - consequence curve.

7.2.2 Develop a Rigorous Accounting of Uncertainties

In applying PRA to future reactor designs, analysts must start with a clean page, i.e., not be biased by expectations from the conclusions of PRAs on old designs. Part of the examination of the unexpected is identification, evaluation, and management of uncertainties.

Uncertainties must be addressed in the calculation of both frequencies and consequences of the event sequences. Since the sequences include rare events and event combinations postulated to occur in complex systems for which there may be limited experience, the consideration of uncertainties are a vital part of understanding the extent of the risk.

Uncertainties in some functional areas may make it difficult to conclude that adequate protection is provided and could lead to the need for additional safety enhancements, such as additional design features to provide more defense-in-depth, additional testing, and additional oversight by the NRC, all with the aim of achieving a high level of safety and confidence. Expected areas where high uncertainty related to modeling and completeness may be present include accident phenomenology, digital electronic instrumentation and control systems (including software and “smart” systems), human reliability, and passive system performance.

Sensitivity studies (e.g., alternative success criteria) are an important means for examining the impacts of modeling uncertainties. This will be of special use early in the licensing process, as the staff can use the PRA to highlight important areas of uncertainty where more research may be required to reduce the uncertainty, or, if the uncertainty cannot be reduced, where more defense-in-depth may be needed. The PRA can be used to examine the tradeoff between reducing the uncertainty through research and adding defense-in-depth or additional safety margin to cope with the uncertainty.

A range of uncertainties in future reactor performance need to be considered including the following:

- Parameter uncertainty associated with the basic data; while there are random effects from the data, the most significant uncertainty is epistemic - is this the appropriate parameter data for the situation being modeled.

- Model uncertainty associated with analytical physical models and success criteria n the PRA can appear because of modeling choices, but will be driven by the state-of-knowledge about the new designs and the interactions of human operators and maintenance personnel with these systems.

- Completeness uncertainty associated with factors that are not accounted for in the PRA by choice or limitations in knowledge, such as unknown or unanticipated failure mechanisms, unanticipated physical and chemical interaction among system materials, and, for PRAs performed during the design and construction stages, all the factors affecting operations (e.g., safety culture, safety and operations management, training and procedures, use of new I&C systems).

All identified and quantified uncertainties (aleatory and epistemic) need to be included in the PRA that support the PRA applications within the framework. The PRA directly uses the results of parameter estimation in the data uncertainty distribution for its basic events. It also uses many results of sensitivity studies to address uncertainty in success criteria, plant conditions and other models - sometimes incorporating model uncertainty, sometimes bounding it. It is important to qualitatively describe and catalog all aspects of uncertainty, even those difficult to quantify, for consideration in balancing structuralist and rationalist aspects of the framework.

7.2.3 Evaluate the Quantitative Health Objectives (QHOs)

As stated in Section 3.1.2, the level of safety that future reactors are expected to meet are the QHOs for each event sequence and for the aggregate of all the event sequences. This means the PRA results must demonstrate that the total integrated risk from the PRA sequences satisfy both the latent cancer QHO and the early fatality QHO. Therefore, the PRA sequences need to be able to characterize the offsite consequences of an accidental release of radioactive material in impacts on human health.

7.2.4 Evaluate the Frequency-Consequence Curve (F-C Curve)

As discussed in Chapter 6, the F-C Curve relates the frequency of potential accidents to acceptable radiation doses at the site boundary. The sequences of the PRA will populate the space under the F-C Curve. Some scenarios will have little or no consequences, primarily because of the inherent characteristics and design features of the plant. Others are likely to approach the F-C Curve and thus make up the important contributors to the plant risk profile. Therefore, in addition to the human health effects discussed in Section 7.2.3, the PRA event sequences need to be able to generate dose estimates. For frequent events, this estimate is for the annual dose to a receptor at the EAB. For infrequent events, this estimate is for the dose at the exclusion area boundary. For rare events this estimate is for the 24-hour dose at one mile from the EAB.

7.2.5 Support the Assessment of Security

Physical protection assessment involves consideration of the potential threat, the potential targets, and the potential consequences. Analysts consider two broad classes of targets: material targets for theft of nuclear material and equipment targets for attack, sabotage or theft of information. Targets are identified using a systematic process to ensure completeness.

In contrast to the identification of material targets, the identification of attack or sabotage targets requires a more complex and analytical process. In this process, typically, an adversary must damage or disable the functions of a number of different equipment items to create a radiological release, or disrupt operations. A target set is defined as a minimum set of equipment functions that must be damaged or disabled to generate a radiological release. In a facility, there will commonly be multiple possible target sets. The number and diversity of equipment functions in each target set provide a measure of the system's redundancy and diversity.

Target set identification is performed routinely during the design of physical protection for nuclear facilities. The approach is similar to that used in PRA to identify combinations of equipment functions (cutsets) that, if failed, could generate radiological releases. PRA studies can provide a starting point for the identification of potential radiological sabotage targets, but must be modified in two ways. First, for attack and sabotage, the probability of multiple, simultaneous failures of diverse and redundant components may be increased substantially. Second, the probability of failure for passive components that normally have high reliability (walls, fire barriers, doors, vessels, etc.) can also increase.

7.2.6 Identify and Characterize the Licensing Bases Events (LBEs)

The identification and characterization of LBEs is derived from the PRA's accident sequences.

Identification

As discussed in Chapter 6, LBEs are bounding PRA event sequences that are subjected to additional analysis and, for the higher frequency sequences, are required to meet additional deterministic criteria. This additional treatment of these events provides added assurance that the design has adequate defense-in-depth and sufficient margin. LBEs are chosen by grouping similar event sequences and associating an LBE with each grouping as described in Chapter 6.

Acceptance Criteria

In addition to meeting the F-C Curve, LBEs categorized as frequent and infrequent are required to meet deterministic requirements as described in Chapter 6. The PRA is used to identify event sequences that fall into various categories defined by frequencies that are ultimately identified as LBEs and assigned deterministic requirements based on these categories.

7.2.7 Identify and Characterize the Treatment of Safety-Significant SSCs

The PRA is used to both identify and characterize the safety-significant SSCs. The requirements for identification and treatment are discussed below.

Identification

The framework's approach for selecting safety-significant SSCs is based on those SSCs that are relied upon to remain functional during the LBEs. Since the safety significant SSCs are linked to the LBEs and the LBEs were chosen in a risk-informed manner, the framework approach for selecting SSCs for special treatment is also risk-informed. Other SSCs, besides those required for the LBEs may also be included based on risk importance measures that result from a plant-specific PRA.

Special Treatment

For those SSCs classified as safety significant, the special treatment they receive will vary since the treatment will be aligned with the mission the SSC needs to fulfill. In other words, the treatment ensures that the SSC will perform reliably (as postulated in the PRA) under the conditions (temperature, pressure, radiation, etc) assumed to prevail in the accident scenarios for which the SSC's successful function is claimed in the risk analysis.

7.2.8 Support the Environmental Impact Statement (EIS) and the Severe Accident Mitigation Design Alternative (SAMDA) Analysis Development

Section 102 of the National Environmental Policy Act (NEPA) (42 USC 4321) directs that an environmental impact statement (EIS) is required for major Federal actions that significantly affect the quality of the human environment. Included in the EIS is a requirement to assess alternatives to the proposed action. This requirement has been codified in 10 CFR 51, Environmental Protection regulations for Domestic Licensing and Regulatory Functions, as requiring an environmental impact statement for issuance of a permit to construct a nuclear power reactor, testing facility or fuel reprocessing plant. The environmental report is required to include an analysis that considers and balances the environmental effects of the proposed action, the environmental impacts of alternatives to the proposed action, and alternatives available for reducing or avoiding adverse environmental effects. This is commonly referred to a the Severe Accident Mitigation Design Alternative (SAMDA) analysis. The SAMDA analysis presents the environmental impacts of the proposal and the alternatives in comparative form. Where important to the comparative evaluation of alternatives, appropriate mitigating measures of the alternative need to be discussed. The PRA is used to support the identification and assessment of these alternatives.

7.2.9 Maintain a Living PRA

The PRA used to support licensing needs to be maintained throughout the construction, startup and operation phases. During these phases, it is expected that the PRA will be maintained consistent with the plant's current performance and design. This will require the monitoring of SSCs included in the PRA to ensure their reliability, availability and performance are sufficient to support the goals of the design certification PRA. It will also require the monitoring of changes in the initiating event scope and frequency, modeling, software, industry experience, etc. In addition to monitoring the PRA inputs, a process will be required that evaluates the impact of deviations in performance or design and maintains the risk-informed framework applications and ultimately the level of safety.

The PRA will be a "living" PRA to a much greater extent than has been common practice for current LWRs. As such, and because the PRA is being used as an input to the plant's licensing basis, it is possible that changes in the PRA will result in the identification of new LBEs or safety significant SSCs as time passes or result in the shifting of an LBE from one frequency category to another. The potentially dynamic nature of the identification and characterization of LBEs and safety significant SSCs makes a formal configuration change process a necessity.

7.2.10 Risk-informed Inspections during Fabrication and Construction

The PRA will provide insights regarding the importance of various plant features and can be used to help identify items for inspection.

Construction errors are one way in which design assumptions can be invalidated. Techniques such as HAZOP may provide useful search schemes for identifying those construction errors that can cause the facility to operate outside the design assumptions. This will require creativity on the part of the PRA analysts beyond the routine that has arisen from the repeated application of PRA to the current generation of LWRs.

The PRA identification of safety-significant SSCs will provide a list of components for which it may be important for the NRC to conduct inspections during the fabrication process. This is especially important for advanced designs, where there is likely to be greater reliance than in the past on

factory fabrication (as opposed to field fabrication). In addition, components may be fabricated outside the U.S., possibly to non-U.S. codes and standards.

7.2.11 Startup

Startup addresses those risk-informed activities that will likely continue to evolve following the receipt of a license but need to be in place prior to reactor startup. These are discussed below:

Support the Staffing Requirements

In developing requirements for staffing, the burden should be on the applicant to demonstrate through modeling of human actions, the use of simulators and/or mockups, and the PRA analysis that staffing is adequate for the evaluated level of safety. The determination includes the assessment of human actions needed which should be consistent with those in the PRA and the reliability of these actions assumed in the PRA. Consideration need to be given to conditions that could shape the action's failure probability such as: complexity, time available for action completion, procedure quality, training and experience, instrumentation and controls, human-machine interface and the environment.

Technical Specifications

Technical Specifications of the past prescribed out-of-service equipment configurations with specific allowed outage times (AOTs) and action statements. In contrast, advanced designs may rely much more on risk-informed Technical Specifications, where allowed equipment configurations and AOTs are fluid, changing as the plant configuration changes. The risk impact of configuration changes will likely be measured by a risk monitor, which in turn relies on the plant PRA. Furthermore, the PRA (input to a risk monitor) will consider all modes of plant operation and will consider both internal and external initiators. This treatment of the plant configuration will be a more integrated assessment than that for current LWRs.

Lessons learned from efforts to risk-inform the technical specifications for currently operating LWRs will be considered in developing the technical specification requirements and any implementing guidance.

Inspection, Testing and Preventive Maintenance

With regard to inspection and testing, the requirements will be set consistent with the importance of a particular SSC within the PRA. Preventive maintenance designed to maintain an assumed reliability will be balanced against increased unavailability of the SSC resulting from the preventive maintenance. It is envisioned that the SSC reliability monitoring program discussed in Section 7.2.9, Maintaining a Living PRA, will also support the process of developing an effective maintenance program.

Development of Procedures and Training

The PRA can provide valuable insights regarding the importance of human actions, which can then be emphasized in procedures and training programs. It is expected that procedural guidance will be developed for all actions credited within the PRA and that training will be risk-informed.

Development of Emergency Preparedness

The analysis of the plant PRA helps to determine the measures that are effective in limiting the public health effects from radionuclide release accidents so that public health effects remain below the limits set in the QHOs.

7.2.12 Operation

The integration of PRA into the design and licensing process enables a coherent application risk into operational processes associated with the design, operation and maintenance of the plant. Some of these processes are discussed below.

Assess and Manage Operational Risk

The Maintenance Rule, 10 CFR 50.65, establishes the requirements for monitoring the effectiveness of maintenance at current plants. It is envisioned that a similar program will exist for future reactors including assessment and management of the increase in risk that may result from proposed maintenance activities. For current reactors, this assessment is to be performed prior to the maintenance activities.

Assess and Manage Plant Changes

In 10 CFR 50.59, Changes, Tests and Experiments, the process for which a current licensee may make changes in the facility or procedures as described in the final safety analysis report and conduct tests or experiments not described in the final safety analysis report without obtaining a license amendment is addressed. As the licensing bases of future reactors are risk-informed, it is expected that the new reactor change process will be fully integrated with the framework's LBE risk-informed acceptance criteria and deterministic defense-in-depth requirements.

Monitor SSC Performance

The SSC monitoring program will confirm the reliability, availability and performance of equipment assumed in the licensing process and will be a part of the living PRA program as describe above.

Maintain a Risk-Informed Training Program

Insights gained from the PRA can help ensure safe operation and need to be integrated into the operation and technical support staff training programs. This will ensure the staff is knowledgeable of the potential initiating events and analyzed accident sequences.

7.3 Functional Requirements for PRAs for Future Plants

This section addresses the functional requirements for PRAs for future plants used to support the framework. These requirements address the following topics:

- Technical Requirements
- Quality Assurance Criteria
- Consensus Standards
- Assumptions and Inputs
- Analytical Methods
- Analytical Tools
- Independent Peer Review

- Documentation
- Configuration Control

Each of these topics is discussed below.

7.3.1 Technical Requirements

Appendix F identifies the high level requirements necessary to ensure the technical adequacy of a PRA used in the licensing, construction, startup and operation of a new reactor. The required scope of the PRA and the corresponding requirements for each technical element are addressed. Specifically, high-level requirements are provided for all the technical elements of a PRA required to calculate the frequency of accidents, the magnitude of radioactive material released, and the resulting consequences. Requirements are also provided for the scope of the PRA which is defined by identification of the complete set of challenges including both internal and external events during all modes of operation.

A key mission of the PRA analysis is to generate a complete set of accident sequences. These sequences are the foundation for many of the PRA's framework applications and are a direct input into the determination of the proposed design's level of safety. They include a spectrum of releases from minor to major and sequences that address conditions less than the core damage sequences of the current reactors and conditions similar to current reactor core damage sequences. This is illustrated by the event tree shown in Figure 7.1. The functions and end states included in this event tree are for illustration purposes only and are not met to represent a current or new plant. For current PRAs, sequences like 1 and 2 would be considered successful and therefore would not be included in the results of the PRA. Sequences similar to 3 through 7 may or may not be included in current PRAs depending on the degree of fuel damage and the degree of conservatism used in the PRA. Sequences 8 through 10 would be core damage sequences included in the results. For a PRA supporting the framework, all these sequences are of interest. Sequences 1 and 2 would likely be considered frequent events, depending on the initiating event frequency and the failure probabilities of the event tree functions, with no or limited release of radionuclides. Given no fuel damage, the potential for radionuclide release would be bounded by the allowable activity within the primary coolant or activity associated with other radiological sources. Sequences 3 through 7 would likely have higher allowable doses as a result of the limits established by the frequency consequence curve discussed in Chapter 6 and the lower frequencies of these sequences due to the increase number of failures. These intermediate sequences may require that different levels of system success criteria be defined within the PRA models to properly assess the dose consequences. Sequences 8 through 10 would need to be of a low enough frequency to allow the higher doses that will likely result from severe fuel damage.

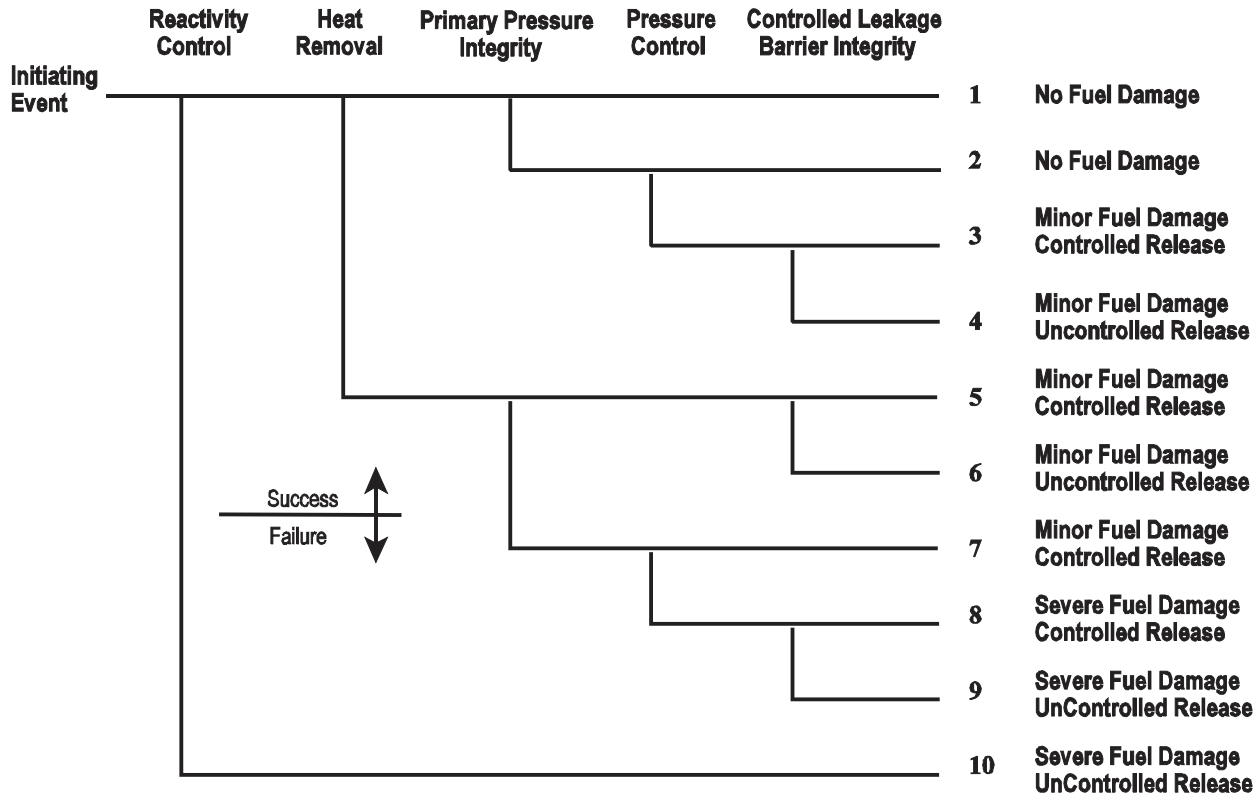

Figure 7-1 Event Sequence Example

Initiating event consideration may also be substantially different from those for current US LWRs. Examples are events associated with on-line refueling, recriticality due to more highly enriched fuel and fuels with higher burnup, and chemical interactions with some reactor coolants or structures. For these reasons, more emphasis will be required on the use of systematic methods to identify the initiating events modeled in the PRA. Searches for applicable events at similar plants, if available (both those that have occurred and those that have been postulated), and use of existing deductive methods (e.g., master logic diagrams, top logic models, fault trees, and failure modes and effects analysis) could both be utilized in this effort.

Appendix F builds on existing PRA requirements delineated in Regulatory Guide 1.200 and the currently available PRA standards. The requirements focus on a PRA of the reactor core but also address other radioactive materials (e.g., spent fuel and radioactive waste) that need to be considered to effectively evaluate risk.

7.3.2 Quality Assurance Criteria

The PRA analyses supporting the framework will be subject to quality control. Given the integration of the PRA into the design and licensing process, the need for completeness, defensibility and transparency are more important than ever in the past. This translates directly into the need for more rigorous quality control requirements than those that are typical for PRAs supporting current

reactors. Table 7-1 list the applicable quality control requirements for a PRA that is supporting a framework analysis [Ref. 2.14] and [Ref. 2.15].

Table 7-1 PRA Quality Assurance Requirements

Topic		Requirement
1	Quality Assurance Program	At the earliest practicable time, consistent with the schedule for the developing, modifying and maintaining the PRA, a quality assurance program needs to be established with written policies, procedures, or instructions and need to be carried out throughout the life cycle of the analysis.
2	PRA Staff	Measures are established to provide for indoctrination, training and qualification of personnel performing PRA-related activities to assure awareness in quality assurance processes and controls and to ensure suitable technical proficiency is achieved and maintained.
3	Requirements and Standards	Measures are established to assure that applicable regulatory requirements and standards are specified and included in the development and maintenance of the PRA and that deviations from such standards and requirements are controlled.
4	Interface Control	Measures are established for the identification and control of PRA process interfaces and for coordination among interfacing design organizations. These measures shall include the establishment of procedures among participating organizations for the review, approval, release, distribution, and revision of documents.
5	Independent Reviews	The PRA control measures shall provide for verifying or checking the adequacy of the PRA, such as by the performance of independent checks and peer reviews. The independent verifying or checking process need to be performed by individuals or groups other than those who performed the original analysis, but may be from the same organization. In addition to the independent checks, an independent peer review process, as described in Section 7.3.7, need to be performed.
6	Procedures	Activities affecting PRA quality are prescribed by documented instructions or procedures and need to be accomplished in accordance with these instructions or procedures.
7	Document Control	Measures are established to control the issuance of PRA documents. These measures shall assure that documents, including changes, are reviewed for adequacy and approved for release by authorized personnel. Changes to documents need to be reviewed and approved by the same organizations that performed the original review and approval unless designated to another responsible organization.
8	Corrective Actions	Measures are established to assure that conditions adverse to PRA quality are promptly identified and corrected. In the case of significant conditions adverse to quality, the measures shall assure that the cause of the condition is determined and corrective action taken to preclude repetition. The identification of the significant condition adverse to quality, the cause of the condition, and the corrective action taken is documented and reported to appropriate levels of management.
9	Audits	A comprehensive system of planned and periodic audits is carried out to verify compliance with all aspects of the quality assurance program and to determine the effectiveness of the program. The audits are performed in accordance with written procedures or check lists by appropriately trained personnel not having direct responsibilities in the areas being audited. Audit results need to be documented and reviewed by management having responsibility in the area audited. Followup action, including reaudit of deficient areas, need to be taken where indicated. This audit requirement is in addition to the independent peer review requirements of Section 7.3.7.

7.3.3 Consensus PRA Standards

One acceptable approach to demonstrate conformance with the regulatory position is to use an industry consensus PRA standard or standards that address the scope of the PRA used in the decision making. The PRA standard must be applicable to the design of the plant and to the PRA applications specified in the framework.

7.3.4 Assumptions and Inputs

7.3.4.1 Assumptions

Assumptions used in the PRA supporting a framework analysis need to be realistic and defensible with their basis and application clearly documented. They should not use significantly conservative or optimistic assumptions and should not use expert judgement except in those situations in which there is a lack of available information regarding the condition or response within the PRA, or a lack of analytical methods upon which to base a prediction of a condition or response. The assumption also should not take credit for SSCs beyond rated or design capabilities or heroic human actions that have a small probability of success. The PRA shall include an assessment of uncertainty of the results for important or key assumptions both individually and in logical combinations.

Key assumptions are those that are related to an issue in which there is no consensus approach or model (e.g., choice of data source, success criteria, reactor coolant pressure seal loss-of-coolant model, human reliability model) and in which the choice of approach or model has an impact on the PRA results in terms of introducing new accident sequences, changing the relative importance of sequences, or affecting the overall results.

7.3.4.2 Inputs

All inputs need to be traceable to a clearly identified source and consistent with the proposed design.

7.3.5 Analytical Methods

The analytical methods used in a PRA supporting a framework analysis need to be sufficiently detailed as to purpose, method, assumptions, design input, references and units such that a person technically qualified in the subject can review and understand the analysis and verify the adequacy of the results without recourse to the originator. Where possible, analytical methods need to be consistent with available codes and standards and checked for reasonableness and acceptability. Method-specific limitations and features that could impact the results need to be identified.

7.3.6 Analytical Tools

PRA quantification software, thermal/hydraulic codes, structural codes, radionuclide transport codes, human reliability models, common cause models, etc. are typically used in the PRA quantification process These models and codes shall have sufficient capability to model the conditions of interest and provide results representative of the plant and need to be used only within known limits of applicability. As errors in such programs may significantly impact the results, it is necessary that the development and application of the computer programs, spreadsheets or other calculation methods exhibit a high level of reliability as ensured through a documented verification and validation process. Verification is a systematic approach to ensure the model or computer code correctly represents the model or code's design. Validation is the demonstration that the verified models or codes meet the requirements. In addition, users need to demonstrate

the appropriateness of the models or codes selected for a specific application and of the way in which these programs are combined and used to produce the needed results (Ref. [Ref. 2.16]).

7.3.7 Independent Peer Review

A PRA that supports a framework application needs to be peer reviewed. An adequate peer review is one that is performed by qualified personnel, according to an established process that compares the PRA against the characteristics and attributes, documents the results, and identifies both strengths and weaknesses of the PRA.

7.3.7.1 Team Qualifications

Team qualifications determine the credibility and adequacy of the peer reviewers. To avoid any perception of a technical conflict of interest, the peer reviewers will not have performed any actual work on the PRA. Each member of the peer review team must have technical expertise in the PRA elements he or she reviews, including experience in the specific methods that are used to perform the PRA elements. This technical expertise includes experience in performing (not just reviewing) the work in the element assigned for review. Knowledge of the key features specific to the plant design and operation is essential. Finally, each member of the peer review team must be knowledgeable in the peer review process, including the desired characteristics and attributes used to assess the adequacy of the PRA.

7.3.7.2 Peer Review Process

The peer review process includes a documented procedure used to direct the team in evaluating the adequacy of a PRA. The review process compares the PRA against desired PRA characteristics and attributes. In addition to reviewing the methods used in the PRA, the peer review determines whether the application of those methods was done correctly. The PRA models are compared against the plant design and procedures to validate that they reflect the as-built and as-operated plant. Key assumptions are reviewed to determine if they are appropriate and to assess their impact on the PRA results. The PRA results are checked for fidelity with the model structure and for consistency with the results from PRAs for similar plants based on the peer reviewer's knowledge. Finally, the peer review process examines the procedures or guidelines in place for updating the PRA to reflect changes in plant design, operation, or experience.

7.3.8 PRA Documentation

A PRA used in a framework application need to be documented such that a person technically qualified in PRA can review and understand the analyses and verify the adequacy of the results without recourse to the originator. The documentation needs to be traceable and defensible with sources of information both referenced and retrievable. It needs to support the determination that the PRA is performed consistent with the applicable standards and the technical requirements contained within the framework and its implementing requirements. The documentation also needs to be maintained current with the plant configuration and the PRA model. The methodology used to perform each aspect of the work need to be described either through documenting the actual process or through reference to existing methodology documents. Key sources of uncertainty need to be identified and their impact on the results assessed. Key assumptions made in performing the analyses need to be identified and documented along with their justification to the extent that the context of the assumption is understood. The results (e.g., products and outcomes) from the various analyses need to be documented. This documentation entails both submittal and archival

documentation. PRA information submitted in support of a new plant application will form part of the licensing basis and, as such, is expected to be docketed.

7.3.8.1 Submittal Documentation

To demonstrate that the technical adequacy of the PRA used in an application is consistent with the expectations and requirements of the framework, the staff expects the following information to be submitted to the NRC:

- **Quality Assurance** – a description of the PRA quality assurance program including the methods used to implement the requirements of Section 7.3.2. Also include a description of the PRA configuration control program used to implement the requirements of Section 7.3.9.

- **Scope and General Methodology** – a description of the scope of the PRA and the overall methodology used in the analysis.

- **Technical Requirements and Consensus Standards** – documentation that demonstrates that the PRA is performed consistent with the framework's technical requirements and the identification of consensus standards applied and a description of the extent of their application.

- **Assumptions and Inputs** – a description of all assumptions, their bases and applications. For key assumptions or other sources of uncertainty, an assessment of the impact of the uncertainty on the results, both individually and in logical combinations needs to be included. These assessments provide information to the NRC staff in their determination of whether the use of these assumptions and approximations is either appropriate and whether sensitivity studies performed to support the decision are appropriate. A list of significant inputs and their application also should be provided.

- **Analytical Methods** – a description of all analytical methods, including selection of empirical factors, data inputs and limitations.

- **Analytical Tools** – a description of all analytical tools including models and computer codes and the verification and validation process used to ensure their accuracy.

- **Logic Models** – all event trees and fault trees with supporting bases information. Include information on structure, initiating events, top events and basic events, including human actions and common cause.

- **Reliability and Availability Data** – a description of the approach used to develop the reliability and availability data including a discussion on the application of reliability and availability goals.

- **Results** – the necessary results to demonstrate that the acceptance criteria are met including the identification of key sources of uncertainty and the treatment of uncertainty within the analysis.

- **Peer Review** – a discussion of the peer review process, the results of the peer review for each reviewed element and comment resolution specifying the action taken to address and resolve identified issues. Also include descriptions of the peer review team members and their qualifications.

7.3.8.2 Archival Documentation

This documentation includes all supporting calculations, procedures and references that were used to demonstrate that the acceptance criteria are met. This documentation is to be maintained as lifetime quality records in accordance with Regulatory Guide 1.33 by the applicant, as part of the normal quality assurance program, so that it is available for examination.

7.3.9 Configuration Control

The PRA used to support the framework needs to be maintained throughout the construction, startup and operation phases of the plant. Therefore a PRA configuration control program should be developed early in the design process and needs to be in place at the time the PRA is submitted for NRC staff review. This program includes the following key elements:

- a process for monitoring PRA inputs and collecting new information.
- a process that maintains and upgrades the PRA to be consistent with the current configuration of the plant as it progresses through construction, startup and operation.
- a process that ensures that planned plant and procedure changes are assessed prior to their implementation to ensure that the licensing acceptance criteria and deterministic defense-in-depth requirements are maintained valid.
- a process that ensures that unplanned changes in performance, new insights or methods, previously unidentified deficiencies or other issues impacting the PRA results are assessed in a timely manner to ensure that the licensing acceptance criteria and deterministic defense-in-depth requirements are maintained valid.
- a process that ensures the cumulative impact of pending changes is considered when applying the PRA.
- a process that evaluates the impact of changes on any other previously implemented risk-informed decisions that have used the PRA.
- a process that maintains configuration control of computer codes used to support PRA quantification.
- documentation of the Program and periodic reporting of updated results to the NRC.

These requirements are based on the requirements for PRA configuration controls for current reactors (Ref. [Ref. 2.17]) with modifications reflecting the various phases of the plant's life cycle and the integral role PRA plays in the licensing process. This results in the need for a more integrated risk-informed monitoring and change evaluation process and specific reporting requirements.

During the construction, startup and operation phases, planned plant and/or procedure changes are to be evaluated for their impact on the licensing acceptance criteria and deterministic defense-in-depth requirements prior to their implementation. This process is expected to be similar to the current 10 CFR 50.59 process where a safety evaluation screening process is typically performed on all proposed changes. Proposed changes need to be consistent with the framework's acceptance criteria prior to implementation of the proposed change.

During operation, a process similar to the monitoring of the performance and condition of structures, systems, or components, against licensee-established goals of 10 CFR 50.65, the Maintenance Rule, is expected to be an integral part of the monitoring program for the PRA. This process will use the framework's reliability and availability goals as the key input for the operational phase monitoring program. Monitoring will consist of periodically gathering, trending and evaluating information pertinent to the performance, and/or availability of PRA related SSCs and comparing the result with the established goals and performance criteria to verify that the goals are being met [Ref. 2.18]. When the goals are met, the plant's performance is consistent with the licensing bases. When a goal or performance criteria is not met, then assessment of the impact of the performance issue on the PRA and licensing bases is required. Cause determination and corrective actions may also be required. Performance issues that result in the failure of a framework acceptance criteria will require licensing action.

Unexpected changes in performance, methods or knowledge can result in changes to the PRA and to the frequency or consequence of identified LBEs or in the identification of new LBEs not previously analyzed. These changes can also impact the identification of safety significant SSCs as a result of their impact on the PRA importance measures. The framework encourages the use of design margin to minimize the impact of PRA changes on the licensing bases. Changes that reduce margin but do not impact the Framework''s required safety margin will not require a re-assessment of the LBEs or the defense-in-depth measures. For plants built according to a certified design, if a proposed change modifies the certified (Tier 1 or Tier 2) portion of the design, a rule change to amend the certification or an exemption request is required.

The PRA update frequency is primarily dependent on the scope and nature of pending changes. It is expected that frequent updates will be performed to minimize the need to separately assess pending changes and to avoid the potential complexity of evaluating the cumulative impact of these changes. A maximum update interval of 5 years is proposed. It is expected that a report containing all plant changes, tests and experiments consistent with similar 10 CFR 50.59 requirements, including a summary of the risk-informed evaluation of each change will be submitted at intervals similar to that of the 10 CFR 50.59 reporting requirement (report of plant changes, tests and experiments at a frequency not exceed 24 months). Included with these submittals is an assessment of the cumulative impact of the changes, including unplanned changes as described above, and an assessment of these changes on the plant's safety margin.

8. REQUIREMENTS DEVELOPMENT PROCESS

8.1 Introduction

The purpose of this chapter is to describe the process for the development of the technology-neutral requirements and to summarize the application of the process to identify the topics which the technology-neutral requirements must cover to ensure the success of the protective strategies. Only the topics which the requirements must address (and any additional guidance regarding the scope and nature of those requirements) are included in this chapter.

As discussed in Chapter 1, the technology-neutral requirements that are to be developed using the guidance contained in the framework are envisioned to be a comprehensive, stand-alone set of requirements that could be incorporated into the regulations as a new 10CFR part that would be an alternative to the 10CFR50 requirements for licensing of new NPPs.

Since a stand-alone new 10CFR part is envisioned, it must be complete with respect to administrative, as well as technical requirements and interface with the other parts of 10CFR similar to 10 CFR 50. To accomplish the above, the approach taken is to ensure that all necessary provisions of 10CFR50 (e.g., technical, process, administrative, etc.) must also appear in the new technology-neutral requirements. Accordingly, since 10CFR50 has some requirements that are already technology-neutral (including technical, process and administrative), it would make sense to carry these over into the new technology-neutral requirements since there is already implementing guidance and experience in their use. It is envisioned that this be accomplished by using as many of the existing 10CFR50 requirements as is reasonable based upon their technology-neutral characteristics. Appendix G of the framework identifies those 10CFR50 requirements considered technology-neutral and recommended to be used. Where those requirements also have technology-neutral Regulatory Guides (RGs), it is intended to use those same RGs for additional implementing guidance. Where new Regulatory Guides are needed for the technology-neutral requirements, they will be written in a technology-neutral fashion, whenever possible. Otherwise they will be written technology-specific.

Discussed below is the process used to identify the topics which the requirements must address (Section 8.2), the application of that process to the technical (Section 8.3) and administrative (Section 8.4) areas, guidelines to be followed in developing the actual requirements (Section 8.5), technology specific considerations (Section 8.6), and how the results of applying the process were checked for completeness (Section 8.7).

8.2 Process for Identification of Requirements

The framework structure described in Chapters 2 through 7 defines an overall set of safety objectives, protective strategies, and criteria for a technology-neutral, risk-informed approach for future plant licensing. The next step is to identify and define the topics which the detailed technical and administrative requirements must address to ensure the safety objectives, protective strategies, and criteria in Chapters 2 through 7 are met. The process for the identification of the topics is shown in Figure 8-1.

For each protective strategy ,a logic tree (Figure 8-2) is developed that identifies what would need to occur to fail the protective strategy (Box 1). As discussed in Chapter 5, these logic trees are developed in a deductive manner that leads to the potential root cause of the failure, that is, identifying the different ways in which the strategy under consideration can fail. At the top level,

each logic tree has three branches. These branches represent three basic pathways that can lead to the failure of a protective strategy.

To understand the meaning of these logic trees, recall the integrated and iterative nature of the design and licensing analysis[2.21] process. As a conceptual design is perfected, lessons from the licensing analysis lead to changes in design requirements, which in turn are reflected in revision to the analysis. As the design is implemented, engineers select specific off-the-shelf components, define performance requirements for new components, develop production processes for new fuel and equipment manufacture, and define QA/QC and test requirements.

All the protective strategy logic trees follow the same basic top logic structure to organize the kinds of failures that can occur and, therefore, to help identify the requirements needed to develop confidence in the performance of the strategies. As illustrated in Figure 8-2, "Functional Failure of a Protective Strategy" can occur in three ways:

1) "Failure to Perform Consistent with the Assumptions of the Licensing Analyses"

The licensing analysis (PRA, deterministic, LBE calculation, etc.) reflects the design expectations for protective strategy performance. If the design is not implemented and maintained in a way to ensure the continuing validity of the licensing analysis, the protective strategy may not provide the anticipated defense-in-depth.

- Errors in the detailed implementation of the design requirements (e.g., specific pump or valve selection or digital I & C errors) introduce errors in system and component performance.

- Construction or installation errors that substitute improper equipment, introduces flaws, or that impede proper operation (e.g., inadequate ventilation of electronic equipment) also can introduce errors in system and component performance.

- Maintenance errors can disable equipment beyond the availability and reliability calculations of the PRA (e.g., installing an improper software update can fail all redundant I&C and protection equipment), thus introducing errors in performance.

- Operations errors also can defeat redundancy and lead to failures beyond those modeled in the PRA. In particular, systematic change in procedures, training, or crew practices (e.g., communications, evaluation, use of procedures) can have sweeping effects.

- Updating the PRA (which is a key part of the licensing analysis) as the design becomes specific, after construction for the as-built plant, routinely as equipment performance and operations practices change, and as evidence of aging accumulates, can reduce the likelihood of failing to perform consistent with the licensing analysis.

2) "Failures Due to Improper Analysis or Implementation of Licensing Requirements"

The licensing analysis is the bases for believing that the design meets the NRC safety, security and preparedness expectations. Errors in the analysis can obscure or mask the risk. The licensing requirements development process in this chapter (and specialized to specific technologies , as they are developed) are the basis for confidence that the design is implemented and maintained in accordance with the assumptions and results of the licensing

[2.21] Licensing Analysis includes all safety analysis performed to support design and licensing.

analysis. Failure to properly implement these requirements means that the risk could become greater than expected.

3) "Unanticipated Challenges / Failures"

This pathway acknowledges completeness uncertainty. There may be initiating events and scenarios not identified in the PRA. This "completeness uncertainty" is not a hopeless problem. While some systemic uncertainty always remains, it can be reduced in a number of ways:

- More thorough and systematic search schemes can be developed for identifying initiating events and scenarios in the PRA.
- Experimental and test programs can address technical knowledge gaps, both basic knowledge gaps and performance under unusual conditions.
- Application of defense-in-depth provisions to help compensate for the uncertainty.

Under each of these three basic pathways, additional branches were developed to identify the root cause of failure. This process was then used as a guide to identify what requirements need to be developed to guard against the root cause of failure, consistent with the overall safety philosophy and criteria discussed in Chapters 2 through 7.

Accordingly, the end point of each branch developed in the logic trees translates into one or more questions corresponding to each of the potential root cause failures. That is, based on the causal events (or the basic events in the fault tree), a series of questions (Box 2) were developed, the answers to which identify the actions that need to be taken to ensure the protective strategy is successful. To facilitate going from the logic trees to the questions, each end point of each branch in the logic trees and each question corresponding to that end point have a unique identifying number (e.g., pp-1 for physical protection - question 1).

The answers to the questions for each protective strategy (Box 3) leads to the identification of specific topics that the requirements will need to address to ensure adequate implementation of the protective strategies. These specific topics define the scope and content of the technology-neutral requirements.

In developing the answers to each question, other issues also need to be considered (Boxes 4 and 5). Box 4 represents the application of the defense-in-depth principles, discussed in Chapter 4, to each protective strategy to ensure that uncertainties (particularly completeness uncertainties) are properly considered at the strategy level. This can also result in additional topics being identified. For convenience, the defense-in-depth principles are repeated below:

- Measures against intentional as well as inadvertent events are provided.
- The design provides accident prevention and mitigation capability.
- Accomplishment of key safety functions is not be dependent upon a single element of design, construction, maintenance, or operation.
- Uncertainties in SSC and human performance are accounted for in the safety analyses.

- The plant has alternative capabilities to prevent an unacceptable release of radioactive material to the public.

- Plants are sited at locations that facilitate protection of public health and safety.

The intent of applying the defense-in-depth principles to each protective strategy is to ensure that defense-in-depth is considered in each line of defense, as well as in a broad sense across the entire design (i.e., protective strategies). Box 5 is intended to ensure that the risk criteria and the design criteria, as described in Chapter 6, are also implemented via the requirements. Before finalizing the topics that need to be addressed by requirements, a final check for completeness was made (Box 6). This check is performed by comparing the developed list of topics against other references. For example, comparing against the requirements for nuclear reactors developed by IAEA.

Once identified, the topics have been categorized as to whether they apply to design, construction or operation of the facility. Specifically,

- design refers to all engineering and analysis activities;

- construction refers to all on-site fabrication activities or off-site manufacturing activities that result in physical changes to the facility or material brought on-site for fabrication of the facility or for use over the life of the facility (e.g., fuel, spare parts, plant modifications, etc.);

- operation refers to all on-site activities to startup, control and shutdown the facility beginning with initial fuel load and continuing through termination of power generation and preparation for decommissioning.

It should be noted that design, construction and operations activities can occur over the life of the plant and simultaneous with each other.

The last step of the process is the actual development of the technology-neutral requirements (Box 7). This step is performed under Task 2 of the regulatory structure as described in Chapter 1. Section 8.3 describes the application of the process in Figure 8-1 to each of the protective strategies. Section 8.4 describes application of the process to the administrative area.

At the end of Section 8.3, a table summarizes the needed technical requirements and which ones can utilize existing 10CFR50 requirements. Likewise, Section 8.4 discusses the identification of topics for administrative requirements and at the end a table summarizes the needed administrative requirements and which ones can utilize existing 10CFR50 requirements. Section 8.5 provides guidance on how to take the topics identified in Sections 8.3 and 8.4 and develop requirements. Finally, in Section 8.6, technology-specific considerations are discussed and in Section 8.7, a completeness check is described.

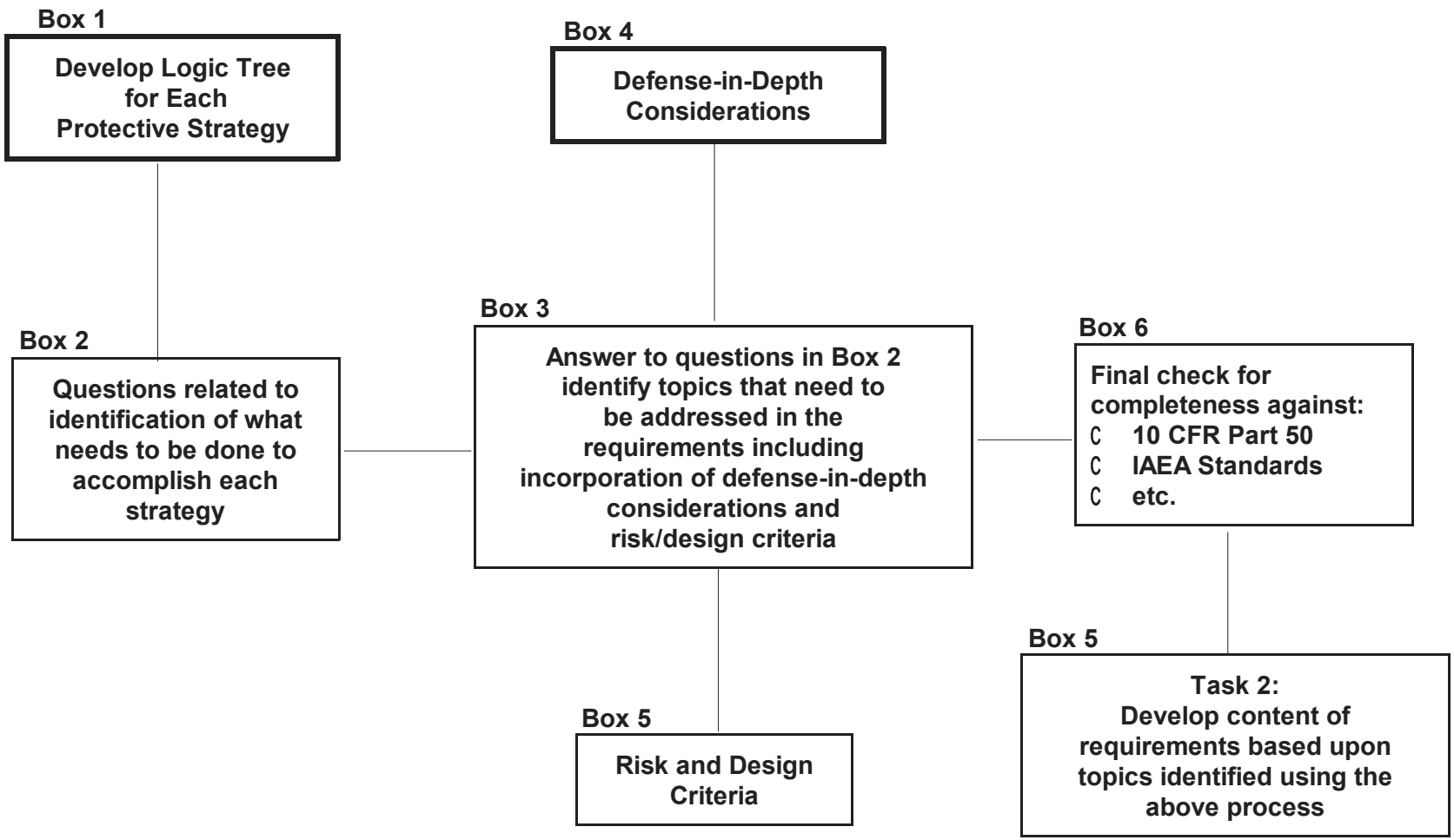

Figure 8-1 Process for identification of requirements topics.

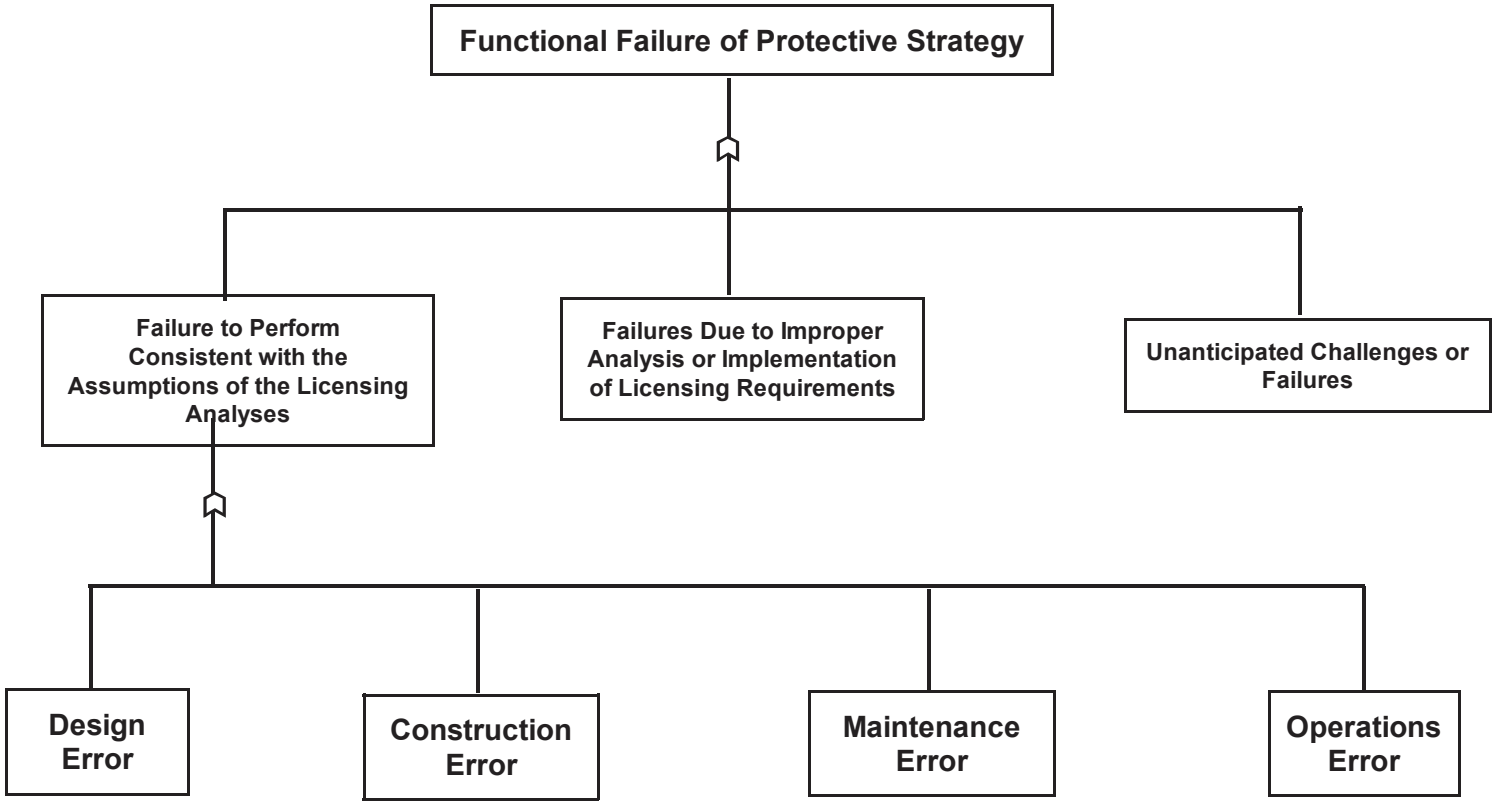

Figure 8-2 Example logic tree.

8.3 Technical Requirements: Topics for the Protective Strategies

Chapter 2 discussed a structure involving protective strategies whereby each protective strategy represents an important element of safety that, if accomplished, will ensure the design, construction and operation of the NPP results in achieving the overall safety objectives. The protective strategies discussed in Chapter 5 are:

- physical protection,
- stable operation,
- protective systems,
- barrier integrity, and
- protective actions.

The protective strategies represent a high level defense-in-depth structure for developing the requirements in that each one represents a line of defense against the uncontrolled release of radioactive material and adverse impact on the health and safety of workers and the public. The process for identification of the scope and content of the detailed technical requirements for each protective strategy is described in Sections 8.3.1 through 8.3.5 below.

8.3.1 Physical Protection

The physical protection protective strategy ensures that adequate measures (e.g., design, operating practice, and intervention capability) are in place to protect workers and the public against intentional acts (e.g., attack, sabotage) that could compromise the safety of the plant or lead to radiological release. Physical protection is applied to all elements of plant design, including the other protective strategies, and involves both extrinsic protective measures ("guns, guards, and gates") to block access to attackers and intrinsic design features to minimize their possible success should they gain access, as well as provide protection from external attack. Diversion of nuclear material is also included in the scope of this protective strategy. The logic tree in Figure 8-2 lays out the possible paths that can lead to failure of the physical protection protective strategy. At the top level, failure of the physical protection protective strategy can occur due to (1) failure of protective measures to perform consistent with assumptions in the security analysis, (2) failure due to improper analysis or implementation of requirements, and (3) failure due to challenges beyond what were considered in the design. Accordingly, the requirements must address all three of the above pathways to ensure physical protection. Discussed below are the three major pathways shown in Figure 8-3 and the topics which the requirements must address to protect against their failure.

For the first major pathway (failure of protective measures), the following three subjects must be addressed:

- theft and diversion,
- sabotage,
- armed intrusion, and
- external attack.

For theft / diversion or sabotage to be successful, there would need to be a failure to prevent or a failure to detect an unauthorized entry. Failure to prevent could be caused by failure of the personnel screening process (i.e., a person who works at the plant is the thief or saboteur) and a failure of physical barriers (e.g., doors, locks) to prohibit entry into vital areas or failure of detection devices or material control and accounting. It is recognized that 10CFR73 "Physical Protection of Plants and Materials" contains requirements to protect against theft / diversion and sabotage,

including checking for personnel trustworthiness and controlling access to plant protected and vital areas. Accordingly, 10CFR73 requirements should be applied.

Likewise, 10CFR73 contains requirements to address armed intrusion, up to and including the design basis threat (DBT). The 10CFR73 requirements address items such as the nature of the guard force, physical barriers and intrusion detection capability. Over time, if the DBT changes, the ability of the plant's physical protection capability to cope with the revised DBT would also need to be assessed.

10CFR73 also includes provisions to address certain types of external attacks. These include requirements for vehicle barriers, physical separation and multiple barriers to prevent access to vital equipment. However, not all types of external attacks are addressed in 10CFR73, particularly those by aircraft or missile.

For the second major pathway, failure prevention is dependent upon the proper implementation of 10CFR73 requirements and correct security analyses. Accordingly, ensuring proper implementation of 10 CFR 73 requirements and quality analyses is essential to the success of this protective strategy. Thus, requirements related to security quality analysis, and the use of validated safety analysis tools are essential.

For the third major pathway (challenges beyond what were considered in the design) protection is provided by the other protective strategies (i.e., they represent additional lines of defense) and by application of the defense-in-depth principles to account for completeness uncertainty, as discussed below.

Applying the defense-in-depth principles to this protective strategy suggests the following topics need to be addressed in requirements for physical protection:

- Physical protection needs to address prevention as well as mitigation. Traditional security measures, in conjunction with the other protective strategies, address both. However, considering security issues integral with the design process can lead to designs with enhanced prevention and mitigation features. Accordingly, a security assessment at the design stage should be performed. (This is discussed further below.)

- Physical protection must not be dependent upon a single element of design, construction or operation. The combination of protective measures (personnel screening, access control, barriers, etc.) defined in 10CFR73 should provide multiple layers of defense, along with the other protective strategies.

- Physical protection needs to account for uncertainties. Requiring security be considered integral with design, including a security assessment assessing beyond DBT threats, will help address uncertainties.

- Physical protection needs to be directed toward preventing an unacceptable release of radioactive material to the environment. In this regard, the security assessment should include an analysis of the release of radioactive material as a metric for decisions.

- Plant siting needs to consider the ability to implement protective measures to protect the public.

Table 8-1 summarizes the logic tree of Figure 8-3 by identifying questions that must be addressed by the technology-neutral requirements to ensure that the pathways that could lead to failure of the physical protection protective strategy are adequately covered in the requirements.

The table is organized by the three top level pathways of the logic tree and the answers to the questions in the table are the topics which must be covered by the requirements. The answers (i.e., topics) are arranged by whether they apply to design, construction, or operation.

As can be seen in Table 8-1, many of the requirements needed to address this protective strategy already exist in 10CFR73. The framework and technology-neutral requirements would not change these requirements (i.e., any future design using the technology neutral requirements would also have to meet 10CFR73 requirements). However, for defense-in-depth reasons, Table 8-1 does propose, that in addition to 10CFR73 future designs also consider physical protection in an integrated fashion as part of the design. This would require designers to perform a security assessment on their designs against a range of threats, including beyond the DBT and consider additional measures that enhance physical protection based upon a set of security performance standards (as proposed in SECY-05-0120).

Accordingly, the technology-neutral requirements need to include a requirement for such a security assessment, including security performance standards. Chapter 6 discusses the security performance standards and each application to build a nuclear power plant under the technology-neutral requirements needs to include a security assessment.

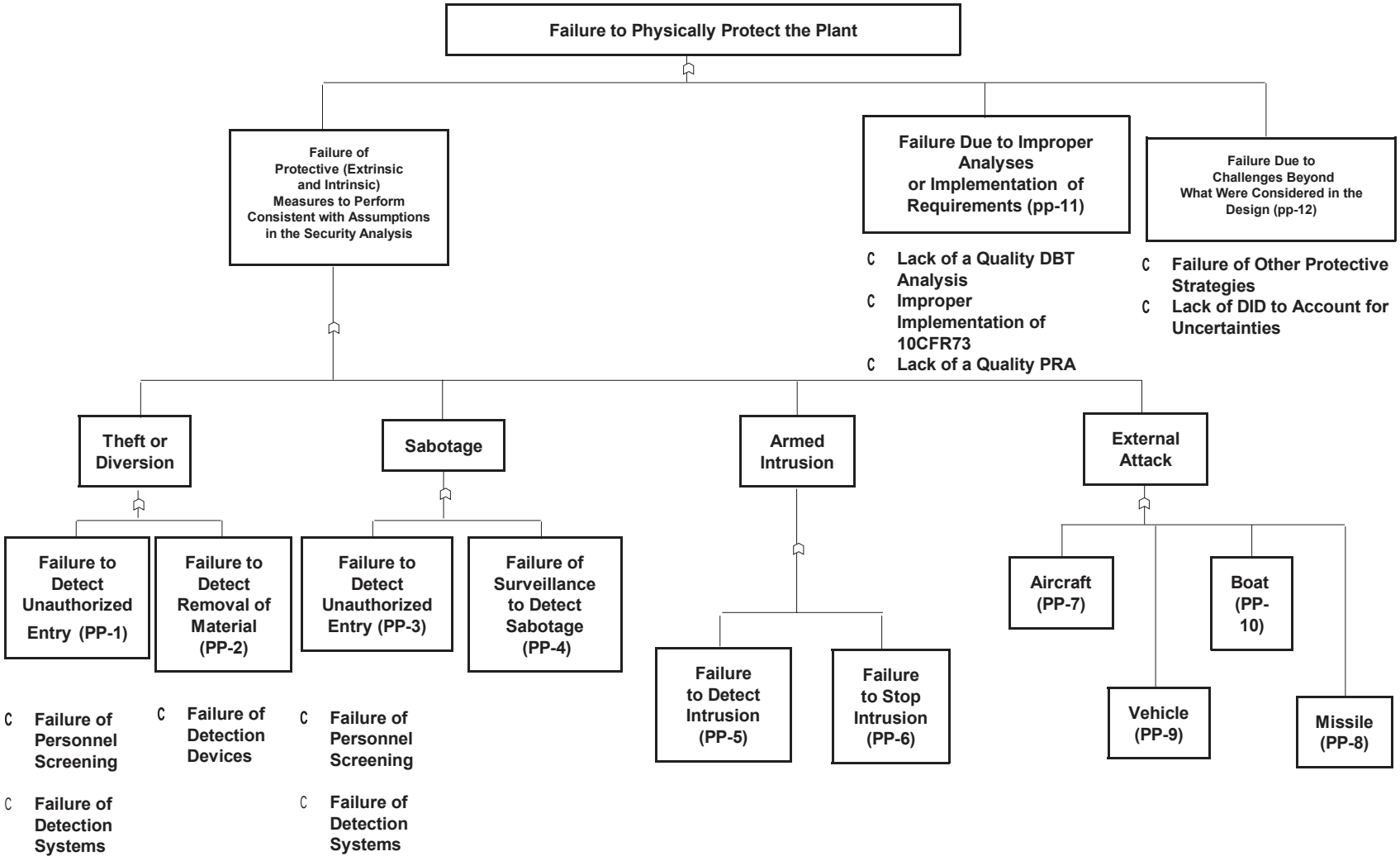

Figure 8-3 Logic tree for the physical protection strategy.

Table 8-1 Physical protection.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Failure of Protective Measures for Theft/Diversion			
• How should theft and diversion be detected? (PP-1) - detection systems	• Use 10CFR73 requirements.	• N/A	• Use 10CFR73 requirements.
• How should unauthorized removal of material be detected? (PP-2) - personnel screening - detection systems	• Use 10CFR73 requirements.	• N/A	• Use 10CFR73 requirements.
Failure of Protective Measures for Sabotage			
• How should unauthorized entry be prevented? (PP-3) - verify trustworthiness of personnel (i.e., personnel, screening) - detection systems	• Use 10CFR73 requirements.	• Access Control	• Use 10 CFR73 requirements
• How can sabotage be detected? (PP-4)	• N/A	• QA and surveillance to check for sabotage	• Surveillance to check for sabotage.
Failure of Protective Measures for Armed Intrusion			
• How can armed intrusion be detected? (PP-5)	• Use 10CFR73 requirements for detection and communication equipment.	• N / A	• Use 10CFR73 requirements for guard force, detection equipment needs and maintenance.
• How can armed intrusion be stopped? (PP-6)	• Use 10CFR73 requirements for barriers.	• N / A	• Use 10CFR73 requirements for guard force, training and maintenance of barriers.

Table 8-1 Physical protection.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Failure of Protective Measures for External Attack			
• How can vital areas be protected from external attacks from:			
• aircraft (PP-7)	• Specify process to require consideration of security integral with design (including performance standards).	• N / A	• Include in training program.
• missile (PP-8)	• Specify process to require consideration of security integral with design (including performance standards).	• N / A	• Include in training program.
• vehicle (PP-9)	• Use 10CFR73 requirements.	• N / A	• Use 10CFR73 requirements
• boat (PP-10)	• Use 10CFR73 requirements	• N / A	• Use 10CFR73 requirements.
Failure Due to Improper Analyses or Implementation of Requirements			
• How can failure be prevented due to incorrect implementation of 10CFR73 requirements or poor PRA/safety analyses? (PP-11)	• Meet 10CFR73 requirements. • Correct DBT and security analyses using validated analytical tools. • Correct security analyses.	• Meet 10CFR73 requirements. • N / A • N / A	• Meet 10CFR73 requirements. • Update analyses, as necessary, to be current with threat situation. • N / A
Challenges Beyond What was Considered in the Design			
• How can challenges beyond what were considered in the design (i.e., uncertainties) be accounted for? (PP -12)	• Apply protective strategies and DID principles. • Require a security assessment integral with design (including performance standards).	• N / A • N / A	• Surveillance to check for sabotage. • Update assessment to be current with threat situation.

N / A = Not applicable

8.3.2 Stable Operation

The stable operation protective strategy ensures that design, construction, maintenance and operating practice minimize the inadvertent challenges that could adversely impact plant performance and safety. Events will occur from time to time that cause the plant to deviate from normal conditions. Some of these events are outside the control of the designers of the plant or operating personnel such as weather, loss of offsite power and seismic events. Most, however, are within the control of the designers and the plant operating personnel such as human error, equipment failure and poor design. In either case, the plant needs to be designed for a range of events (i.e., those that are expected to occur one or more times during the life of the plant as well as those that are not expected to occur but, nevertheless, are within the frequency range of events to be considered in the design). However, the risk from plant operation is directly proportional to the number and nature of events that affect stable operation. Therefore, limiting the number and nature of these events as a protective strategy can directly improve safety.

Figure 8-4 is a logic tree that shows the various pathways that can affect stable operation. At the top level, stable operation can be affected by (1) failure to design, construct, maintain and operate the plant consistent with the assumptions in the licensing analysis, (2) failure due to improper analyses or implementation of requirements, and (3) failure due to challenges beyond what were considered in the design. Accordingly, the requirements must address all three of the above major pathways to ensure stable operation. Discussed below are the three major pathways shown in Figure 8-4 and the topics which the requirements must address to protect against their failure.

The first major pathway involves failure to maintain the assumptions in the licensing analysis. One item that can cause assumptions in the licensing analysis to not be maintained is a poor design. Such design errors could result in a design that has failed to include certain events (and, therefore, the design does not address them), wrong assumptions on equipment availability, reliability or performance (e.g., inadequate environmental qualification), design attributes that do not promote minimizing errors (e.g., poor human factors design) or other items the design failed to consider (e.g., plant aging, wrong materials, etc.). Thus the use of good engineering practices (e.g., use of accepted codes and standards, EQ, etc.) and QA in design is important to stable operation. To ensure safety significant SSCs are identified, a safety classification process should be used (see Chapter 6 for discussion). Safety significant SSCs should then receive special treatment to demonstrate their functionality. Another item that can affect stable operation is inadequate security. If protection against security related events is not sufficient, then unanticipated events affecting operation could be the result. The discussion on physical protection (Section 8.3.2) provides guidance on protection in this area.

Construction and/or fabrication errors can also cause a failure to maintain assumptions in the licensing analysis. Such errors can leave undetected flaws in structures or equipment that, when triggered by a demand or by additional degradation over time, can lead to a failure that was not assumed in the analyses. Thus, good construction and manufacturing practices are important to stable operation, as well as good QA, QC, NDE, inspection, etc.

Maintenance errors can also cause assumptions in the licensing analysis to not be met. Such errors can lead to equipment failures, plant transients or common cause failures. Good procedures, training, QA and QC can help prevent such errors.

During plant operation, a number of items could lead to events affecting stable operation that are not consistent with what was considered in the licensing analysis. Events can be caused by poor work control, misalignments or poor communication. Events can also be caused by organizations and/or personnel not performing as assumed in the licensing analysis. This could be due to poor training, procedures, personnel errors or organizational influences (e.g., lack of staff or resources).

To help protect against these kinds of failures, training programs and procedure development should incorporate the use of plant specific simulators to test procedures and train personnel.

Finally, operating limits can be exceeded that affect stable operation. Exceeding operating limits can result from a number of factors, including operator error, organizational pressures (e.g., production pressure) or equipment failure. To help protect against these kinds of failures, training programs and procedures should incorporate the use of plant specific simulators to test personnel and procedures.

Failure of the protective strategy can also be caused by improper analysis or implementation of requirements as represented by the second major pathway. The licensing analysis and the predicted plant response to postulated accidents depends upon assumptions related to equipment performance, reliability and availability and proper implementation of requirements. Thus, proper implementation and modeling of requirements (such as the event selection criteria in Chapter 6) and the use of validated analytical tools and QA are essential. Also, the use of monitoring and feed back and technical specifications to ensure key requirements / limits are implemented and emphasized.

In a risk-informed and performance-based regulatory process, performance monitoring and feedback play an important role, Accordingly, it is important that the equipment and parameters selected for monitoring align closely with the key equipment and assumptions in the licensing analysis and with the parameters identified in the performance-based requirements. With respect to the PRA, the purpose of the monitoring and feedback will be to obtain actual data on equipment reliability, availability and performance for feedback into the living PRA. Such feedback will help confirm PRA data, adjust it to conform with reality and reduce uncertainties. With respect to performance-based requirements, monitoring will be mandatory to comply with the requirements. The frequency of monitoring and feedback will need to be determined so as to achieve its intended purpose.

For challenges beyond what were considered in the design, protection is provided by the other protective strategies (i.e., they are additional lines of defense) and by application of the defense-in-depth principles to account for completeness uncertainty, as discussed below.

Applying the defense-in-depth principles to this protective strategy suggests the following topics be included in the requirements for stable operation:

- Intentional acts to disrupt operation need to be considered. Section 8.3.2 "Physical Protection" provides guidance on how to prevent and protect against such disruptions.

- Designing the plant to prevent accidents is the main emphasis of the stable operation protective strategy. To ensure that the assumptions in the PRA on IEs are preserved, each applicant needs to be required to propose cumulative limits on IE frequency for each of the frequent, infrequent and rare event frequency categories. These would then be used to ensure PRA assumptions regarding initiating event frequencies are maintained over the life of the plant. In addition, considering accident mitigation in the design can also contribute to maintaining stable operation by limiting the effects of disruption so that plant personnel and unaffected equipment can respond to the disruption and limit its affect. Accordingly, plant systems and features directed toward accident mitigation also need to be included in the design. Sections 8.2.3, 8.2.4, and 8.2.5 address such systems and features.

- Event sequences considered in the design that could disrupt stable plant operation must not be of such a nature as to defeat the protective systems, barrier integrity and protective actions strategies simultaneously. Accordingly, events with the potential to defeat all of these

strategies need to be kept to a frequency of less than 10^{-7}/plant year. Such events might include reactor pressure vessel rupture, combustible gas explosion, or energetic recriticality. Reducing the frequency of such events to less than 10^{-7}/plant year will help ensure that no single event can defeat all protective strategies.

- Uncertainties need to be considered in assessing the frequency of events that could disrupt stable plant operation. Accordingly, the PRA and safety analysis need to quantify uncertainties.

- Event sequences with the potential to simultaneously defeat the protective systems, barrier integrity and protective actions strategies need to have a frequency of less than 10^{-7}/plant year.

- The effect plant siting could have on contributing to the disruption of stable plant operation needs to be considered in the design consistent with 10 CFR 100. This would include consideration of natural as well as man-made events.

Table 8-2 presents a set of questions , based upon the logic tree in Figure 8-4, that address the pathways that can affect stable operation. The questions focus on what can be done at the design, construction and operating stage to maintain stable operation. The answers to these questions are the topics which the requirements must address to help ensure stable operation. The topics are arranged according to whether they apply to design, construction or operation. Discussed below are additional considerations related to implementation of the items discussed above.

Design Stage

At the design stage the key topics that should be covered in the requirements are related to (1) ensuring that the analysis that supports the plant design and safety is as complete as possible, is based upon accepted methods and data applicable to the design and quantifies uncertainties and (2) using good engineering practices in the design to help ensure high reliability / availability of equipment and promote good man-machine interface. Good engineering practices can generally be considered to include items such as the use of accepted codes, standards and practices; QA and QC; EQ; qualified materials and analytical tools and other items that promote good design.

Other important considerations for new plants are ensuring that the reliability and availability of equipment is consistent with assumptions in the licensing analysis (i.e., reliability assurance and special treatment), siting, the need for research and development and how to use the results of prototype testing to support licensing. Each of these is discussed below.

Reliability Assurance Program

For all safety significant equipment (as determined by the safety classification process described in Chapter 6) which is first of a kind equipment, or equipment with little operating experience under the planned conditions, the applicant will be required to have a reliability assurance program to demonstrate the reliability, availability and performance assumed in the licensing analyses. Such a reliability assurance program should include sufficient research and development, EQ, testing and analysis to demonstrate that the equipment will perform as assumed. At the operating stage, the program should also call for the monitoring of equipment performance, reliability and availability for consistency with the licensing analysis over the life of the plant, including feedback into the licensing analysis. To help mitigate the effects of aging on SSC performance, reliability or availability, an aging

management program should also be developed in conjunction with the design and implemented over the life of the plant.

Special Treatment

SSCs that are identified as safety significant (using the safety the safety classification process described in Chapter 6) are to receive special treatment to demonstrate they perform under the conditions in which they are expected to operate. Special treatment can be different, depending upon the SSC and the conditions under which it needs to perform its functions. Special treatment generally consists of one or more of the following items:

- QA / QC
- EQ (for temperature, humidity, radiation, etc.)
- Seismic qualification

For safety significant first of a kind equipment or equipment being used under new service conditions, the reliability assurance program described above will provide the special treatment. For other safety significant SSCs, the special treatment needed will be technology and design specific. The PRA will be a useful tool for identifying under what conditions the SSCs are to function and thus identifying what special treatment is needed.

Siting

Each design needs to have a link to the siting dose criteria. For current LWRs this is established through demonstrating that the releases that occur from design basis accidents do not exceed the dose criteria defined in 10 CFR 50.34(a)(1)(ii)(D) for the worst 2 hours at the exclusion area boundary (EAB) and for 30 days at the outer edge of low population zone (LPZ), as defined in 10 CFR 100.

The relationship between the technology-neutral requirements and 10 CFR 100 “Siting Requirements of Nuclear Power Plants” is intended to be one where the requirements of 10 CFR 100 would continue to apply and the technology-neutral requirements would contain requirements on the dose calculation necessary to demonstrate the “worst” 2-hour dose and the dose at the outer edge of the Low Population Zone are less than 25 rem TEDE (same requirement as is currently in 10 CFR 50.34). The dose calculation would be based upon the deterministic accident selected to meet defense-in-depth principle # 5, which requires a controlled leakage barrier, independent from the fuel and RCS, with a capability to limit releases of radioactive material to the environment to acceptable levels. As discussed in Section 8.3.4, the accident would be selected to address uncertainties in source term and would be analyzed mechanistically. However, it needs to be recognized that the technology-neutral requirements also require a range of low probability accidents (rare event category) to be analyzed and meet the doses represented by the F-C curve. Accordingly, design acceptability includes consideration of accidents beyond what has traditionally been considered.

Research and Development

Applicants are responsible for performing sufficient research and development to validate analytical assumptions and tools. Such research and development may consist of separate effects and/or integral system tests and may be conducted in full scale or partial scale facilities. In general, the requirements should specify that research and development would be expected on key plant safety features when these features are new (i.e., not previously licensed) or are to be used under conditions which go beyond previous use or experience. The scope of research and development should be sufficient to verify performance of the

features over the range of conditions for which they are expected to function, including the effects of fuel burnup and plant aging. Examples of the types of research and development which might be expected are:

- fuel performance testing (steady state and transient)
- passive decay heat removal system testing
- NDE methods testing
- reactor shutdown system testing
- materials testing.

Applicants should propose the research and development necessary to support the licensing of their designs.

Use of Prototype Testing

New plants may also propose the use of a demonstration plant, in lieu of conducting extensive research and development. In this case, the demonstration plant would be used to demonstrate the safety of the design in lieu of a series of separate research and development efforts. If such an approach is to be accepted, the applicant would need to address:

- What would be the objective of the test program:

  - Which aspects of plant safety can be addressed by demonstration plant testing?
  - Which types of analytical tools could be validated?
  - What phenomena could be addressed?

- What would be the scope of the test program:

  - How would the test program be selected?
  - Would it be conducted during initial startup only?
  - How would plant aging, irradiation, burnup effects be tested?
  - Would tests cover the full range of the accidents or only partial ranges, with the remainder done by analysis?
  - What instrumentation would be required?

- Are any special provisions needed in case the tests do not go as planned (e.g., containment, EP, has to be on a remote site, DOE site, etc.)?

- How would equipment reliability assumptions be verified?

- What acceptance criteria would be necessary (e.g., scope, treatment of uncertainties)?

- Would there be any limitations on future design changes?

- If the initial demonstration plant is to be licensed, how would this be accomplished?

Also, documentation for the test program results needs to be specified.

Construction Stage

At the construction stage, good construction practices will help ensure the plant is built as intended. Accordingly, each of the topics identified for construction is directed toward ensuring the application of good construction practices so that the plant is built as intended. Many regulatory requirements related to the construction of new plants are expected to be similar in many ways to those employed in the past (e.g, QA, QC, inspection). Where existing requirements are applicable, they will be incorporated into the new licensing structure. It is expected that NRC's role in construction will be similar to that employed previously involving QA/QC and on-site inspections. A framework regarding such inspections is contained in NUREG-1789, "10 CFR Part 52 Construction Inspection Program Framework Document" and should be used as guidance in preparing construction / inspection requirements. In addition, the PRA will provide insights regarding the importance of various plant features and can be used to help identify items for inspection. The construction of new plants, however, is expected to rely more on the following:

- factory fabrication to produce modules that can be installed in the field, thus reducing the amount of field fabrication;
- utilize components fabricated outside the U.S. and possibly to non-U.S. codes and standards; and
- in the case of HTGRs, have safety highly dependent upon the quality of the fuel fabrication and inspection process.

NRC has had experience with each of these; however, requirements will need to be developed addressing these topics, as follows:

Factory Fabrication

NRC's role in the scope of vendor inspection and transportation needs to be addressed, focusing on those aspects of fabrication and transportation that can affect safety. In particular, insights from the PRA can be used to identify key features that are important to safety and should be inspected.

Fabrication Outside the United States

The role of NRC in inspecting and regulating components fabricated outside the U.S. needs to be addressed, building upon current experience in this area. The preferred approach would be to establish requirements on the applicant to provide controls and inspections on non-U.S. vendors that ensure quality, thus putting the burden on the applicant, not NRC. NRC would then specify what documentation is to be submitted by the applicant to confirm the appropriate quality has been achieved. In addition, the use of non-U.S. codes and standards for design and fabrication will require staff review and acceptance. As directed by the Commission in its SRM of June 26, 2003, staff review of international codes and standards is to be done on a case-by-case basis, in the review of applications or pre-application submittals.

Fuel Quality

How to ensure fuel quality over the life of the plant is an issue of concern (this particularly applicable to HTGRs, whose fuel quality is key to plant safety and needs to be controlled at the fuel fabrication facility). To address fuel quality over the life of the plant, the requirements

need to cover what documentation, controls and testing an applicant / licensee must provide to ensure the fuel that is put into their reactor is satisfactory (this approach would put the burden on the licensee versus NRC to ensure fuel quality).

Operating Stage

At the operating stage, good operating practices (such as the use of procedures, training, etc.) will help minimize human errors and maintain the plant in a condition consistent with the PRA and safety analysis.

Since the operation of a NPP can have a large impact on safety and risk, it is important that the requirements for future NPPs address the key aspects of operation that are important to safety. Many areas associated with operation are expected to be similar to those for currently operating plants. For these areas, requirements for new plants can build upon and utilize much of the existing regulatory requirements, since they are largely technology-neutral in nature; however, some of the regulatory guidance in these areas may need to be risk-informed. These areas would include:

- training;
- use of procedures;
- radiation protection from routine operation (e.g., ALARA);
- maintenance;
- work control;
- configuration control; and
- surveillance, testing, ISI.

However, due to the technology-neutral nature of the proposed licensing approach, the use of PRA, the protective strategy structure and the defense-in-depth principles, certain aspects of the requirements will need to be different. Specifically, the development of requirements in the following areas will require a technology-neutral approach:

- radiation protection,
- worker protection during accidents;
- staffing;
- technical specifications;
- human factors; and
- corrective actions.

Additional discussion regarding each of these is provided in the paragraphs below.

Radiation Protection

The design also needs to consider limiting radiation doses to workers and the public from routine operation consistent with 10 CFR 20. This includes implementing the concept of "As Low As Reasonably Achievable (ALARA) for workers and for releases to the environment. In this regard, 10 CFR 50, Appendix I provides guidance on permissable releases to the environment for LWRs. The technology-neutral requirements will need to develop criteria or generic guidance to apply the ALARA concept to other technologies.

Staffing

The size, composition and role of the operating staff may be different for new plants. Factors that could affect staffing are:

- the modular nature of some designs,
- the use of passive safety features,
- longer plant response times, and
- the use of non-LWR technologies.

The PRA will be an important source of information to help establish the number, role and responsibilities of the operating staff. In developing requirements for staffing, the burden should be on the applicant to demonstrate through modeling of human actions, the use of simulators and/or mockups, the PRA and safety analysis what human actions are needed and what size and qualifications of the operating staff are necessary to carry out these actions, consistent with the guidelines for worker protection described above.

Technical Specifications

Technical specification limits for the new reactor technologies will need to be established at the technology-specific and design specific level. A scheme that utilizes insights from the PRA will need to be developed. This scheme would involve selecting events from the frequent, infrequent and rare categories that represent risk significant deviations from normal operations. Risk insights should be used to establish what SSCs are included in the technical specifications and what the limits on unavailability and allowable outage times should be. Lessons learned from efforts to risk-inform the technical specifications for currently operating LWRs should be considered in developing the requirements and any implementing guidance. It is likely that some experience will be needed in order to gain confidence in the limits that would be established by such a scheme.

Human Factors

A design that employs good human factors and man-machine interface practices will contribute to stable and safe plant operations. In this regard, guidelines have been developed for good human factors designs practices and good control room design practices for LWRs. These are found in NUREG-0711, “Human Factors Engineering Program”, and could be used as guidance to supplement the requirements. However, in general the requirements should, in a technology-neutral manner, address good human factors engineering practices that promote carrying out operations in a timely and accurate fashion, such as:

- lighting,
- accessability,
- labeling,
- color coding,
- environmental conditions (e.g., temperature, humidity, radiation),
- procedures, and
- training.

Likewise, good man-machine interface practices (especially when interfacing with computer controlled equipment) should be addressed in a technology-neutral manner in the requirements. This would include:

- navigation through computerized procedures or diagnostic systems, and
- information displays.

Guidance on good man-machine interface practices is found in NUREG-0700, "Human-System Interface Design Review Guidelines". Finally, the PRA can provide valuable insights regarding the importance of human actions, which can then be emphasized in procedures and training programs.

Corrective Actions

Establishing and maintaining a corrective action program is fundamental to ensuring good operations. However, in a technology-neutral, risk-informed approach, the PRA can provide valuable insights when problems arise regarding risk, which can factor into allowable outage times and priorities for corrective actions. Accordingly, the requirements should call for a corrective action program to be established and maintained with the following characteristics:

- the scope of the corrective action program should be defined by the scope of the PRA,

- the priority of corrective actions should be consistent with their risk importance, as identified using the PRA,

- the extent of performance monitoring should be commensurate with the safety importance of the SSCs,

- performance monitoring information should be fed back into the PRA in a timely fashion, and

- corrective actions should be directed toward ensuring the assumptions in the PRA remain valid or appropriate changes should be made to the design/operations to reflect the as monitored performance.

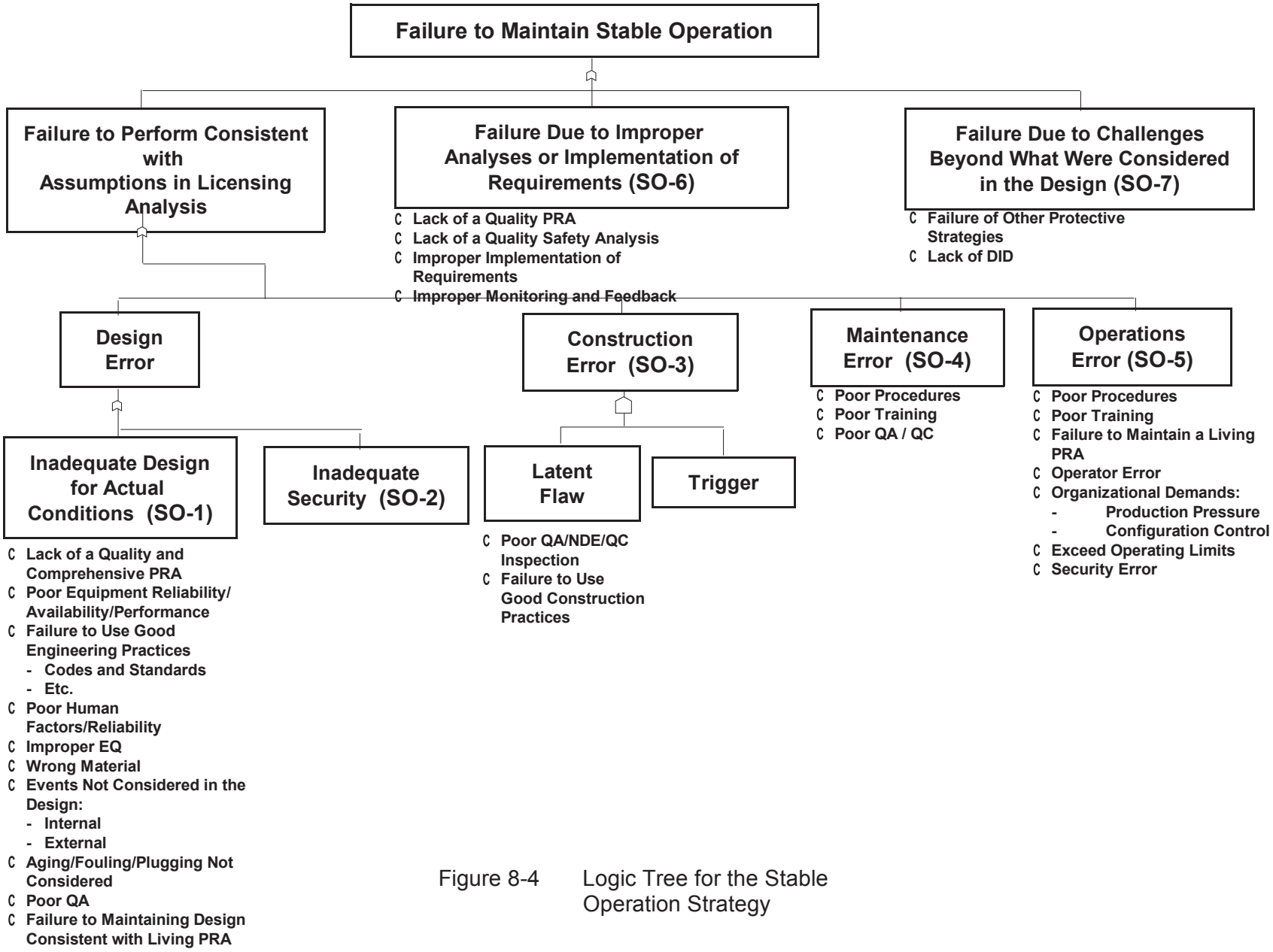

Figure 8-4 Logic Tree for the Stable Operation Strategy

Table 8-2 Stable operation.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Failure to Maintain Assumptions - Design Error			
• What needs to be done to ensure the design is adequate for the expected actual conditions? (SO-1)	• use event selection criteria in Chapter 6 • consider effect of site specific events • ensure proper scope and quality of licensing analysis and consideration of uncertainties • use of good engineering practices: - use of consensus design codes and standards - good human factors design (e.g., automatic vs. operator action) - QA - proper EQ - reactor inherent protection (e.g., no positive power coefficient) - qualified materials - qualified safety analysis tools • Research and Development • safety classification (see Chapter 6) • fire protection • prevention of brittle fracture • leak before break • consider plant aging, corrosion, etc. in the design • reliability assurance program • maintain design consistent with living PRA	• N / A • N / A • N / A • QA / QC • Testing • Inspection • N / A • N / A • N / A • N / A • N / A • N / A • N / A • N / A • N / A	• monitoring and feedback into the design • maintenance • training • procedures • ISI • IST • aging management program • living PRA • monitoring and feedback
• What needs to be done to provide adequate security? (SO-2)	• see physical protection protective strategy	• see physical protection protective strategy	• see physical protection protective strategy

Table 8-2 Stable operation.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Failure to Maintain Assumptions - Construction Error			
• What needs to be done to prevent construction or manufacturing flaws? (SO-3)	• Specify construction / manufacturing methods to be used.	• Use of good construction / manufacturing practices. • QA / QC • NDE • Inspection	• Surveillance • ISI • Testing
Failure to Maintain Assumptions - Maintenance Errors			
• What needs to be done to prevent maintenance errors? (SO-4)	• N / A	• N / A	• procedures • maintenance training • maintenance QA / QC
Failure to Maintain Assumptions - Operation Error			
• What needs to be done to limit operational errors? (SO-5)	• Consider human factors and man-machine interface as part of the design .	• N / A	• Utilize good operating practices: - training - procedures - maintenance - configuration control - use of simulators • technical specifications • security
Failure Due to Improper Analyses or Implementation of Requirements			
• How can failures due to improper analyses or implementation of requirements be prevented? (SO-6)	• Ensure plant is designed consistent with PRA and safety analysis, including event selection criteria in Chapter 6. • QA	• Ensure plant is constructed consistent with design. • QA / QC	• Ensure plant is maintained and operated consistent with PRA and safety analysis. • Monitoring and feedback • Technical specifications
Challenges Beyond What were Considered in the Design			
• How can challenges beyond what were considered in the design (i.e., uncertainties) be accounted for? (SO-7)	• Apply other protective strategies and DID principles. • Frequency of events that could simultaneously defeat the protective systems, barrier integrity and protective actions strategies should be kept below 10^{-7} per	• N / A • N / A	• Surveillance • Monitoring and feedback • N / A

Table 8-2 Stable operation.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
	plant year. • PRA needs to quantify uncertainties.	• N / A	• N / A

N / A = Not Applicable

8.3.3 Protective Systems

The protective systems protective strategy ensures that, should a challenge occur, systems are in place that will mitigate the resulting event sequences, i.e., arrest the sequences with no damage or minimize damage to the suite of barriers considered in the barrier integrity protective strategy.

The pathways leading to functional failure of a set of protective systems are shown in the logic tree of Figure 8-5. The scope of the protective systems covered by this strategy include the front line protective systems and their support systems: those systems that provide needed services to the front line protective systems (e.g., I&C, electric power, and cooling). Note that the actual definition of protective system sets that must fail to lead to the actual loss of a protective function will depend on the details of final system design. At the top level, the major pathways leading to functional failure of protective systems are (1) failure of the protective systems to perform consistent with assumptions in the licensing analyses, (2) failures due to improper analyses or implementation of requirements, and (3) failures due to challenges beyond what were considered in the design. Each of these top level pathways is discussed further below.

Items that contribute to failures in the first top level pathway are design errors, construction (which includes manufacturing) errors, maintenance and operational errors. Design errors can lead to system failure by not properly including the events or conditions under which protective systems must function, the system performance needed to respond to these events, or the support systems needed into the design. Such design errors can result from poor QA, wrong assumptions on equipment performance or reliability / availability or not using good engineering practices in the design. Failures can also result from inadequate support systems or poor design for security. Accordingly, good QA is needed along with the use of good engineering practices and validated analytical tools. Also, protective systems should receive a safety classification consistent with their safety importance to ensure they are available and operable when needed during the operating stage.

Construction and manufacturing errors can also lead to protective systems failure by introducing latent flaws or by not thoroughly testing the systems for conditions under which they are to operate. The latent flaws can be the result of poor inspection, poor QA or QC, use of the wrong material or fabrication techniques or sabotage. Accordingly, the use of good construction and QA / QC practices are important to preventing failures.

Maintenance errors can also contribute to failure of protective systems. Maintenance programs that are incomplete may miss important contributors to failure such as plant aging, corrosion, etc.

Poor training, procedures, spare parts, or QA / QC can cause maintenance errors and allow them to go undetected. Accordingly, maintenance programs should be comprehensive, including items such as aging management, and use of trained personnel and verified procedures.

Operations errors can also cause failure of protective systems. Such errors can result from poorly trained operators, poor procedures, poor work or configuration control or sabotage. Accordingly, the requirements must address these factors.

The second major pathway to failure of protective systems is that associated with failures due to improper analyses or implementation of requirements. Accordingly, ensuring quality analyses, the use of validated analytical tools and QA, along with items such as monitoring/feedback, technical specifications and safety classification should be used to ensure proper analyses and implementation of requirements during design and operation.

For the third major pathway (failures due to challenges beyond what were considered in the design), protection is provided by the other protective strategies (i.e., they are additional lines of defense) and by application of the defense-in-depth principles to account for completeness uncertainty.

Applying the defense-in-depth principles to this protective strategy leads to the following:

- Protective systems can respond to intentional acts as well as inadvertent events. As described in Section 8.3.1 "Physical Protection", security related issues and events need to be considered as an integral part of the design process. Where protective systems design can be modified to make them less vulnerable to intentional acts or better able to mitigate intentional acts, a process needs to be used (as discussed in Section 8.3.1) to guide design decisions regarding whether or not to make such modifications.

- Protective systems are provided that prevent events from leading to major plant damage as well as preventing the uncontrolled release of radioactive material to the environment should major plant damage occur. Applicants need to propose availability and reliability goals for the protective systems in consideration of the expected frequency of the events they are intended to respond to. Protective systems responding to events expected to occur one or more times during the life of the plant (frequent events in Chapter 6) should have high availability and reliability, whereas protective systems that are in the design to respond to events not expected to occur (infrequent and rare events in Chapter 6) need to have a lower availability and reliability. To ensure this concept is implemented, the requirements need to require the designer to propose availability and reliability goals for the protective systems commensurate with the above, with overall plant risk goals and with assumptions used in the PRA..

- Key plant safety functions (i.e., reactor shutdown and decay heat removal) are not dependent upon a single protective system. Accordingly, it is envisioned that each of those functions, be accomplished by redundant, independent and diverse means, with each means having reliability and availability goals commensurate with overall plant risk goals. It is intended that the requirement for redundant, diverse and independent means for reactor shutdown and decay heat removal be applied in the following manner:

    - The design should ensure that for frequent and infrequent event sequences, redundant, diverse and independent means for reactor shutdown and decay heat removal are available. In other words, given an initiating event (which may involve loss of one decay heat removal path or means of reactor shutdown), the other path or means should have

sufficient reliability and availability to be considered functional and ensure that the acceptance criteria for frequent and infrequent event sequences are met.

  - This functional requirement would not apply to event sequences in the rare category.

- This represents a structuralist approach to defense-in-depth for these important functions to account for unquantified uncertainties, including common cause failure.

- In assessing the performance of protective systems, uncertainties in reliability, and performance need to be accounted for. For new types of equipment or equipment with little or no operating experience at the conditions it will experience, a reliability assurance program (see Section 8.3.2) needs to be provided to demonstrate and monitor equipment to ensure the assumptions of reliability, availability and performance used in the PRA and safety analyses are met.

- The unacceptable release of radioactive material must be prevented. Accordingly, a means to prevent the uncontrolled release of radioactive material needs to be included in the design, consistent with the barrier integrity protective strategy (Section 8.3.4).

- Plant siting can affect the types and performance of safety systems since site specific hazards may be different. Site specific hazards and conditions need to be considered in the design consistent with 10 CFR 100 and the licensing analysis.

The above defense-in-depth considerations are reflected in the topics which the requirements must address, as shown in Table 8-3.

Table 8-3 identifies the questions that need to be answered to address each of the potential causes of protective system failure. The answers to these questions are organized by whether they apply to design, construction or operation and identify the topics which the technology-neutral requirements must address to ensure the success of this protective strategy. These topics are directed toward ensuring that quality analyses is used in the design process, that good engineering practices are used in the design and construction, that the equipment is tested, maintained and inspected over the life of the plant and that plant operations are conducted in a fashion that assures high reliability and availability of the protective systems (e.g., use of procedures and training need to be employed to minimize human errors). These considerations also apply to support systems as well as the front line protective systems.

Finally, in assessing the performance of the protective systems (and the performance resulting from the other protective strategies) the design should meet the F-C curve and the QHOs, as described in Chapter 6. The F-C curve is to be met by each accident sequence in the PRA and in the LBE analysis. The QHOs represent an overall assessment of plant risk (considering all plant operating states and SSCs, including spent fuel storage). It is intended that the QHOs be assessed in an integrated fashion such that all new reactors on a site must meet the QHOs considering their risk in a cumulative fashion.

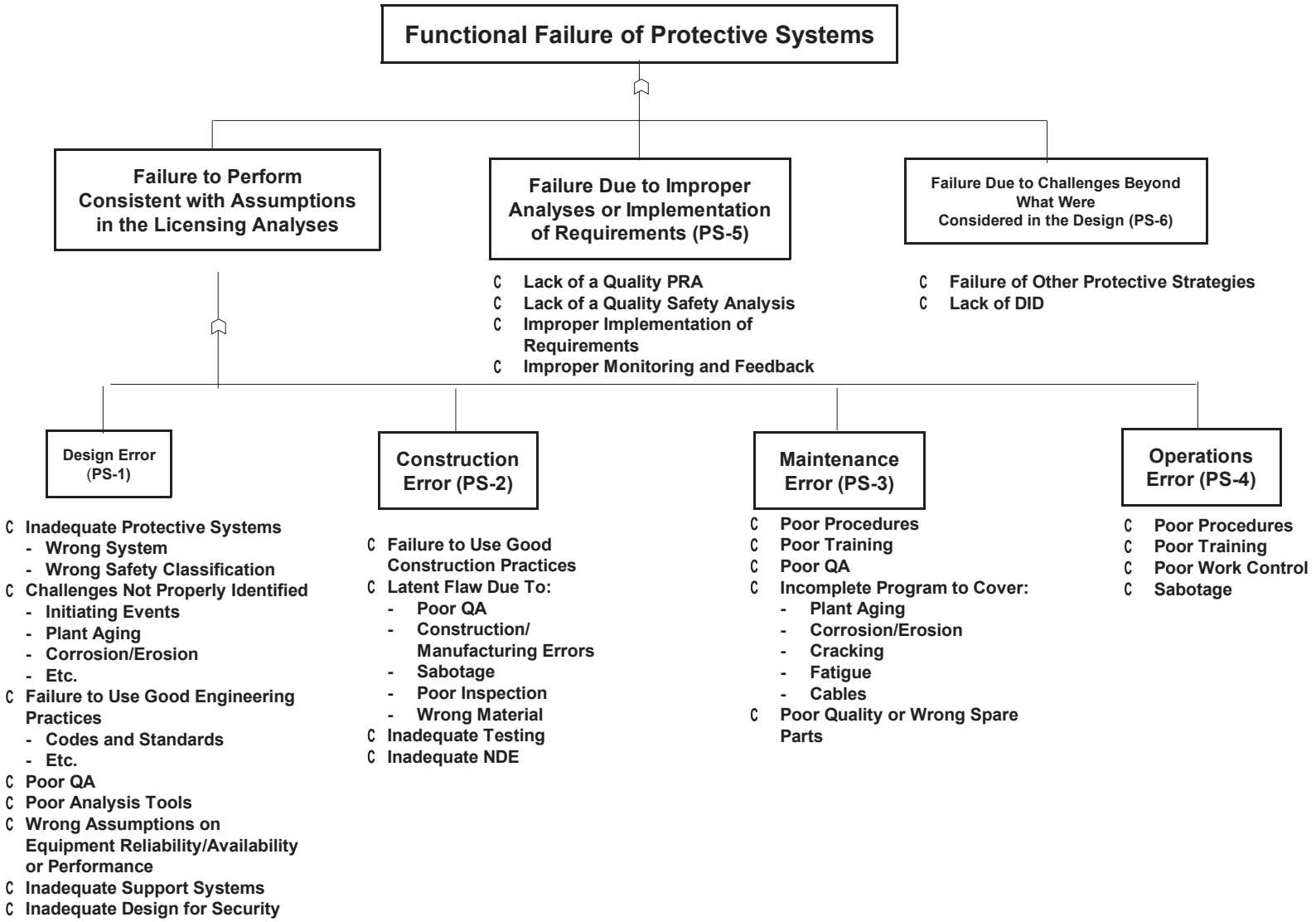

Figure 8-5 Logic tree for the protective systems strategy.

Table 8-3 Protective systems.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Failure to Perform Consistent with Assumptions - Design Errors			
• How should systems be designed to ensure adequate performance and safety? (PS-1)	• Use PRA and safety analysis to determine protective and support system needs (i.e., need quality PRA and safety analysis)	• N / A	• Use living PRA to feedback operational experience into design.
	• Meet F-C curve	• N / A	• N / A
	• Meet QHOs cumulatively	• N / A	• N / A
	• Use good engineering practices: - consensus design codes and standards - QA - qualified materials - EQ - qualified analytical tools - quality PRA and safety analysis to determine performance and reliability needed	• N / A	• N / A
	• Safety classification (see Chapter 6)	• N / A	• Tech specs
	• Consider plant aging / corrosion, etc.	• N / A	• Surveillance
	• Designer to specify reliability / availability goals consistent with PRA	• N / A	• Monitoring and feedback

Table 8-3 Protective systems.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	**Construction**	**Operation**
Failure to Perform Consistent with Assumptions - Construction Error			
• What needs to be done to prevent construction errors? (PS-2)	• Specify good construction / fabrication practices as part of the design.	• Use good construction / fabrication practices: • consensus codes and standards • QA / QC • access control	• N / A
Failure to Perform Consistent with Assumptions - Maintenance Errors			
• What needs to be done to prevent maintenance errors? (PS-3)	• N / A	• N / A	• procedures • training • QA / QC • comprehensive maintenance program, including: - plant aging - cables - corrosion - etc.
Failure to Perform Consistent with Assumptions - Operation Errors			
• What needs to be done to prevent operations errors? (PS-4)	• Consider human factors and man-machine interface as part of design (e.g., automatic vs. operator actions)	• N / A	• procedures • training • use of simulator • technical specifications • surveillance • ISI • testing
Failures Due to Improper Analyses or Implementation			
• How can failures due to improper analyses or implementation of requirements be prevented? (PS-5)	• Ensure plant is designed consistent with PRA and safety analysis. • QA	• Ensure plant is constructed consistent with design. • QA / QC	• technical specifications • safety classification • monitoring and feedback

Table 8-3 Protective systems.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Failures Due to Challenges Beyond What Were Considered in the Design			
• How can challenges beyond what were considered in the design (i.e., uncertainties) be accounted for? (PS-6)	• provide 2 independent redundant and diverse ways to shutdown the reactor and remove decay heat • reliability assurance program	• N / A • N / A	• N / A • N / A

N/A = Not applicable

8.3.4 Barrier Integrity

The barrier integrity protective strategy is intended to ensure that the design provides sufficient physical (or chemical) barriers to prevent the uncontrolled release of radioactive material. The number and nature of the barriers will be technology and design dependent. Barrier integrity depends on adequate design, construction, maintenance and operation and, in some cases, on the success of protective systems. The logic tree of Figure 8-6 lays out the events that can lead to functional failure of the barriers. If at least one barrier remains, the public is protected and workers are given a measure of protection. Barrier integrity applies to barriers associated with the reactor as well as spent fuel storage. Figure 8-6 begins by identifying three major top level pathways that can lead to failure. These are:

- Failure to perform consistent with assumptions in the licensing analyses;
- Failures due to improper analyses or implementation of requirements; and
- Failures due to challenges beyond what were considered in the design.

Each of these is discussed in more detail in the following paragraphs.

The first major pathway (Failure to Perform Consistent with Assumptions in the Licensing Analyses) can be affected by design, construction, maintenance or operation errors, as discussed below.

Design errors leading to barrier failure can occur because the design is inadequate for the actual conditions that occur or conditions in excess of the design conditions occur. Failure can also occur by a failure of security, i.e., a loss of physical protection. Other design factors affecting barrier integrity are failure to consider barrier degradation mechanisms or poor QA / QC.

Construction and manufacturing errors are another source of barrier failure. Using good construction practices and having a good QA and QC program during the construction phase is

essential to ensuring the plant is built as intended. Inspection, NDE and testing of barriers as construction proceeds are means to ensure the plant has been built as intended. Manufacturing processes for the fuel need to be controlled and qualified to ensure that fuel performance is consistent with design assumptions.

Maintenance errors are another potential source of barrier failure. These can occur due to leaving equipment in the wrong position, making a work error (e.g., forgetting to install a seal), not being trained or not following procedures. Accordingly, good work control, training and procedures are needed as well as a post maintenance test program to verify that barrier integrity is established. Finally, the maintenance program must cover all important degradation mechanisms that can affect barrier integrity.

Preventing operation errors are also important to maintaining barrier integrity. Poor procedures, training or work control could lead to barrier bypass or loss of integrity. To help prevent these errors, good training programs, verified procedures, surveillance, ISI and testing are needed. Also, sabotage is a potential source of barrier failure.

The second major pathway to barrier failure is associated with failures due to improper analyses or implementation of requirements. The licensing analysis will determine what barriers need to be in the design and how they should be designed. For normal operation and anticipated operational occurrences, reliable barriers to retain the fission products in the reactor and reactor coolant in the coolant system are necessary to meet the low levels of radioactive material release specified for normal operation. To ensure reliable barriers, the barriers should be designed and built to accepted consensus design codes using materials qualified for the intended service and accepted quality assurance measures.

For off-normal conditions, the event selection criteria discussed in Chapter 6 can be used to define the event scenarios and conditions which must be considered in designing the barriers. These criteria categorize event scenarios into those that are expected to occur one or more times during the life of the plant (frequent events), those that may occur once in a population of plants (infrequent events) and those considered in assessing overall plant risk and emergency preparedness (rare events).

Deterministic acceptance criteria for frequent and infrequent events have been developed in Chapter 6. Criteria on plant risk have also been developed in Chapter 6. To ensure the barriers perform as intended, they need to be qualified for the service conditions expected. This may involve research and development to verify fuel performance and equipment qualification (EQ) to verify the performance of mechanical items. Also, the analysis of barrier performance under normal and off-normal conditions will require safety analysis tools that need to be validated against experimental data. Depending upon the importance of the barriers to meeting the acceptance criteria, they may be assigned a safety classification (as described in Chapter 6) that will help ensure their performance availability and operability is maintained over the life of the plant.

It is also important that the assumptions associated with the analysis be properly implemented and controlled. Accordingly, items such as monitoring/feedback, technical specifications and safety classification needs to capture the key assumptions and provide control over the plant configuration and operation.

For the third major pathway (unanticipated challenges and failures), protection is provided by the other protective strategies (i.e., they are additional lines of defense) and by application of the defense-in-depth principles to account for completeness uncertainty.

Applying the defense-in-depth principles to the barrier integrity protective strategy leads to the following:

- The number of barriers and their design need to be based upon both intentional as well as inadvertent events. By requiring the design be done in an integral fashion considering security (see Section 8.3.1), the barriers need to consider both.

- The barriers need to be designed with both accident prevention and mitigation in mind. Accident prevention will be achieved by ensuring that the barriers are designed to be highly reliable and can withstand a range of off-normal conditions. High reliability needs to be achieved by the use of good engineering practices (such as the use of consensus design codes and standards, qualification of materials, QA, etc.) in the design and performing surveillance, inspection and testing during the plant lifetime. Barriers also need to be designed to maintain their integrity for events expected to occur during the plant lifetime such that their failure does not become an initiating event.

  Accident mitigation will be achieved by ensuring the barriers perform their function of containing radioactive material. The events for which they must perform their function, their design and their degree of leak tightness will be design dependent, as will the total number of barriers needed. Minimum requirements for barriers are discussed below.

- Defense-in-depth requires that key safety functions not be dependent upon a single element of design, construction, operation or maintenance. Application of this principle to barrier integrity implies multiple barriers are needed, since containment of radioactive material is considered a key safety function. Accordingly, at least two barriers to the release of radioactive material need to be provided, since the failure of one of these barriers (most likely the reactor coolant system barrier) could be an initiating event. In general, the barriers, in conjunction with other plant features, need to be capable of limiting dose to the public consistent with the frequency consequence curve in Chapter 6.

- In the design and safety analysis, uncertainties in reliability and performance need to be accounted for. However, not all uncertainties can be quantified. Therefore, it is considered reasonable to require each design to have additional capability (beyond the two barriers described above) to mitigate against accident scenarios that result in the release of larger amounts of radioactive material by providing margin to account for unquantified uncertainties that result in a larger source term available for release to the environment (e.g., security related events). Accordingly, as a structuralist defense-in-depth provision, each design needs to have a containment functional capability (i.e., the capability to establish a controlled low leakage barrier) in the event plant conditions result in the release of radioactive material from the core and reactor coolant system in excess of anticipated conditions. The specific conditions regarding the leak tightness, temperature, pressure and time available to establish the containment functional capability will be design specific. The design of the containment functional capability is to be based upon a process that defines an event representing a serious challenge to fission product retention in the core and coolant system. The event needs to be agreed upon between the applicant and the NRC consistent with the technology and safety characteristics of the design. The event could represent an event where fission product retention in the core and coolant system suddenly changes due to small changes elsewhere, a low probability event from the PRA, a security related event or an assumed fuel damage event.

  For LWRs, core melt accidents will likely continue to be used to establish the design conditions for the containment functional capability. For non-LWRs, examples of the types

of events that could be considered for establishing the design conditions for the controlled leakage barrier are:

- HTGRs

  - graphite fire in the core
  - water ingress to the core
  - loss of coolant accident in conjunction with poor quality fuel

- LMRs

  - flow blockage in the core
  - large liquid metal fire
  - loss of normal heat removal in conjunction with poor quality fuel

The selection of the event to be used to establish the design conditions for the containment functional capability is not intended to impose a traditional LWR type containment on all technologies, but rather to allow each technology to have designs that reflect their unique safety characteristics while providing margin for uncertainties in the source term available for release to the environment (e.g., venting to the atmosphere early in an accident scenario may be acceptable for some technologies).

The selected event should be analyzed mechanistically to determine the timing, magnitude and form of radionuclide released into the reactor building, and the resulting temperature, pressure and other environmental factors (e.g., combustible gas) in the building over the course of the event. The timing of closure and the allowable leak rate should then be established such that the worst two-hour exposure at the EAB and the exposure at the outer edge of the LPZ for the duration of the event do not exceed 25 rem TEDE. Chapter 6 contains additional guidance regarding analysis of this event.

- Barriers need to prevent the unacceptable release of radioactive material. Accordingly, to account for uncertainties (see paragraph above), the design needs to have a containment functional capability independent from the fuel and RCS, as discussed above.

- Barrier integrity interfaces with siting in that some aspects of barrier performance may be determined by site characteristics (e.g., meteorology, population distribution). Likewise, barrier integrity can also affect the type and extent of off-site protective measures needed. These need to be accounted for in the design.

The above defense-in-depth considerations have been factored into the requirement topics shown in Table 8-4.

Table 8-4 shows a set of questions and answers associated with the Barrier Integrity protective strategy. The questions are organized by the top level branches of the logic diagram and the answers (i.e., the topics which must be covered by the requirements) are arranged by whether they apply to design, construction or operation.

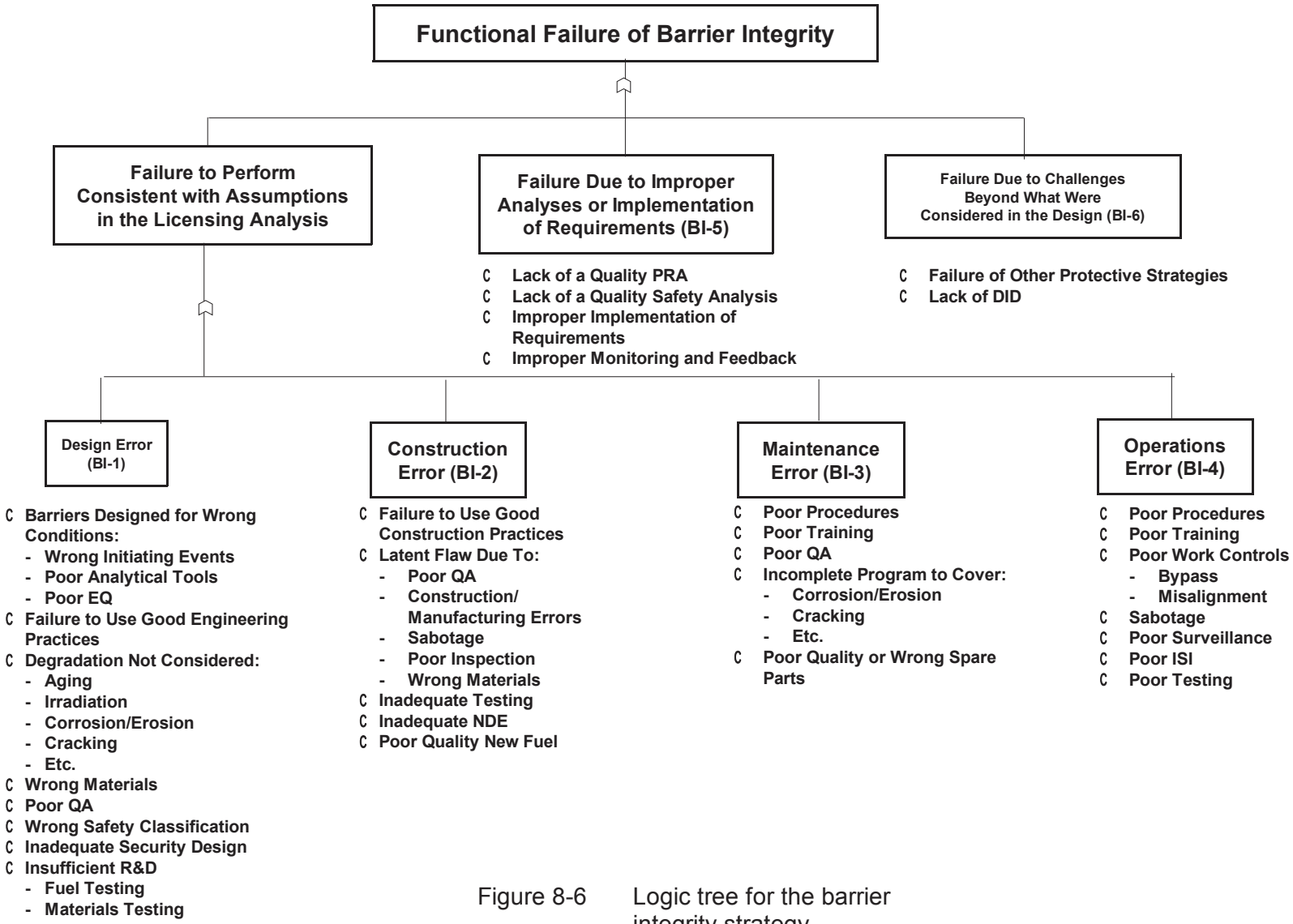

Figure 8-6 Logic tree for the barrier integrity strategy.

Table 8-4 Barrier integrity.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	**Construction**	**Operation**
Failure to Perform Consistent with Assumptions - Design Errors			
• How should adequate barrier design (integrity and reliability) be assured? (BI-1)	• Design barriers consistent with: - Chapter 6 event selection criteria - Chapter 6 acceptance criteria (probabilistic and deterministic) - Safety classification - EQ - Consider degradation mechanisms • Provide barriers for: - fission product retention (in the fuel) - coolant retention (in the reactor and spent fuel cooling system) - Other capability, as necessary to meet safety objectives • Use good engineering practices: - quality assurance - materials qualification - use of accepted	• N / A	• N / A

Table 8-4 Barrier integrity.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	**Construction**	**Operation**
	design codes and standards - use of validated safety analysis tools - consider aging and other degradation phenomena		
Failure to Perform Consistent with Assumptions - Construction Errors			
• What needs to be done to prevent construction errors? (BI-2)	• specify construction / manufacturing techniques at the design stage.	• use good construction / manufacturing practices: - consensus construction codes and standards - QA / QC - inspection - testing - NDE - assure fuel quality over the life of the plant • access control • surveillance	• N / A
Failure to Perform Consistent with Assumptions - Maintenance Error			
• What needs to be done to prevent maintenance errors? (BI-3)	• N / A	• N / A	• verified procedures • good training • QA / QC • have a comprehensive maintenance program • use quality spare parts
Failure to Perform Consistent with Assumptions - Operations Error			
• What needs to be done to	• Use good HF and HMI	• N / A	• verified procedures

Table 8-4 Barrier integrity.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	**Construction**	**Operation**
prevent operational errors? (BI-4)	engineering • Use fault tolerant designs		• good training • use of simulator • good work control • good surveillance • ISI • testing
Failures Due to Improper Analyses or Implementation of Requirements			
• How can failures due to improper analyses or implementation of requirements be prevented? (BI-5)	• Use verified analytical tools • Quality PRA and safety analyses • Ensure plant is designed consistent with PRA and safety analysis. • QA	• Ensure plant is constructed consistent with design. • QA / QC	• technical specifications • safety classification • monitoring and feedback
Failures Due to Challenges Beyond What Were Considered in the Design			
• How can challenges beyond what were considered in the design (i.e., uncertainties) be accounted for? (BI-6)	• at least 2 barriers for the reactor and spent fuel storage • capability to establish a containment functional capability independent of fuel and RCS for the reactor.	• N / A • N / A	• technical specifications • technical specifications

N / A = Not applicable

8.3.5 Protective Actions

The protective actions strategy ensures that adequate systems, equipment, and practices are in place to control and terminate the accident progression, to minimize damage to the barriers, to limit the release of radionuclides, to protect workers, and to limit public health effects. Protective actions generally include EOPs, accident management and on-site and off-site emergency preparedness.

Figure 8-7 is a logic tree showing the pathways that can lead to failure of protective actions. At the top level, three major pathways to failure are: (1) failure to take protective actions consistent with assumptions in the licensing analysis, (2) failure due to improper analyses or implementation of requirements, or (3) failures due to challenges beyond what were considered in the design. Each of these top level pathways is discussed further below.

In the first top level pathway (Failure to Take Protective Action Consistent with Assumptions in the PRA and Safety Analysis), failure can be associated with either on-site or off-site actions, as shown in Figure 8-7. Failure of on-site protective actions can be associated with operations, hardware or software, training or design. Off-site failures can occur in areas regulated by the NRC or in areas controlled by other agencies. For example, state and local officials are responsible for many aspects of the off-site response (e.g., evacuation).

On-site failures due to operational problems can result in failure to terminate the accident (thus making conditions on-site, and possibly off-site, worse) or failure to adequately protect operating personnel. Operating personnel are vital to plant safety and are called on to perform safety related actions during design basis and beyond-design-basis events (e.g., accident management actions). Accordingly, protection of the operating staff during accidents also needs to be considered in the design and operation of future reactors.

General Design Criteria (GDC) 19 of 10 CFR Part 50 Appendix A currently requires main control rooms to be designed to ensure habitability under a variety of conditions, including design basis accident conditions. The conditions which must be considered include a postulated source term representative of a LWR core melt accident (or an alternate source term) and chemical releases. As a result, LWR main control rooms are provided with shielding and habitability systems that ensure the safety of the operators during the postulated conditions. Accordingly, the technology-neutral requirements should include a similar provision for protection of control room staff during accidents, recognizing the use of the PRA to select the accident scenarios which must be considered and the use of scenario specific source terms.

However, no corresponding requirements exist in 10 CFR 50 for protection of operating staff outside the main control room, who may be called upon to perform accident management actions and communicate with other staff during accident situations. In the development of accident management programs for existing LWRs (which were developed on the basis of a voluntary industry initiative), it was recognized that access by the operating staff to certain portions of the plant was essential to carry out the planned actions. Accordingly, NEI, in its "Severe Accident Issue Closure Guidelines" document (NEI-91-04, Rev. 1, dated December 1994) on the development of accident management programs, identified operational and phenomenological conditions as factors which must be assessed in planning and implementing operator accident management actions.

For new plants, the technology-neutral requirements should require that the procedures and accident management programs consider the environment (e.g., temperature, radiation) in which local operator actions take place and ensure that the design (e.g., shielding, access) and

procedures sufficiently protect all the operators so that the actions can be safely accomplished without serious injury. For radiation exposure (during such activities), the limits in 10 CFR Part 20.1201, "Occupational Dose Limits" should be used for frequent event scenarios and 10 CFR Part 20.1206, "Planned Special Exposures" should be used as the measure to prevent serious injury for personnel outside the control room during frequent and rare event scenarios. Regulatory Guide 8.38 provides additional guidance in this area regarding access to high radiation areas. For personnel inside the control room, limits similar to those in GDC-19 could be used. Scenario specific source terms may be used in the assessment, consistent with those used in other accident analyses. Other accepted limits should be applied for other hazards (temperature, chemicals, etc.).

On-site hardware or software problems can lead to unintended actions and/or poor decisions. Accordingly, measures to ensure reliable equipment and software are needed. Poor training can also lead to the same consequences as poor operations or poor hardware/software. Training programs need to be complete and conducted periodically to keep operating personnel skills current. Design problems can result in needed equipment not being present, instrumentation and/or communication not sufficient to understand the accident, personnel access and habitability restricted more than anticipated or personnel injury or death. Therefore, during the design stage, accident scenarios (including those related to security failure) must be considered integral with the design and measures to ensure good EOPs and accident management need to be provided.

Off-site preparedness failures can lead to failure to take measures needed to protect the public. Such failures could be due to hardware problems (e.g., failure to notify), poor planning (e.g., traffic jams delay evacuation) or an insufficient implementation for the accident consequences. Off-site organizational failures can also lead to failures to adequately protect the public. Such failure can be due to poor coordination among off-site authorities, poor communication, poor training or poor decisions (i.e., not implementing the appropriate protective measures at the appropriate time).

The second top level pathway is associated with failures due to improper analyses or implementation of requirements. Quality analyses and the use of verified analytical tools are essential. In addition, the EOPs and AM procedures should be developed in an integrated fashion with the design so that the design can provide reasonable measures for AM and ensure the procedures are consistent with the PRA and safety analysis.

For the third top level pathway (failures due to challenges beyond what were considered in the design), protection is provided by the application of the defense-in-depth principles to account for completeness uncertainty. Applying the defense-in-depth principles to this protective actions strategy leads to the following:

- The development of protective actions needs to consider intentional acts as well as inadvertent events. The physical protection protective strategy (Section 8.3.1) provides further guidance on evaluating security integral with design.

- Protective actions need to include measures to terminate the accident progression (referred to as EOPs, and accident management) and pre-planned measures to mitigate the accident consequences (referred to as emergency preparedness). The EOPs, AM procedures and EP need to be developed in an integrated fashion with the design.

- The accomplishment of protective actions must not rely on a single element of design, construction, maintenance or operation. As such, EOPs, accident management and EP procedures need to be developed so as not to be dependent upon a single operator or human action or piece of equipment.

- Protective actions need to be developed in consideration of uncertainties. As a structural defense-in-depth measure, emergency preparedness needs to be included in the design and operation to account for unquantified uncertainties.

- Prevention of unacceptable releases of radioactive material need to be part of the AM program.

- Plant siting will affect EP and needs to be considered in developing EP plans.

The above defense-in-depth considerations are reflected in Table 8-5.

Table 8-5 below summarizes each of these pathways in the form of questions, the answers to which identify the topics that the technology-neutral requirements must address to prevent pathway failure. The answers (i.e., topics) are arranged according to whether they apply to design, construction or operation.

As can be seen from Table 8-5, there are a number of topics that should be addressed in the requirements to assure an adequate protective actions strategy. Some of these (e.g., drills, training) can utilize the technology-neutral requirements contained in 10CFR50, while others will need to be developed in a technology-neutral fashion consistent with a risk-informed approach. A major item in this regard would be a requirement for the development of the design (and its associated systems and instrumentation) in an integrated fashion with the development of EOP and AM procedures. Such an integrated process would help ensure that the procedures address all of the relevant accident scenarios in the PRA (and scenarios from security considerations) and that the design includes features that facilitate AM.

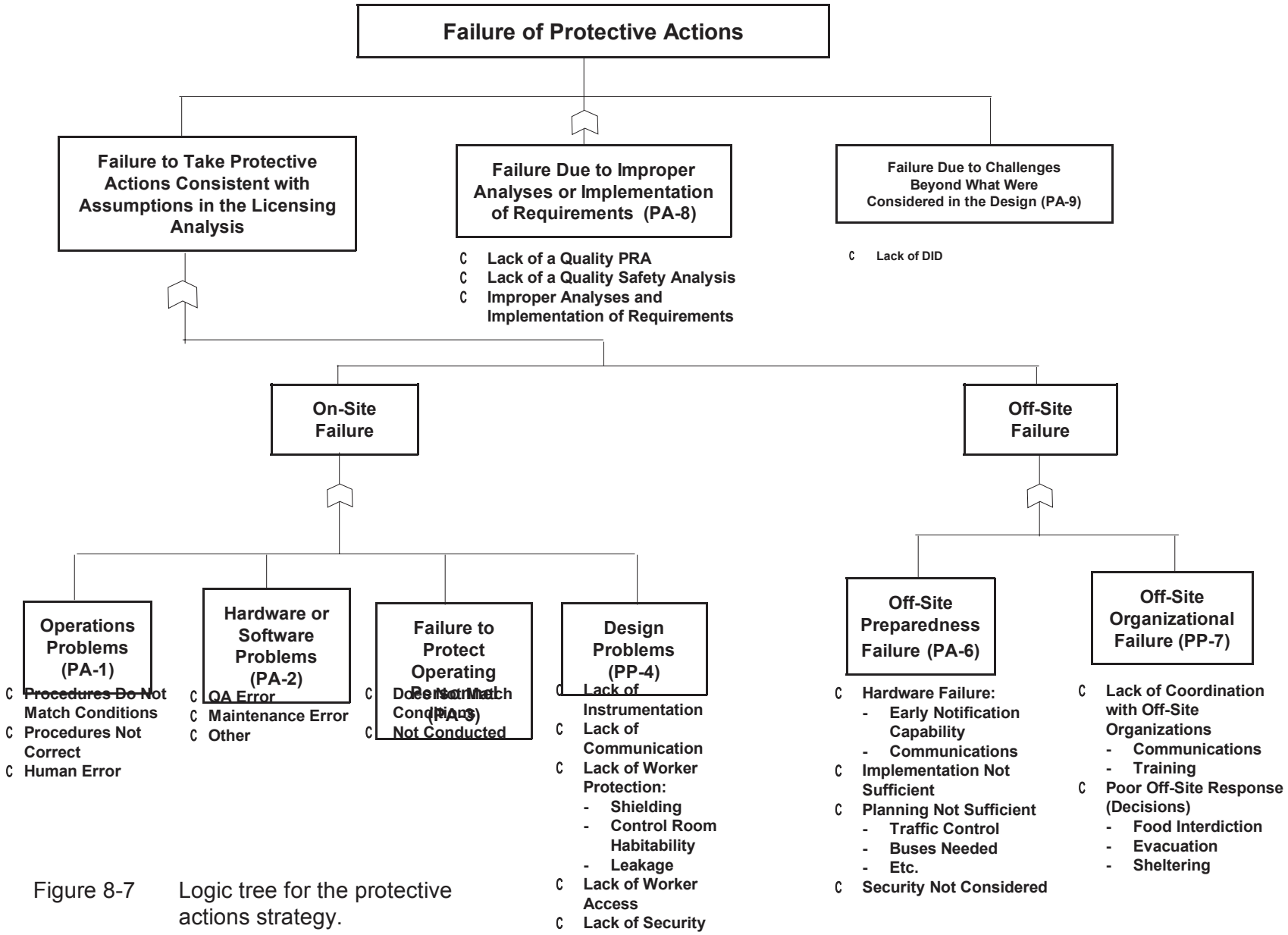

Figure 8-7 Logic tree for the protective actions strategy.

Table 8-5 Protective actions.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Failure to take Protective Actions Consistent with Assumptions: On-Site Failure			
• How can operations problems be prevented? (PA-1)	• N / A	• N / A	• Develop comprehensive training programs and require periodic training. • Use of simulator • Use of verified procedures
• How can hardware and software be assured to be operable? (PA-2)	• Reliability assurance program for hardware • Software V and V	• Testing • QA / QC • N / A	• Maintenance program • Testing
• How can it be assured operating personnel are properly protected? (PA-3)	• Provide appropriate shielding and habitability for the control room and other areas needing access.	• N / A	• Establish comprehensive worker protection programs, training and monitoring.
• How can design deficiencies / problems be prevented? (PA-4)	• Develop EOP and AM design features and procedures integral with design, including identifying equipment, instrumentation, and communication needs. • Provide alternate	• N / A • N / A • N / A	• Ensure 10CFR20 requirements are complied with. • N / A • N / A

Table 8-5 Protective actions.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
• How can adequate on-site preparedness be assured? (PA-5)	shutdown location • Develop on-site EP plans and procedures integral with design		• Training • Procedures • Coolant drills and training to demonstrate effectiveness of on-site EP
Failure to Take Protective Actions Consistent with Assumptions - Off-Site Failure			
• How can adequate off-site preparedness be assured? (PA-6)	• Provide adequate emergency planning • Consider security related events	• N / A	• Conduct drills and training to demonstrate effectiveness of off-site EP • Integrate security and preparedness
• How can adequate off-site organizational performance be assured? (PA-7)	• Provide reliable communication equipment	• N / A	• Conduct drills and training to demonstrate effectiveness of EP
Failures Due to Improper Analyses or Implementation of Requirements			
• How can failures due to improper analyses or implementation of requirements be prevented? (PA-8)	• Quality licensing analyses • Use verified analytical tools • Develop EOPs and AM procedures integral with design. • QA	• N / A • N / A • N / A • N / A	• Ensure training program is comprehensive and conducted periodically. • Use of simulator • N / A

Table 8-5 Protective actions.

Protective Strategy Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Failures Due to Challenges Beyond What Were Considered in the Design			
• How can challenges beyond what were considered in the design (i.e., uncertainties) in protective actions be accounted for? (PA-9)	• Consider security related events (Section 8.3.1). • Develop EOPs and AM integral with design. • Do not have EOPs or AM dependent upon a single operator or human action or piece of hardware.	• N / A • N / A • N / A	• Consider security related events (Section 8.3.1). • Training • Drills • EP

N / A = Not applicable

8.3.6 Summary of Technical Topics

Sections 8.3.1 through 8.3.5 identify the topics that the technology-neutral requirements must address to ensure the success of the protective strategies. Some of the topics identified are applicable to more than one protective strategy (e.g., QA, training, etc.). Accordingly, a summary table (Table 8-6) has been prepared that consolidates the technical topics from Tables 8-1 through 8-5, eliminating any duplication. Table 8-6 also organizes the topics in a more logical fashion (i.e., by subject) and provides a space for comments where reference can be made to the appropriate section of the framework (for additional guidance), to the scope the requirement must address or to possible sources for the requirements.

It needs to be recognized that Table 8-6 presents a broad, high level overview of the topics which the technology-neutral technical requirements must address. Many details need to be developed in the course of writing the requirements. Section 8.5 provides guidelines on how to take the information in Table 8-6 (as well as Table 8-9 in Section 8.4) and write technology neutral requirements.

As described in Section 8.3.1 through 8.3.5, the identification of the topics which the requirements must address comes from considering the logic diagrams (Figures 8-3 through8-7) and how to protect against the various pathways that can lead to failure of the strategies. In addition, the defense-in-depth principles from Chapter 4 were applied to each protective strategy to ensure adequate treatment of uncertainties.

Application of the defense-in-depth principles to each of the protective strategies (as described in Section 8.3.1 through 8.2.5) has also led to the identification of a number of specific topics to address uncertainties. Although included in Table 8-6, these are also summarized in Table 8-7 to

illustrate the defense-in-depth provisions identified by the application of the DID principles in Chapter 4. The technology-neutral requirements also need to include the defense-in-depth principles and process, so that applicants and licensees are required to implement a defense-in-depth review on their designs.

Table 8-6 Summary of Technical Topics.

Topic	Comments
A) General:	
• F-C curve	• See Chapter 6
• QHOs (including integrated risk)	• See Chapter 6 and Section 8.3.3
• Criteria for selection of LBEs	• See Chapter 6
• Keep initiating events with potential to defeat two or more protective strategies<10^{-7}/plant year	• See Chapter 6
• Criteria for safety classification and special treatment	• See Chapter6
• LBE deterministic acceptance criteria: • frequent events • infrequent events • rare events • link to siting	• See Chapter 6
• Analysis guidelines: • realistic analysis, including failure assumptions • treatment of uncertainties • qualification of analysis tools • source term	• See Chapter 6
• Siting	• See Section 8.3.2
• Defense-in-Depth principles and process	• See Chapter 4
• QA / QC	• See 10 CFR 50, Appendix B
• PRA scope and quality	• See Chapter 7
(B) Physical Protection:	
• General	• Use 10 CFR 73
• Perform security assessment integral with design	• See Chapter 6 for guidance on security performance standards
• Security performance standards	

Table 8-6 Summary of Technical Topics.

Topic	Comments
(C) Good Design Practices:	
• Use consensus design codes and standards	• Details will need to be technology-specific
• Materials qualification	• Details will need to be technology-specific
• Provide 2 redundant, diverse, independent means for reactor shutdown and decay heat removal	• Will also need applicant to establish reliability goals. (Also see Section 8.3.3.)
• Minimum - 2 barriers to FP release	• See Section 8.3.4
• Containment functional capability	• See Section 8.3.4
• Need to consider degradation and aging mechanisms in design	
• Reactor Inherent Protection (i.e., no positive power coefficient, limit control rod worth, stability)	
• Human factors considerations	
• Fire protection	• Must address other sources of fires (e.g., graphite, liquid metal) as well as traditional fire protection.
• Control room design	• See Section 8.3.6
• Alternate shutdown location	• See Section 8.3.6
• Flow blockage prevention	
• Reliability Assurance Program	• See Section 8.3.2
• Research and Development	• See Section 8.3.2
• Combustible gas control	
• Coolant / water reaction control	• See 10 CFR 50.44 (a) and (d)
• Prevention of Brittle Fracture	
• Leak before break	
• Spent fuel storage	
• I and C System	
• analog	
• digital	
• HMI	
• Criticality prevention	
• Protection of operating staff during accidents	• See Section 8.3.6

Table 8-6 Summary of Technical Topics.

Topic	Comments
(D) Good Construction Practices:	
• Use accepted codes, standards, practices	• Details will need to be technology-specific.
• Security	• Access control
• NDE	
• Inspection	
• Testing	
(E) Good Operating Practices:	
• Radiation protection during routine operation	• See 10 CFR 20 and 10 CFR 50, Appendix I. (Also see Section 8.3.6.)
• Comprehensive maintenance program	• See 10 CFR 50.65
• Personnel qualification	• Operations and maintenance
• Training	• Operations and maintenance
• Procedures	• Operations and maintenance
• Use of simulators	• See Section 8.3.6
• Staffing	
• Aging management program	
• Surveillance	
• ISI	
• Testing	• Use risk-informed approach
• Technical specifications	• Use risk-informed approach
• Develop EOP and AM procedures integral with design	• See Section 8.3.5
• EP	
• Monitoring and feedback	
• Corrective action program	
• Work control	
• Living PRA	• See Chapter 7
• Security	• See 10CFR73

Table 8-7 Defense-in-Depth (DID) Provisions

DID Principle	Physical Protection	Stable Operation	Protective Systems	Barrier Integrity	Protective Actions
1) Consider intentional and inadvertent events	Integral Design Process	Integral Design Process	Integral Design Process	Integral Design Process	Integral Design Process
2) Consider prevention and mitigation in design	Vulnerability Assessment	Applicant should propose cumulative limit on IE frequencies.	Accident prevention and mitigation:	Accident prevention and mitigation:	Develop EOPs and AM integral with design EP
3) Not dependent upon a single element of design, construction, maintenance, operation	Vulnerability Assessment	Ensure events that can fail multiple PS are $<10^{-7}$ /plant year.	Provide 2 independent, red diverse means for: reactor shutdown and DHR.	Provide at least 2 barriers:	Not dependent upon a single operator action
4) Account for uncertainties in performance	Vulnerability Assessment	Reliability Assurance Program	Applicant to propose reliability and availability goals and RAP, and margin to account for modeling uncertainties.	Provide containment functional capability independent from fuel and RCS	EP
5) Prevent unacceptable release of radioactive material	Vulnerability Assessment	Ensure events that can fail (stable oper, PS and BI) PS are $<10^{-7}$ / remaining plant year.	N / A	Provide containment functional capability independent from fuel and RCS	AM
6) Siting	Vulnerability Assessment	Applicant should propose limits on ext. event cumulative frequencies.	N / A	N / A	EP

N/A = Not applicable

8.4 Administrative Requirement Topics

As discussed earlier in this document, the framework is to define the scope and content, and provide the overall technical basis for a new part to 10 CFR containing technology-neutral, risk-informed and performance-based requirements for new plant licensing which can serve as an alternative to 10 CFR 50. Accordingly, as an alternative to 10 CFR 50, the new part should address the administrative aspects of licensing using the new process, similar to the administrative aspects of 10 CFR 50. Where possible, existing administrative requirements should be used provided they are technology-neutral. However, the administrative aspects of this new part will have some differences from those in 10 CFR 50 because of the technology-neutral, risk-informed and performance-based nature of the new part. In either case, the administrative requirements need to be complete, so as to make the technology-neutral set of requirements a stand alone alternative to 10 CFR 50. Guidance on the use of existing requirements is provided in Section 8.5.

Administrative requirements have an impact on safety in that they define processes, documentation and practices that are necessary to ensure accurate and adequate information is developed, maintained and reviewed such that there is assurance that the plant is designed, constructed, operated and maintained in accordance with the safety analysis. The administrative requirements also ensure sufficient information is provided to the regulator to allow independent verification of plant safety. In effect, this serves as an administrative defense-in-depth measure by providing an independent check on plant safety.

Figure 8-8 is a logic tree that illustrates schematically the various elements of administration whose failure could impact safety. Each of the branches on the tree is discussed below with respect to identifying what must be done to ensure success of the branch. This then leads to identifying what topics the administrative requirements must address to be complete. Table 8-8 then provides the questions resulting from Figure 8-8, the answers to which identify the topics that need to be addressed by the administrative requirements.

The first branch on the tree is associated with ensuring that the information necessary for licensing decisions is adequate. The licensing decisions that require information are:

- the initial application to build and operate a nuclear power plant;
- any amendments to the license after the initial OL is granted; and
- any exemptions to the regulations for initial licensing or subsequent amendments.

Each of these licensing actions requires certain types of information which the administrative requirements should address. However, due to the risk-informed and performance-based nature of the requirements, where PRA information will play a central role in establishing the safety case, the types of information required for each of these decisions will be different that what is required under 10 CFR 50. In developing the requirements, such information needs will need to be defined.

Issues that will need to be addressed include:

- What information from the PRA should be part of the initial application, license amendment requests and exemption requests? (See Chapter 7 for guidance.)

- What level of design, construction and operational detail needs to be submitted?

- What supporting research and development information needs to be submitted?

The second branch on the tree relates to maintaining the plant configuration up to date. This would include having a change control process that requires adequate review and approval of proposed changes and clearly identifies what changes require NRC approval and which do not. Since the

regulatory structure for new plant licensing makes use of a living PRA, the selection of basis events (and the selection of SSCs for special treatment) may not be a one-time licensing step, carried out at the time of plant licensing and remaining fixed. (See Chapter 6 for a description of the selection process.) Instead, it can be expected that both the selection of LBEs and the safety classification of SSCs may change over the lifetime of the plant as operational experience and other new information add to, and reshape, the risk insights from the living PRA. This potential for change in the LBEs and safety classification over time, due to the use of a living PRA, has to be addressed. The frequency and manner of updating the living PRA will have to be determined in a way that allows for regulatory stability and predictability, including compatibility with the design certification process in 10 CFR 52. Accordingly, the requirement will need to address a process for changes to the licensing basis. It needs to be noted the licensing basis is also dependent on defense-in-depth, therefore, while the risk insights may change, the licensing basis may not necessarily change. Also, if the design has received design certification, the interface between the change control process and the design certification rule-making needs to be defined. To develop a change control process that accommodates the above, the following guidelines are to be used.

- The results of the "living" PRA update should be compared to the plant licensing basis. Where changes in the licensing basis are needed to be consistent with the PRA update, they should be submitted to NRC for approval in a timely fashion.

- For plants built according to a certified design, if any of the proposed changes modify the certified (Tier 1 or Tier 2) portion of the design, a rule change to amend the certification should be processed and backfit considerations used to determine whether other plants of that same design need to make conforming changes.

- All other changes can be made by the licensee, with appropriate documentation available for NRC audit.

Plant configuration can also be affected by inadequate record keeping. This could be due to incomplete or out of date documentation. Requirements for record keeping also need to be established.

The third branch of the tree relates to information and processes necessary for NRC oversight. This will require (1) the licensee to report certain information to NRC (e.g., events, inspection results, performance indicators, etc.) in an accurate and timely fashion, (2) the licensee to monitor certain aspects of plant performance and take corrective action (via design or operation) when necessary and (3) the NRC to initiate enforcement or backfit action if licensee performance or action is judged inadequate. Requirements addressing what is expected from the licensee and what will trigger NRC actions will be necessary.

Table 8-9 summarizes the topics which the administrative requirements need to address based on the above. Other administrative requirements not related to safety will also be needed and these can be identified by a careful review of 10 CFR 50 and by including the appropriate requirement from 10 CFR 50 in the technology-neutral requirements, provided it is technology-neutral. Appendix G provides an initial assessment of the applicability of 10 CFR 50 requirements for incorporation into a technology-neutral set of requirements, following the guidelines in Section 8.5.1.

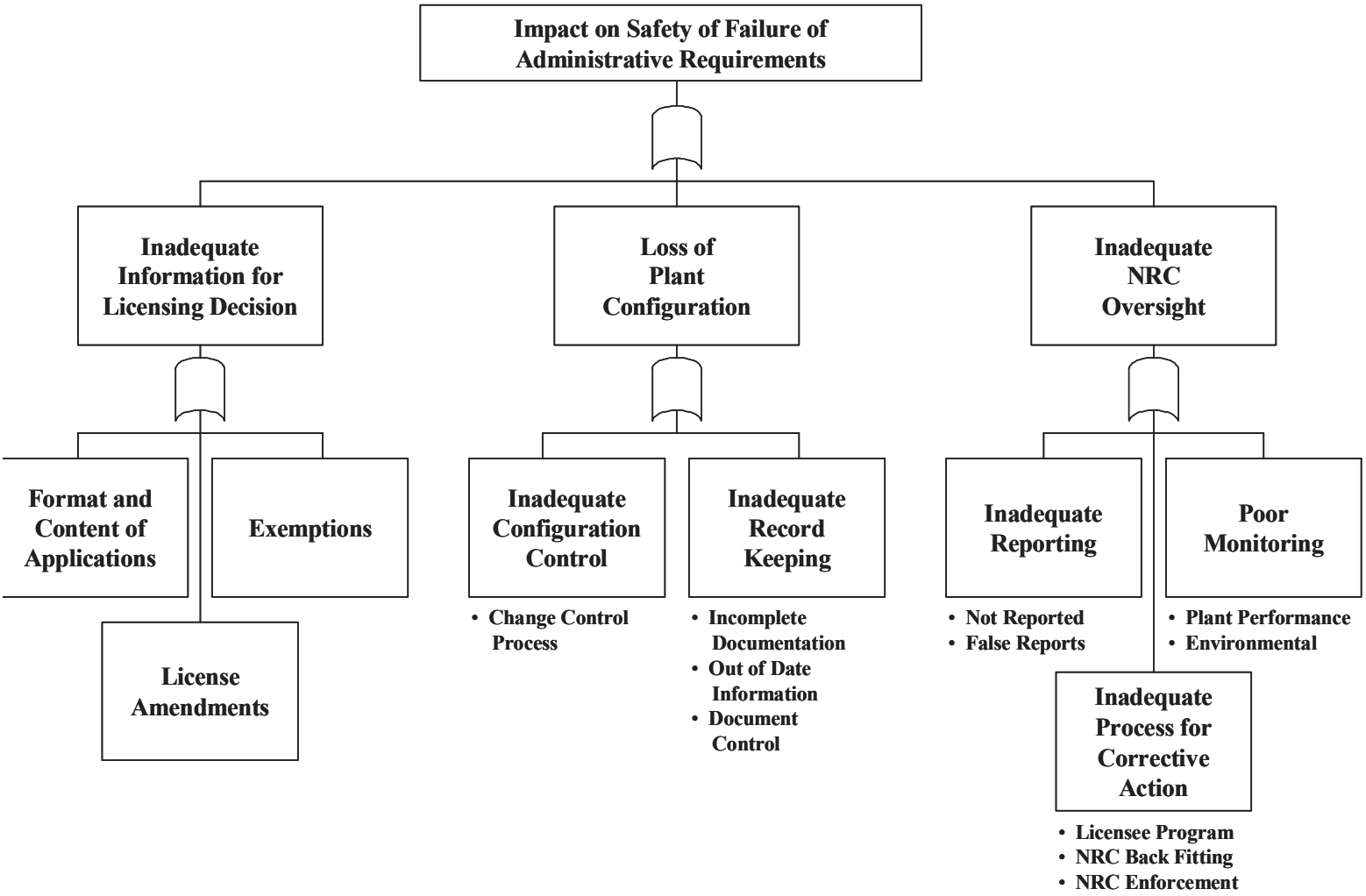

Figure 8-7
Logic Diagram for Administrative Area

Figure 8-8 Logic tree for the administrative area.

Table 8-8 Administrative requirement topics.

Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
Inadequate Information for Licensing Decisions			
• What information needs to be submitted to support initial licensing? (AR-1)	• Standard format and content of applications	• Standard format and content of applications	• Standard format and content of applications
• What in formation needs to be submitted to support license amendments? (AR-2)	• N / A	• N / A	• Standard format and content of applications
• What information needs to be submitted to support exemptions? (AR-3)	• Standard format and content of applications	• Standard format and content of applications	• Standard format and content of applications
Loss of Plant Configuration			
• What is needed to ensure configuration control? (AR-4)	• Change control process	• Change control process	• Change control process
• What information needs to be maintained? (PA-5)	• Identify documentation to be maintained • Documentation control process	• Identify documentation to be maintained • Documentation control process	• Identify documentation to be maintained • Documentation control process
Inadequate NRC Oversight			

Table 8-8 Administrative requirement topics.

Questions	Topics to be Addressed in the Requirements		
	Design	Construction	Operation
• What license information is needed to support NRC oversight? (AR-6)	• N / A	• Reporting requirements	• Reporting Requirements
• What information is the licensee expected to monitor? (AR-7)	• N / A •	• Inspection • Testing	• Plant performance • environmental releases
• What corrective action processes are needed? (AR-8)	• N / A	• Licensee program • NRC enforcement	• Licensee program • NRC enforcement • NRC backfitting

N / A = Not Applicable

Table 8-9 Summary of administrative topics.

TOPIC	COMMENTS
• Standard format and content of application	• See Chapter 7 for PRA related guidance
• Change • control process	• See section 8.4
• Record keeping • Documentation control • Reporting	
• Monitoring: - plant performance - environmental releases - testing results	• Make consistent with monitoring
• Corrective action program • Backfitting • License Amendments	
• Exemptions	• Make risk-informed
• Other legal and process items (e.g.) - anti-thrust - termination of license - etc.	• Make risk-informed • Use 10CFR50 requirements

8.5 Guidelines for Developing Technology-Neutral Requirements

Sections 8.3 and 8.4 identify the topics which the requirements need to address to ensure the protective strategies are effectively implemented and appropriate administrative controls are in place. These requirements are to be written in a technology-neutral fashion with any additional implementing guidance provided by technology-neutral or technology-specific Regulatory Guides. It is envisioned that the technology-neutral requirements be written to identify the broad principles and objectives associated with the requirements. As such, the General Design Criteria (GDC) currently contained in 10 CFR 50, Appendix A, serve as a good model of the scope, approach and depth envisioned in the technology-neutral requirements. In fact, it may be possible to use some of the existing GDC directly as technology-neutral requirements (this is discussed further below). In some cases, more specificity may be needed in some requirements where specific criteria or design features are considered necessary. In either case, certain guidelines should be followed in writing the requirements so as to ensure consistency in their scope and approach. This section provides the guidelines to be followed and addresses:

- use of 10 CFR 50 requirements and their supporting regulatory guides;
- development of a stand-alone set of requirements;
- use of a risk-informed and performance-based approach;
- ensure requirements do not allow repeating mistakes of the past;
- need for technology-specific regulatory guides; and
- relation of requirements to the licensing review and plant oversight.

Each of these is discussed in the sections that follow. Following these guidelines will likely be an iterative process and should be guided by a group of experts serving in a capacity similar to a PIRT (Phenomena Identification and Ranking Table) panel when it assesses a technical issue.

8.5.1 Use of 10 CFR 50 Requirements and Their Supporting Regulatory Guides

10 CFR 50 contains many requirements (both technical and administrative) that are technology-neutral. In developing the requirements for the technology-neutral framework, it would be most effective to use existing technology-neutral requirements whenever possible, since there is experience in their use and any needed implementing guidance has already been developed. Accordingly, as a first step, 10 CFR 50 should be examined to see where its requirements could be used in the technology-neutral requirements. In assessing whether or not to utilize existing wording from 10 CFR 50 in developing the technology-neutral requirements, the following approach should be followed:

- Is the wording acceptable as is (i.e., is it technology-neutral as risk-informed and performance-based as it can be)? If so, use the exact same wording as is in 10 CR 50.

- Can the wording be used with some modification (i.e., can it be made technology-neutral, more risk or more performance-based)? If so, suggest the appropriate modifications.

- Is the wording not usable (i.e., too technology-specific or prescriptive)? If so, do not use. Develop new requirement.

A preliminary examination of 10 CFR 50 has been conducted as described in Appendix G to identify which requirements are technology-neutral and are candidates for use in the technology-neutral requirements. Where they can be used they should, along with their regulatory guides, providing these guides are also technology-neutral. Where they cannot be used, modifications may be

appropriate to make them technology-neutral. The tables in Section 8.3 and 8.4 also provide some thoughts on where 10 CFR 50 requirements can be used.

8.5.2 Development of Stand Alone Requirements

It is intended that the complete set of technology-neutral requirements be a stand alone alternative to licensing under 10 CFR 50. As such, it is essential that the technology-neutral requirements contain all the administrative and process requirements essential to regulation, as well as the technical requirements.

10 CFR 50 should be used as a guide to identify the needed requirements and, as discussed in Section 8.5.1, perhaps the same wording as is contained in 10 CFR 50 can be used in the technology-neutral requirements. If not, a technology-neutral version of the requirement will have to be developed.

8.5.3 Use of a Risk-Informed and Performance-Based Approach

In licensing under the technology-neutral requirements, a design specific PRA will play a central role in assessing the safety of the design, both in the initial licensing review and over the life of the plant. Accordingly, it is important that the requirements be written to be compatible, as much as possible, with the type of information that a PRA can provide. This means that in writing the requirements, technology-neutral risk measures, criteria and other information that PRAs can produce (e.g., event sequences) should be used consistent with the framework guidance. In addition, deterministic criteria should also be used in selected areas (e.g., design basis accidents) so as to make the requirements risk-informed, not risk based. However, in addition to being risk-informed, the NRC has encouraged the use of a risk-informed and performance-based approach.

A risk-informed and performance-based approach is one in which the risk insights, engineering analysis and judgement, and performance history are used to: (1) focus attention on the most important activities; (2) establish objective criteria based upon risk insights for evaluating performance; (3) develop measurable or calculable parameters for monitoring system and licensee performance; and (4) focus on the results as the primary basis of regulatory decision-making. Accordingly, whenever possible, a performance-based approach should be used.

A performance-based approach brings about a focus on results as the primary basis for regulatory decision making, whether PRA information is available or not.

A performance-based approach is characterized and recognized by the occurrence of five defined attributes. These attributes are:

1.) A framework exists or can be developed to show that performance, as indicated by identified parameters, will serve to accomplish desired goals and objectives.

2.) Measurable, calculable, or constructable parameters to monitor acceptable plant and licensee performance exist or can be developed.

3.) Objective criteria to assess performance exist or can be developed.

4.) Margins of performance exist such that if performance criteria are not met, an immediate safety concern will not result.

5.) Licensee flexibility in meeting the established performance criteria exists or can be developed.

Appendix H provides additional guidance on the application of these attributes in developing performance-based requirements.

Another important aspect of performance-based requirements is the selection of parameters to be monitored. Performance-based requirements will require the monitoring of parameters that can be tied directly to the objectives of the requirements. Examples of performance-based parameters are:

- temperature
- pressure
- flow-rate
- fluid level
- radiation level
- voltage
- current

The frequency of monitoring, the instrumentation to be used, its calibration, accuracy and operability all need to be considered. It is likely that any instrumentation necessary for monitoring performance-based requirements will be classified as safety significant and included in technical specifications.

8.5.4 Lessons Learned and Mistakes of the Past

Lessons learned from the past (e.g., good plant housekeeping) should be applied in writing the requirements. Mistakes from the past should not be repeated. Examples include:

- preventing flow blockage
- no positive power coefficient;
- limiting control rod worth, and
- preventing direct impingement of molten core material on the containment shell.

A more complete list will be added in a future update.

8.5.5 Licensing Review and Plant Oversight

In developing the requirements, it is important to keep in mind how NRC reviews will determine whether or not the requirements have been met and what needs to be monitored and reviewed over the life of the plant as part of NRC's oversight program. Writing the requirements with clear criteria will help in formulating standard review plans that give guidance to the NRC reviewers as to what is acceptable. Also, as described in Section 8.5.3 above, developing requirements that are performance-based will be useful in plant oversight by providing clearly identified parameters to be monitored and allowing the formulation of performance indicators based upon these parameters. In this way there can be coherence between the regulations and plant oversight and the amount of oversight can be tied directly to regulation based plant performance. Also, clear criteria will assist in ensuring consistent and understandable enforcement actions.

8.5.6 Technology-Neutral Requirements

Applying the guidelines above to the topics identified in Section 8.3 and 8.4 will result in a set of technology-neutral requirements that can form the basis for a rulemaking to implement a risk-informed alternative to 10 CFR 50 for licensing new NPPs. These requirements are currently under development and will be included as Appendix I in a future update. However, currently a preliminary Appendix I contains some example proposed requirements to illustrate the format and level of detail envisioned in the technology-neutral requirements.

8.6 Technology-Specific Considerations

Some of the technology-neutral requirements will have technology specific solutions. For example, a technology-neutral requirement to maintain "coolable geometry" will require technology-specific guidance as to what represents a loss of coolable geometry. Other technology-neutral requirements will, likewise, require technology-specific guidance. Appendix I provides a preliminary identification of which topics will likely require technology-specific guidance for implementation.

Accordingly, it is envisioned that technology-specific regulatory guides will be necessary to implement some of the technology-neutral requirements. In fact, it may be desirable to develop, for each technology, a regulatory guide that addresses all of the technology-neutral regulations by either:

(1) providing technology-specific guidance, or

(2) referencing existing guidance that, due to its technology-neutral nature, would apply to any technology.

In this way, each technology would have a stand alone regulatory guide addressing all requirements. In developing the technology-neutral requirements, judgements should also be made and documented regarding the use of existing regulatory guides.

8.7 Completeness and Consistency Check

The framework provides general guidance regarding factors to consider when developing the requirements. As the requirements are developed, they will need to be checked for conformance with the framework. Specific criteria should be developed to guide the check and should include the following questions:

- Are all the topics identified in framework addressed?
- Have the requirements addressed all of the criteria and guidance in the framework?
- Have 10 CFR 50 requirements been used to the extent practical?
- Are the requirements risk-informed?
- Are the requirements performance-based?
- Do the requirements address mistakes of the past?
  - What regulatory oversight is needed?
  - What information is needed?
- Are the requirements enforceable?

Each of these criterion should be used to check the requirements after they are developed to ensure they are consistent with the intent of the framework and a practical regulatory process.

In addition, a check has been made on the completeness of the topics listed in Tables 8-6 and 8-9. This check consisted of comparing the topics in these tables to the content of 10 CFR 50, the IAEA safety standards for nuclear reactor design (IAEA document NS-R-1) and operation (IAEA document NS-R-2) and NEI document 02-02. These documents represent stand alone sets of requirements applicable to nuclear reactor design, construction and operation. The purpose of the review was to help ensure that the framework has identified all technical topics necessary for safety and all administrative topics necessary to licensing and regulatory oversight. The results of the review are documented in Appendix G of the framework.

Based upon the completeness check, the following items were included in the IAEA documents, but not identified using the process described in this chapter.

Items from IAEA Document NS-R-1

- management and organization
- safety culture
- minimizing radioactive waste generation
- ensuring fasilure of non-safety SSCs will not fail safety SSCs
- passive safety or continuously operating safety systems
- automatic safety actions in initial stage of accidents
- single failure criterion (framework uses probabilistic approach)
- escape routes
- consider decommissioning as part of the design
- design fuel assemblies to permit inspection
- coverings and coatings integrity
- design should address transport and packaging of radioactive waste
- design for on-line maintenance

Items from IAEA Document NS-R-2

- organizational responsibilities and functions
- qualification of personnel
- commissioning program
- core management and fuel handling
- spare parts procurement, storage and dissemination
- preparation for decommissioning

Each of these items will be reviewed against the protective strategies and their logic trees and if considered necessary to prevent failure of one or more protective strategies, will be added in a future update.

Appendix G also makes a preliminary assessment of what parts in 10 CFR 50 can be considered technology-neutral (or can be made technology-neutral) and thus should be considered for use in the technology-neutral requirements. As can be seen in Table 1 of Appendix G, there are many candidates for consideration.

6.1 U. S. Nuclear Regulatory Commision, “Safety Goals for the Operation of Nuclear Power Plants; Policy Statement,” Federal Register, Vol. 51, p. 30028, August 21, 1986.

6.2 U. S. Environmental Protection Agency, Office of Radiation and Indoor Air Radiation Protection Division, Protective Action Guides (PAG) Manual.

6.3 U. S. Nuclear Regulatory Commission, “Abnormal Occurrence Reports: Implementation of Section 208 Energy Reorganization Act of 1974,” 62 FR 18820, 1997.

6.4 International Commission on Radiation Protection, ICRP 41: Non-stochastic effects in ionizing radiation, 1984.

6.5 U. S. Nuclear Regulatory Commission, “Code manual for MACCS2,” NUREG/CR-6613, 1998.

6.6 U. S. Nuclear Regulatory Commission, “Health Effects Models for Nuclear Power Plant Consequence Analysis: Low LET Radiation,” NUREG/CR-4214, 1989.

6.7 Commission Policy Statement on the Regulation of Advanced Nuclear Power Plants, 59 FR 35461, 1994.

6.8 OECD Nuclear Energy Agency, “Definition of Generalized Concepts of Safety Margins and Characterization of Safety Margin Sources,” SMAP Technical note (SMAP Sub-task 1B), 2005.

6.9 U. S. Nuclear Regulatory Commission, White Paper on Integrating Risk and Safety Margins, Mirela Gavrilas, RES/DSARE/SMSAB.